WEBTRUST® FOR REGISTRATION AUTHORITIES

WEBTRUST PRINCIPLES AND CRITERIA FOR REGISTRATION AUTHORITIES

Version 1.1

Release Date:
1 November 2020

Effective Date:
For engagement periods commencing on or after 1 November 2020

Document History

Version	Publication Date	Revision Summary
1.0	April 2019	Initial release
1.1	November 2020	Updated to reflect changes to WebTrust for CA

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 (Staff Contact)
- Bryan Walker, Consultant
- Janet Treasure, Vice President, Member Development and Support
- Gord Beal, Vice President, Research, Guidance and Support

Table of Contents

Introduction

This document provides a framework for third party assurance providers to assess the adequacy and effectiveness of the controls employed by a Registration Authority (RA) that performs either a portion or all of the registration related functions for a Certification Authority (CA) *on an outsourced basis*. Assurance guidance for registration functions that are conducted directly by the CAs entirely are covered in the document, *WebTrust Principles and Criteria for Certification Authorities*.

The purpose of this guide is to set criteria and provide practitioner guidance for outsourced registration functions. It is important to note that, even when a CA outsources its RA function, the CA still must comply with *WebTrust Principles and Criteria for Certification Authorities* and ensure, through monitoring activities, that outsourced registration authorities comply with the relevant provisions of the CA's business practices disclosures, often documented in a Certification Practice Statement and applicable Certificate Policy(ies). Where an RA assists a CA in its registration process for Extended Validation Certificates, the RA must meet the applicable requirements of WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL. Where an RA assists a CA in its registration process for Extended Validation Code Signing, the RA must meet the applicable requirements of WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing. Where the CA is publicly trusted it also needs to comply with *WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security.* With this in mind, the relevant sections of those principles have been included in this RA framework as Principles 4 and 5.

This version is regarded as "open-source" and can be used in the conduct of any assurance engagement, internal or external, by any third-party service provider. It also represents an effective benchmark for RAs to conduct self-assessments. Further, it provides a mechanism for CAs to better monitor registration authority functions performed by their outsourced business partners.

The public accounting profession has continued to play its role, with an intent to increase consumer confidence in the application of PKI technology by establishing a basis for providing third party assurance to the assertions made by RAs, as well as CAs.

This document was developed by the CPA Canada WebTrust / PKI Assurance Task Force leveraging Version 2.2.1 of the CPA Canada WebTrust Principles and Criteria for Certification Authorities,, WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security. Input was also obtained from the Certification Authority Browser Forum (CA/Browser Forum – see www.cabforum.org) for the content and control activities contained in 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 various PKI related standards.

Effective Date

These Principles and Criteria are effective for engagement periods commencing on or after 1 November 2020. Earlier adoption is permitted and encouraged.

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. Anyone could also encrypt a message using the Subscriber's public key. The message can be decrypted only by the Subscriber using his/her 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 (CA) or a Registration Authority (RA), which acts as a delegated third party for the CA. The CA or RA verifies the identity of the subscriber in accordance with the CA's established business practices (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 securely 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. This is required in cases where the Certificate is used to "sign" something (for example when used for S/MIME or Code Signing). It is not required for "Authentication" services (Client/Server TLS).

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 a natural person's or legal entity's public key actually belongs to that natural person or legal entity? A digital certificate, which is an electronic document containing information about a natural person or legal entity and public key is the answer. This document is digitally signed by a trusted organization referred to as a Certification Authority (CA). The basic premise is that the CA is vouching for the link between an identity and a 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 publicly trusted 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 Internet Explorer and Edge, Mozilla Firefox, etc.) and serve as trust anchors. In the enterprise, a company may choose to provision users’ devices with additional Root CA certificates for its own internal PKI, or the PKI 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 internally. 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.

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 authorized the purchase.

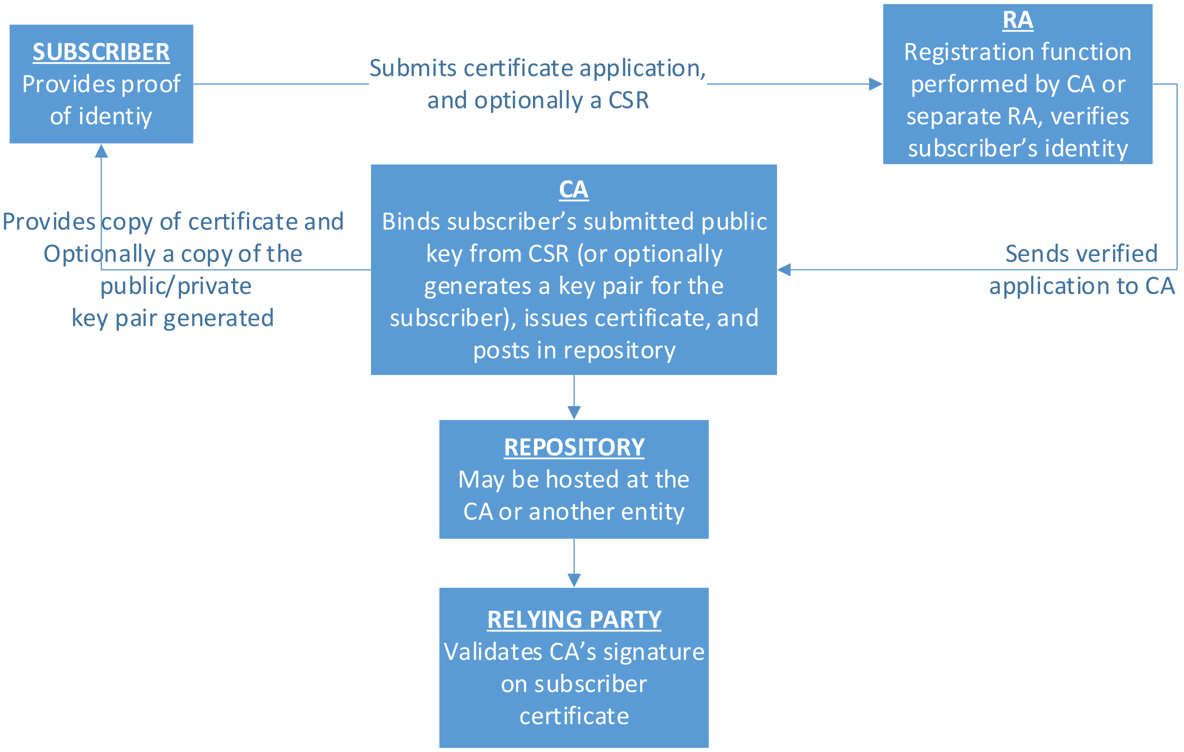
What is a Registration Authority?

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. It is typically submitted to the RA function. The RA function then delivers it to the CA function as part of the Certificate Signing Request (CSR) to sign and issue the end-entity certificate. 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.) 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 Delegated Third Party contracted for that purpose, 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. However, the purpose of the repository is to also provide certificate status information, like revocation dates, suspension and so on. This information is typically signed in a CRL but could also be an online database that is vulnerable to hacking attempts that might maliciously alter the status information of certain certificates.

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


SUBSCRIBER
Provides proof of identiy
Submits certificate application, and optionally a CSR
RA
Registration function performed by CA or separate RA, verifies subscriber's identity
Sends verified application to CA
CA
Binds subscriber's submitted public key from CSR (or optionally generates a key pair for the subscriber), issues certificate, and posts in repository
Provides copy of certificate and Optionally a copy of the public/private key pair generated
REPOSITORY
May be hosted at the CA or another entity
RELYING PARTY
Validates CA's signature on subscriber certificate

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 they 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 or both 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 is operated by the same entity as the CA) it should be included in the WebTrust for Certification Authorities engagement. Therefore, this guide would not be applicable.

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(ies). 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. Per the current CAB Forum requirements, 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(ies). These RAs are important to the CAs certificate issuance process, especially in regard to the additional validation requirements for Extended Validation Certificates. Since there is an expectation that the entire hierarchy for the CA is subject to third party assurance, including RAs. RAs are not part of the WebTrust for CA engagement of the CA since they are separate entities not controlled by the CA. They are, however, the focus of this WebTrust for Registration Authorities guide.

In order to be understandable to subscriber and relying parties, the principles set out in the following sections have been developed with the relying parties in mind and, as a result, are intended to be practical and nontechnical in nature.

Various RA Arrangements

There can be a wide variance in the services that an RA might perform for a CA. In some cases, they might perform only minor validation roles. (Consider, for example, some government agencies or postal offices sometimes play a role in validation of an individual's identity. It may be through face recognition, manual signature verification, ID check, etc. The rest of validation, including access to actual RA system, and other pre-issuance and issuance procedure happen at the CA.) The WebTrust for CA engagement covers the RA activities that are performed by the CA. The scope of the WebTrust for RA engagement will cover only the controls/activities exercised by the RA on behalf of the CA. They would not be extensive if the RA only acts as an independent agent.

Assignment of Responsibility and Accountability

The use of an external RA does not reduce the responsibility or accountability of the CA for its PKI operations. Aa a result, for example, the RA is not responsible for determining what changes need to be made to the CA-RA contract to meet ongoing CA needs. It is the responsibility of the CA to determine what requirements are needed and agree through its contract with the RA as to the procedures that need to be undertaken to meet such requirements. It would also be the responsibility of the CA to ensure that the RA has relevant updated Certificate Policy(ies) / Certification Practice Statement (CP/CPS) requirements. The RA would be responsible to the CA for meeting updated requirements according to its contractual obligations.

WebTrust Principles and Criteria for Registration Authorities

These Principles and Criteria are derived from WebTrust for Certification Authorities 2.1. In addition, principles and criteria have been added based on the requirements of WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security. These latter principles and criteria may be considered optional for private SSL at the present time.

Where the RA is contracted to provide its RA services on behalf of a number of CAs, the Criteria will need to be applied to each CA. For example, in RA business practices disclosure, each CA would need to be named and have its CP (or CPS as appropriate) referenced. If different security controls were employed, they would need to be identified and tested.

As addressed earlier, there can be a wide variance in the services that an RA might perform for a CA. In some cases, they might perform only minor validation roles. (Consider, for example, some government agencies or postal offices sometimes play a role in validation of an individual's identity. It may be through face recognition, manual signature verification, ID check, etc. The rest of validation, including access to actual RA system, and other pre-issuance and issuance procedure happen at the CA.) The scope of the WebTrust for RA engagement will cover only the controls/activities exercised by the RA on behalf of the CA. They would not be extensive if the RA only acts as an independent agent. Because of the wide variance, the RA system description, RA management assertion and detailed testing will only address the procedures and controls exercised by the RA that are in place to meet the contract with the CA. However, the relevant sections of the CA's CPS will need to be referenced as part of the business disclosure.

Registration Authorities Principles and Criteria

1.0: RA Business Practices Disclosure

The Registration Authority:

- Discloses its Business Practices (meaning, the identification and authentication process related to binding the individual subscriber to the certificate) in reference to the relevant provisions of the CA's business practices disclosures in the CA's Certification Practice Statement; and
- Discloses its Business Practices in compliance with the relevant provisions of the CA's business practices disclosures in the CA's Certificate Policy (if applicable).
- Where applicable, discloses any additional business practices that it undertakes that are not contained in the CA's business practice disclosure that might be relevant activities performed on behalf of the CA.

The RA should publicly disclose, or make reference to specific sections of the CA's CP/CPS for each CA that it provides services to, the relevant sections of the CA's Certification Practice Statement and, where applicable, the Certification Practice Statement of the CA that it is contracted to follow. There is normally no need for public disclosure of its detailed business practices where the RA is subject to the provisions of the CA's CP/CPS and at least one of these documents are publicly disclosed by the CA.

If the RA undertakes additional procedures that are not contained in a CA's CP/CPS, it may be useful for disclosure of such in a publicly available document.

2.0: RA Business Practices Management

The RA maintains effective controls to provide reasonable assurance that:

The RA provides its services in accordance with the applicable sections of the CA's Certification Practice Statement and Certificate Policy (if applicable) for those CAs under contract;

- Where applicable, the RA provides its services in accordance with any additional business practices that it undertakes that are not contained in the CA's business practice disclosure that are relevant activities performed on behalf of the CA.

It is important that the RA has controls in place to ensure that it is aware of the current service requirements of the CAs under contract in order to be able to meet such requirements. It is likewise important that it has controls in place to ensure that it performs any addition services in accordance with its disclosed business practices regarding such.

3.0: RA Environmental Controls

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

- Logical and physical access to RA systems and data is restricted to authorized individuals;
- RA systems development, maintenance and operations are properly authorized and performed to maintain RA/CA systems integrity.

The establishment and maintenance of a trustworthy RA environment is essential to the reliability of the RA's and CA's business processes.

The specific components of an RA system will likely vary according to its complexity. In general, however, it includes the full server infrastructure and databases supporting the RA function – including the RA application installed on the RA authorized personnel's workstation that then connects to the CA's back end order processing and signing systems.

Without strong RA environmental controls, the CA's key and certificate life cycle management controls are severely diminished in value. RA environmental controls include personnel security, physical and environmental security of the RA facility, operations management, system access management, systems development and maintenance, business continuity management, monitoring and compliance. The strength of the physical controls will normally be less than that expected at the CA facility where PKI materials need to be protected.

1.0 RA BUSINESS PRACTICES DISCLOSURE

The Registration Authority:

- Discloses its Business Practices (meaning, the identification and authentication process related to binding the individual subscriber to the certificate) in reference to the relevant provisions of the CA's business practices disclosures in the CA's Certification Practice Statement; and
- Discloses its Business Practices in compliance with the relevant provisions of the CA's business practices disclosures in the CA's Certificate Policy (if applicable).
- Where applicable, discloses any business practices that are not contained in the CA's business practice disclosure that are relevant activities performed on behalf of the CA.

#	**RA's Business Practices:**
1.1	The RA discloses, for each CA that it provides registration services for, • a summary of the services performed; • direct references to the relevant sections of the CA's CPS addressing the control requirements for the services it performs; • a link to the publicly available CPS for CA in scope for the RA.
1.2	Where applicable, for each CA that it provides registration services for, • direct references to the relevant sections of the CA's CP addressing the control requirements for the services it performs; • a link to the publicly available CP for CA in scope for the RA.

#	**Additional Business Practices**
1.3	Where applicable, for each CA that it provides registration services for, RA • discloses any business practices that are not contained in the CA's business practice disclosure that are relevant to the activities performed on behalf of the CA in a publicly available document.

2.0 RA BUSINESS PRACTICES MANAGEMENT

The RA maintains effective controls to provide reasonable assurance that:

- The RA provides its services in accordance with the applicable sections of the CA's Certification Practice Statement and Certificate Policy (if applicable) for those CAs under contract;
- Any additional business practices that it undertakes that are not contained in the CA's business practice disclosure are performed on behalf of the CA after approval by RA management.

#	**Criterion: Managing to CA Certification Practice Statement (CPS)**
2.1	The RA maintains controls to provide reasonable assurance that it follows the relevant sections of the CA's current Certification Practice Statement (CPS).

#	**Illustrative Controls: Managing to CA Certification Practice Statement (CPS)**
2.1.1	Responsibilities for contracting with the CA and identification of the relevant sections of the CA's CPS have been formally assigned.
2.1.2	Responsibilities for liaising with the CA to obtain any relevant changes to the CP/CPS have been assigned.

#	**Criterion : Provision of Additional Services**
2.2	The RA maintains controls to provide reasonable assurance that any additional services performed on behalf of the CA are risk-assessed and approved by RA management. … .

#	**Illustrative Controls : Additional Services Policy Management**
2.2.1	The RA management has final authority and responsibility for approving and implementing any additional services as requested by the CA.
2.2.2	A defined review process exists to assess whether controls in place sufficiently mitigate incremental risks resulting from introducing additional services.
2.2.3	Practices supporting additional services are made available in the underlying business practice disclosures.

3.0 RA ENVIRONMENTAL CONTROLS

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

- Logical and physical access to RA systems and data is restricted to authorized individuals;
- RA systems development, maintenance and operations are properly authorized and performed to maintain RA systems integrity.

3.1 Security Management

Criteria:

The RA maintains controls to provide reasonable assurance that:

- security is planned, managed and supported within the organization;
- security risks are identified and managed;
- the security of RA 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 by the RA to another sub service organization or entity.

#	**Illustrative Controls: 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	The information security policy includes the following: • a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing; • a statement of management intent, supporting the goals and principles of information security; • an explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization; • a definition of general and specific responsibilities for information security management, including reporting security incidents; and • references to documentation, which supports the policy.
3.1.3	There is a defined review process for maintaining the information security policy, including responsibilities and review dates.

#	**Illustrative Controls: Information Security Infrastructure**
3.1.4	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.
3.1.5	A management group or security committee exists to co-ordinate the implementation of information security controls and the management of risk.
3.1.6	Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined.
3.1.7	A management authorization process for new information processing facilities exists and is followed.

#	**Illustrative Controls: Security of Third Party Access**
3.1.8	Procedures exist and are enforced to control physical and logical access to RA facilities and systems by third parties (e.g., on-site contractors, trading partners and joint ventures).

#	**Illustrative Controls: Security of Third Party Access**
3.1.9	If there is a business need for the RA to allow third party access to RA facilities and systems, a risk assessment is performed to determine security implications and specific control requirements.
3.1.10	Arrangements involving third party access to RA facilities and systems are based on a formal contract containing necessary security requirements.

#	**Illustrative Controls: Outsourcing**
3.1.11	If the RA outsources the management and control of all or some of its information systems, networks, and/or desktop environments, the security requirements of the RA are addressed in a contract agreed upon between the parties. The RA maintains responsibility for the completion of the outsourced functions in accordance with the CA's CPS.

3.2 Asset Classification and Management

Criteria:

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

#	**Illustrative Controls:**
3.2.1	Owners are identified for all RA assets and assigned responsibility for the protection of the assets.
3.2.2	Inventories of RA assets (including an equipment inventory) are maintained.
3.2.3	The RA has implemented information classification and associated protective controls for information based on business needs and the business impacts associated with such needs (based on expectations of the CAs for which services are being performed).
3.2.4	Information labeling and handling are performed in accordance with the RA's information classification scheme and documented procedures.

3.3 Personnel Security

Criteria:

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

#	**Illustrative Controls:**
3.3.1	The RA employs personnel (i.e., employees and contractors) who possess the relevant skills, knowledge and

#	**Illustrative Controls:**
	experience required for the job function.
3.3.2	Security roles and responsibilities, as specified in the organization's security policy, are documented in job descriptions.
3.3.3	The RA's policies and procedures specify the requirement for performing background checks and clearance procedures on a regular basis (including job application).
3.3.4	RA employees sign a confidentiality (non-disclosure) agreement as a condition of employment.
3.3.5	Contractors are subject to at least the same background check and personnel management procedures as employees.
3.3.6	Any contract arrangement between contractors and RAs allows for the provision of temporary contract personnel explicitly allowing the organization to take measures against contract staff who violate the organization's security policies. Protective measures may include: • bonding requirements on contract personnel; • indemnification for damages due to contract personnel willful harmful actions; and • financial penalties.
3.3.7	A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures. The RA's policies and procedures specify the sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems.
3.3.8	Physical and logical access to RA facilities and systems is disabled upon termination of employment.
3.3.9	All employees of the organization and, where relevant, third party contractors, receive appropriate training in organizational policies and procedures. The RA's policies and procedures specify the following: • The training requirements and training procedures for each role; and • Any retraining period and retraining procedures for each role.

3.4 Physical and Environmental Security

Criteria:

Based on the CA's risk requirements and the requirements as set out in each relevant CA's CPS, the RA maintains controls to provide reasonable assurance that:

- physical access to RA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control;
- RA 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.

#	**Illustrative Controls: RA Facility Physical Security**
3.4.1	Entry to the building or site is achieved only through a limited number of controlled access points.

#	**Illustrative Controls: RA Facility Physical Security**
3.4.2	A staffed reception area or other means to control physical access is in place to restrict access to the building or site housing RA operations to authorized personnel only.
3.4.3	Fire doors on security perimeters around RA operational facilities are alarmed and conform to local fire regulations.
3.4.4	Intruder detection systems are installed and regularly tested to cover all external doors of the building housing the RA operational facilities.
3.4.5	RA operational facilities are physically locked and alarmed when unoccupied.
3.4.6	All personnel are required to wear visible identification.
3.4.7	Access to RA operational facilities is controlled and restricted to authorized persons through the use of multi-factor authentication controls.
3.4.8	All personnel entering and leaving RA operational facilities are logged (i.e., an audit trail of all access is securely maintained). Use of a Badging system is sufficient for permanent personnel.
3.4.9	Entry, exit within RA facilities are monitored by cameras.
3.4.10	Visitors to RA facilities are supervised and their date and time of entry and departure recorded.
3.4.11	Third party support services personnel are granted restricted access to secure RA operational facilities only when required and such access is authorized and accompanied.
3.4.12	Access rights to RA facilities are regularly reviewed and updated.

#	**Illustrative Controls: Equipment Security**
3.4.13	Equipment is sited or protected such as to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
3.4.14	Equipment is protected from power failures and other electrical anomalies.
3.4.15	Power and telecommunications, within the facility housing the RA operation, cabling carrying data or supporting RA services is protected from interception or damage.
3.4.16	Equipment is maintained in accordance with the manufacturer's instructions and/or other documented procedures.
3.4.17	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.

#	**Illustrative Controls: General Controls**
3.4.18	Sensitive or critical business information is locked away when not required and when the RA facility is vacated.
3.4.19	Procedures require that personal computers and workstations are logged off or protected by key locks, passwords or other controls when not in use.
3.4.20	The movement of materials to/from the RA facility requires prior authorization.

3.5 Operations Management

Criteria:

The RA maintains controls to provide reasonable assurance that:

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

#	**Illustrative Controls: Operational Procedures and Responsibilities**
3.5.1	RA operating procedures are documented and maintained for each functional area.
3.5.2	Formal management responsibilities and procedures exist to control all changes to RA equipment, software and operating procedures.
3.5.3	Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorized 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.

#	**Illustrative Controls: System Planning and Acceptance**
3.5.6	Capacity demands are monitored and projections of future capacity requirements are 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 are carried out prior to acceptance.

#	**Illustrative Controls: Protection Against Viruses and Malicious Software**
3.5.8	Detection and prevention controls (including employee awareness programs) to protect against viruses and malicious software are implemented.

#	**Illustrative Controls: 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 that warrant communication based on policy are reported to management as a matter of urgency.
3.5.10	Users of RA 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.

#	**Illustrative Controls: Media Handling and Security**
3.5.14	Procedures for the management of removable computer media require the following: • if no longer required, the previous contents of any reusable media that are to be removed from the organization are erased or media is destroyed; • authorization is required for all media removed from the organization and a record of all such removals to maintain an audit trail is kept; and • all media are stored in a safe, secure environment, in accordance with manufacturers' specifications.
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 unauthorized disclosure or misuse.
3.5.17	System documentation is protected from unauthorized access.

3.6 System Access Management

Criteria:

The RA maintains controls to provide reasonable assurance that RA system access is limited to authorized individuals. Such controls provide reasonable assurance that, where used and controlled by the RA:

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

#	**Illustrative Controls: 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: • roles and corresponding access permissions; • identification and authentication process for each user; and • segregation of duties
3.6.2	There is a formal user registration and de-registration procedure for access to RA information systems and services.
3.6.3	The allocation and use of privileges is restricted and controlled.
3.6.4	The allocation of privileges and passwords is controlled through a formal management process.
3.6.5	Access rights for users 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 is protected.

#	**Illustrative Controls: Network Access Control**
3.6.8	RA employed personnel are provided direct access only to the services that they have been specifically authorized to use. The path from the user terminal to computer services is controlled.
3.6.9	Remote access to RA systems, made by RA employees or external systems, if permitted, requires authentication.
3.6.10	Connections made by RA employees or RA systems to remote computer systems are authenticated.
3.6.11	Access to diagnostic ports is securely controlled.
3.6.12	Controls (e.g., firewalls) are in place to protect the RA's internal network domain from any unauthorized access from any other domain.

#	**Illustrative Controls: Network Access Control**
3.6.13	Controls are in place to limit the network services (e.g., HTTP, FTP, etc.) available to authorized users in accordance with the RA's access control policies. The security attributes of all network services used by the RA organization are documented by the RA.
3.6.14	Routing controls are in place to ensure that computer connections and information flows do not breach the RA's access control policy.
3.6.15	The RA maintains local network components (e.g., firewalls and routers) in a physically secure environment and audits their configurations periodically for compliance with the RA's configuration requirements.
3.6.16	Sensitive data is encrypted when exchanged over public or untrusted networks.

#	**Illustrative Controls: Operating System and Database Access Control**
3.6.17	Operating systems and databases are configured in accordance with the RA's system configuration standards and periodically reviewed and updated.
3.6.18	Operating system and database patches and updates are applied in a timely manner when deemed necessary based on a risk assessment.
3.6.19	Automatic terminal identification is used to authenticate connections to specific locations and to portable equipment.
3.6.20	Access to RA systems requires a secure logon process.
3.6.21	All RA 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.
3.6.22	Uses of system utility programs are restricted to authorized personnel and tightly controlled.
3.6.23	Inactive terminals serving RA systems require re-authentication prior to use.
3.6.24	Restrictions on connection times are used to provide additional security for high-risk applications.
3.6.25	Sensitive data is protected against disclosure to unauthorized users.

#	**Illustrative Controls: Application Access Control**
3.6.26	Access to information and application system functions is restricted in accordance with the RA's access control policy.
3.6.27	RA personnel are successfully identified and authenticated before using critical applications related to certificate management.

3.7 Systems Development and Maintenance

Criteria:

The CA maintains controls to provide reasonable assurance that RA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain RA system integrity.

This may be optional depending on the extent to which the RA has built its own system and workflow to enforce defined CA requirements.

#	Illustrative Controls:
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 and emergency software fixes.
3.7.3	Change control procedures exist and are followed for the hardware, network, 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	Modifications to software packages are discouraged and all changes are strictly controlled.
3.7.8	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 Business Continuity Management

Criteria:

The RA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation or degradation of the RA's services. The RA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls include, at a minimum:

- the development and testing of a RA business continuity plan that includes a disaster recovery process for critical components of the RA system based on, as a minimum, the requirements of the CAs that services are being provided to;
- the storage of backups of systems, data and configuration information at an alternate location.

#	Illustrative Controls
3.8.1	The RA has a managed process for developing and maintaining its business continuity plans. The RA has a business continuity planning strategy based on an appropriate risk assessment.

#	Illustrative Controls
3.8.2	The RA has a business continuity plan to maintain or restore the RA's operations, in a time period acceptable to the CAs to which the RA provides service, following interruption to, or failure of, critical RA processes. The RA's business continuity plan addresses the following: • the conditions for activating the plans; • emergency procedures; • fallback procedures; • resumption procedures; • a maintenance schedule for the plan; • awareness and education requirements; • the responsibilities of the individuals; • recovery time objective (RTO); and • regular testing of contingency plans.
3.8.3	The RA's business continuity plans include disaster recovery processes for all critical components of the RA system, including the hardware, software and, where applicable, keys, in the event of a failure of one or more of these components.
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 RA identifies and arranges for an alternate site where core registration related operations can be restored in the event of a disaster at the RA's primary site. Fallback equipment and backup media are sited at a safe distance to avoid damage from disaster at the main site.
3.8.6	The RA'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 RA's business continuity plans address the recovery procedures used if computing resources, software, and/or data are corrupted or suspected to be corrupted.
3.8.8	Business continuity plans are maintained by regular reviews and are tested regularly to ensure that they are up to date and effective.
3.8.9	Business continuity plans define an acceptable system outage time, recovery time, and the average time between failures as disclosed in the CA's CP and/or CPS.
3.8.10	The RA maintains procedures for the termination, notification of affected entities, and for transferring relevant archived RA records to a custodian as disclosed in the CA's CP and/or CPS.

3.9 Monitoring and Compliance

Criteria:

To the extent applicable. The RA maintains controls to provide reasonable assurance that:

- it conforms with the relevant legal, regulatory and contractual requirements with relevant CAs and others as applicable;
- compliance with the RA's security policies and procedures is ensured;

- the effectiveness of the system audit process is maximized and interference to and from the system audit process is minimized; and
- unauthorized RA system usage is detected.

#	**Illustrative Controls: Compliance with Legal Requirements**
3.9.1	Relevant statutory, regulatory and contractual requirements are explicitly defined and documented in the business practices disclosure.
3.9.2	The RA 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.
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: ● the information that must be kept confidential by RA; ● the information that is not considered confidential; ● the policy on release of information to law enforcement officials; ● information that can be revealed as part of civil discovery; ● the conditions upon which information may be disclosed with the subscriber's consent; and ● any other circumstances under which confidential information may be disclosed.
3.9.6	RA records are protected from loss, unauthorized destruction and falsification.

#	**Illustrative Controls: Review of Security Policy and Technical Compliance**
3.9.7	Managers are responsible for ensuring that security procedures within their area of responsibility are carried out correctly through appropriate monitoring activities.
3.9.8	The RA's operations are subject to regular review by either internal or external assessors to ensure timely compliance with the relevant CA's CPS and additional disclosed business practices, if applicable.
3.9.9	RA systems are periodically checked for compliance with security implementation standards.

#	**Illustrative Controls: System Audit Process**
3.9.10	Audits of operational systems are planned as to minimize the risk of disruptions to business processes.
3.9.11	Access to system audit tools is protected to prevent possible misuse or compromise.

#	**Illustrative Controls: Monitoring System Access and Use**
3.9.12	Procedures for monitoring the use of RA systems are established which include the timely identification and follow up of unauthorized or suspicious activity. Alerting mechanisms are implemented to detect unauthorized access.

3.10 Audit Logging

Criteria:

To the extent applicable, the RA maintains controls to provide reasonable assurance that:

- significant events (as defined by the relevant CA) 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 authorized personnel.

#	**Illustrative Controls: Audit Logs**
3.10.1	All journal/transactional entries include the following elements: • date and time of the entry; • serial or sequence number of entry (for automatic journal entries); • kind of entry; • source of entry (e.g., terminal, port, location, customer, etc.); and • identity of the entity making the journal entry.

#	**Illustrative Controls: Events Logged**
3.10.2	The RA records the following certificate application information: • the method of identification applied and information used to meet subscriber requirements; • record of unique identification data, numbers, or a combination thereof (e.g., applicant’s driver’s license number) of identification documents, if applicable; • storage location of copies of applications and identification documents; • identity of entity accepting the application; • method used to validate identification documents, if any; • name of receiving CA or submitting RA, if applicable; • the subscriber’s acceptance of the Subscriber Agreement; and • where required under privacy legislation, the Subscriber’s consent to allow the RA to keep records containing personal data, pass this information to specified third parties, and publication of certificates.
3.10.3	The RA logs the following security-sensitive events: • security-sensitive files or records read or written including the audit log itself; • actions taken against security-sensitive data; • security profile changes; • use of identification and authentication mechanisms, both successful and unsuccessful (including multiple failed authentication attempts); • system crashes, hardware failures and other anomalies; • actions taken by individuals in computer operators, system administrators, and system security officers;

#	**Illustrative Controls: Events Logged**
	• change of affiliation of an entity; • decisions to bypass encryption/authentication processes or procedures; and • access to the RA system or any component thereof.
3.10.4	RA computer system clocks are synchronized for accurate recording as defined in the relevant CA's CP and/or CPS that specifies the accepted time source.

#	**Illustrative Controls: Audit Log Protection**
3.10.5	Current and archived audit logs are maintained in a form that prevents their modification, substitution, or unauthorized destruction.
3.10.6	Digital signatures are used to protect the integrity of audit logs where applicable or required to satisfy legal requirements.
3.10.7	The private key used for signing audit logs is not used for any other purpose.

#	**Illustrative Controls: Audit Log Archival**
3.10.8	The RA archives audit log data on a periodic basis as disclosed in the CA's CP and/or CPS.
3.10.9	In addition to possible regulatory stipulation, a risk assessment is performed to determine the appropriate length of time for retention of archived audit logs.
3.10.10	The RA maintains archived audit logs at a secure off-site location for a predetermined period as determined by risk assessment and legal requirements.

#	**Illustrative Controls: Review of Audit Logs**
3.10.11	Current and archived audit logs are only retrieved by authorized individuals for valid business or security reasons.
3.10.12	Audit logs are reviewed periodically according to the practices established in the CA's 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 unauthorized or suspicious activity.

4.0 CERTIFICATE LIFE CYCLE MANAGEMENT CONTROLS

The Certification Registration Authority maintains effective controls to provide reasonable assurance that Subscriber information is properly authenticated.

4.1 Subscriber Registration

Criteria:

The RA maintains controls to provide reasonable assurance that:

For authenticated certificates

- Subscribers are accurately identified in accordance with the RA's business practices; and
- Subscriber's certificate requests are accurate, authorized and complete.

For domain validated certificates

- Subscribers' domain names are accurately validated in accordance with the RA's business practices; and
- Subscriber's certificate requests are accurate and complete.

#	Illustrative Controls: Identification and authentication
4.1.1	For authentication certificates, the RA verifies the credentials presented by a subscriber as evidence of identity or authority to perform a specific role in accordance with the requirements of the relevant CA's CP/CPS. For individual end entity certificates, the 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. For organizational certificates (including role based, server, network resource, code signing, etc.), the RA verifies the legal existence of the organization's name and the authority of the requesting party to be included in the organization attribute in the subscriber distinguished name field of the certificate. An unauthenticated organization name is not included in a certificate. For organizational certificates containing a domain name of an organization, the RA verifies the organization'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.
4.1.2	The RA verifies the accuracy of the information included in the requesting entity's certificate request in accordance with the relevant CA's CP/CPS.
4.1.3	The RA checks the Certificate Request for errors or omissions in accordance with the relevant CA's CP/CPS.
4.1.4	The RA verifies the uniqueness of the subscriber's distinguished name within the boundaries of community defined by the CA's CP/CPS.
4.1.5	Encryption and access controls are used to protect the confidentiality and integrity of registration data in transit and in storage.
4.1.6	At the point of registration (before certificate issuance) the RA informs the Subscriber of the terms and conditions regarding use of the certificate.

#	**Illustrative Controls: Identification and authentication**
4.1.7	Before certificate issuance, the RA informs the Subscriber of the terms and conditions regarding use of the certificate.

#	**Illustrative Controls: Certificate Request**
4.1.8	The RA requires that an entity requesting a certificate must prepare and submit the appropriate certificate request data as specified in the CA's CP.
4.1.9	The RA requires that the requesting entity submit its public key in a self-signed message to the RA for certification. The RA 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: • allow the detection of errors in the certificate application process; and • prove possession of the companion private key for the public key being registered.
4.1.10	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.
4.1.11	The RA submits the requesting entity's certificate request data to the CA in a message (Certificate Request) signed by the RA.
4.1.12	The RA secures that part of the certificate application process for which it assumes responsibility in accordance with the CA's CPS.
4.1.13	The RA records their actions for a certificate request in an audit log.

4.2 Certificate Renewal (if supported)

Criteria:

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

#	**Illustrative Controls: Certificate Renewal Request**
4.2.1	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.
4.2.2	The RA 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.
4.2.3	For renewal of authenticated certificates, the RA processes the certificate renewal data to verify the identity of the requesting entity and to identify the certificate to be renewed.
4.2.4	The RA validates the signature on the Certificate Renewal Request.

#	**Illustrative Controls: Certificate Renewal Request**
4.2.5	The RA verifies the existence and validity of the certificate to be renewed.
4.2.6	The RA verifies that the request, including the extension of the validity period, meets the requirements defined in the relevant CA's CP/CPS.
4.2.7	The RA submits the Certificate Renewal Data to the CA in a message (Certificate Renewal Request) signed by the RA.
4.2.8	The RA secures that part of the certificate renewal process for which it assumes responsibility in accordance with the relevant CA's CP/CPS.
4.2.9	The RA records their actions in an audit log.
4.2.10	The RA checks the Certificate Renewal Request for errors or omissions.

4.3 Certificate Rekey

Criteria:

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

#	**Illustrative Controls:**
4.3.1	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 RA to identify the certificate to rekey.
4.3.2	The RA requires that the requesting entity digitally sign, using the existing private key, the Certificate Rekey Request containing the new public key.
4.3.3	For authenticated certificates, the RA processes the Certificate Rekey Request to verify the identity of the requesting entity and identify the certificate to be rekeyed.
4.3.4	The RA validates the signature on the Certificate Rekey Request.
4.3.5	The RA verifies the existence and validity of the certificate to be rekeyed.
4.3.6	The RA verifies that the Certificate Rekey Request meets the requirements defined in the relevant CA's CP.
4.3.7	The RA submits the entity's certificate rekey request to the CA in a message signed by the RA.
4.3.8	The RA secures that part of the certificate rekey process for which it assumes responsibility.
4.3.9	The RA records their actions in an audit log.
4.3.10	The RA checks the Certificate Rekey Request for errors or omissions.

#	**Illustrative Controls:**
4.3.11	Prior to the generation and issuance of rekeyed certificates, the RA verifies the following: • the signature on the certificate rekey data submission; • the existence and validity supporting the rekey request; and • that the request meets the requirements defined in the CA's CP/CPS.

4.4 Certificate Revocation

Criterion

The RA maintains controls to provide reasonable assurance that validated certificate revocation requests are processed within the time frame in accordance with the relevant CA's business practices.

#	**Illustrative Controls:**
4.4.1	The RA verifies the identity and authority of the entity requesting revocation of a certificate in accordance with the relevant CA's CP.
4.4.2	If an external RA accepts revocation requests, the RA submits signed certificate revocation requests to the relevant CA in an authenticated manner in accordance with that CA's CP.
4.4.3	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.
4.4.4	The RA records all certificate revocation requests and their outcome in an audit log.
4.4.5	The RA may provide an authenticated acknowledgement (signature or similar) of the revocation to the entity who perpetrated the revocation request.
4.4.6	Where certificate renewal is supported, when a certificate is revoked, all valid instances of the certificate are also revoked and are not reinstated.
4.4.7	The Subscriber of a revoked or suspended certificate is informed of the change of status of its certificate.

Appendix 1

RA Additional Baseline and Network Security Criteria and Controls (public SSL)

The Network Security Requirements apply to all CAs within a publicly trusted PKI hierarchy, even if those certificates are designed for other uses (i.e. code signing, client authentication, secure email, document signing, etc.). Where an RA acts on behalf of a public CA, it needs to make sure that the relevant sections of the baseline and network security requirements are met.

Where the CA is publicly trusted and is required to follow the Baseline and Network Security requirements of the CA Browser Forum, the following criteria should be added to the engagement:

5.1 RA SSL Baseline Requirements Business Practices Disclosure

The Registration Authority

- discloses its SSL Certificate practices and procedures (meaning, the identification and authentication process related to binding the individual subscriber to the certificate) in reference to the relevant provisions of the CA's EV business practices disclosures in the CA's Certification Practice Statement in reference to the Baseline and Network security requirements; and
- discloses its Business Practices in compliance with the relevant provisions of the CA's business practices disclosures in the CA's Certificate Policy (if applicable).

Consistent with non-EV and EV SSL registration activities, the RA should publicly disclose, for each CA that it provides services to, the relevant sections of the CA's Certification Practice Statement and, where applicable, the Certification Practice Statement of the CA that it is contracted to follow for EV registration services. There is normally no need for public disclosure of its detailed business practices where the RA is subject to the provisions of the CA's CP/CPS and at least one of these documents are publicly disclosed by the CA.

#	**RA's Business Practices:**
5.1.1	The RA discloses, for each CA that it provides registration services for, • a summary of the services performed; • direct references to the relevant sections of the CPS addressing the control requirements for the services it performs • a link to the publicly available CPS.
5.1.2	Where applicable, for each CA that it provides registration services for, • direct references to the relevant sections of the CP addressing the control requirements for the services it performs • a link to the publicly available CP.

#	**Additional Business Practices**
5.1.3	Where applicable, for each RA that it provides registration services for, • discloses any business practices that are not contained in the CA's business practice disclosure that might be relevant activities performed on behalf of the CA in a publicly available document.

5.2 RA SSL Service Integrity

The RA maintains effective controls to provide reasonable assurance that:

- Subscriber information was properly collected, authenticated (for the registration activities performed by the Registration Authority) and verified.

#	**Criterion**
5.2	When acting on behalf of a CA in performing RA verification procedures, the RA performs the verification procedures contracted with the CA to meet the verification requirements set out by the CA/Browser Forum

#	**Illustrative Controls:**
5.2.1	The RA maintains controls to provide reasonable assurance that the RA, prior to the issuance of a Certificate by the CA obtains the following documentation from the Applicant: 1. A certificate request, which may be electronic; 2. An executed Subscriber or Terms of Use Agreement, which may be electronic; and 3. Any additional documentation the CA determines necessary to meet the Baseline Requirements. (See Baseline 4.1.2)
5.2.2	The RA maintains controls to provide reasonable assurance that the Certificate Request is: • obtained and complete prior to the issuance of Certificates; • signed by an authorized individual (Certificate Requester); • properly certified as to being correct by the applicant; and • contains the information specified in Section 4.2.1 of the SSL Baseline Requirements. (See Baseline 4.1.2 and 4.2.1)
5.2.3	For verification of Subject Identity Information, the RA maintains controls to provide reasonable assurance that the following information provided by the Applicant is verified directly by performing the steps established by the SSL Baseline Requirements: • Identity (SSL Baseline Requirements Section 3.2.2.1) • DBA/Trade name (SSL Baseline Requirements Section 3.2.2.2) • Authenticity of Certificate Request (SSL Baseline Requirements Section 3.2.5) • Verification of Individual Applicant (SSL Baseline Requirements Section 3.2.3) • Verification of Country (SSL Baseline Requirements Section 3.2.2.3) (See Baseline 3.2.2.1, 3.2.2.2, 3.2.5, 3.2.3, 3.2.2.3)

#	**Illustrative Controls:**
5.2.4	For verification of Subject Identity Information, the RA maintains controls to provide reasonable assurance that it inspects any document relied upon for identity confirmation for alteration or falsification. (See Baseline 3.2.2)
5.2.5	For verification of Subject Identity Information, the RA maintains controls to provide reasonable assurance that the CA does not use any data or document from a source specified under Section 3.2 of SSL Baseline Requirements to validate a certificate request if the data or document was obtained more than 825 days prior to issuing the Certificate (See Baseline 4.2.1)
5.2.6	For verification of Subject Identity Information, the RA maintains controls to provide reasonable assurance that the RA identifies high risk certificate requests and conducts additional verification activities in accordance with the SSL Baseline Requirements and that sufficient records are kept to document which method was used. (See Baseline 4.2.1)
5.2.7	For verification of Subject Identity Information, the RA maintains controls to provide reasonable assurance that, prior to using a data source, the RA evaluates the data source's accuracy and reliability in accordance with the requirements set forth in Section 3.2.2.7 of the SSL Baseline Requirements. (See Baseline 3.2.2.7)

#	**Criterion**
5.3	When acting on behalf of a CA in performing RA verification procedures, the RA maintains proper segregation of duties and ensures its employees are properly screened and trained.

#	**Illustrative Controls:**
5.3.1	The RA maintains controls to verify the identity and trustworthiness of an employee, agent, or independent contractor prior to engagement of such persons in the Certificate Management Process. (See Baseline 5.3.1)
5.3.2	The RA maintains controls to provide reasonable assurance that: • the RA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements. • the RA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. • the RA documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. • the RA requires all Validation Specialists to pass an examination provided by the RA on the information verification requirements outlined in the Baseline Requirements. • all personnel in Trusted Roles maintain skill levels consistent with the RA's training and performance programs. (See Baseline 5.3.3 and 5.3.4)

#	Illustrative Controls:
5.3.3	For High Risk Certificate Requests, the RA maintains controls to provide reasonable assurance that the RA verifies that the Delegated Third Party's processes to identify and further verify High Risk Certificate Requests meets the requirements of the relevant CA's own processes for High Risk Certificate Requests. (See Baseline 4.2.1)

5.4: RA Environmental Security

The RA maintains effective controls to provide reasonable assurance that:

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

#	Criterion
5.4.1	The RA maintains controls to provide reasonable assurance that it develops, implements, and maintains a comprehensive security program based on the relevant CA's requirements and risk assessment designed to: • protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes; • protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes; • protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes; • protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and • comply with all other security requirements applicable to the CA by law. (See Baseline 5.0)
5.4.2	The RA maintains controls to provide reasonable assurance that it performs a risk assessment at least annually which: • Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes; • Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and • Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the RA has in place to counter such threats. (See Baseline 5.0, 5.4.8)
5.4.3	The RA maintains controls to provide reasonable assurance that it develops, implements, and maintains a Security Plan consisting of security procedures, measures, and products designed to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan: • includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes;

#	Criterion
	• takes into account then-available technology and the cost of implementing the specific measures; and • is designed to implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected. (see Baseline 5.0)
5.4.4	The RA maintains controls to provide reasonable assurance that it develops, implements, and maintains a Business Continuity Plan that includes at a minimum: • the conditions for activating the plan; • emergency procedures; • fall-back procedures; • resumption procedures; • a maintenance schedule for the plan; • awareness and education requirements; • the responsibilities of the individuals; • recovery time objective (RTO); • regular testing of contingency plans; • the RA's plan to maintain or restore the RA's business operations in a timely manner following interruption to or failure of critical business processes; • a requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • what constitutes an acceptable system outage and recovery time; • how frequently backup copies of essential business information and software are taken; • the distance of recovery facilities to the RA's main site; and • 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. The Business Continuity Plan is tested at least annually, reviewed, and updated.[1] (See Baseline 5.7.1).
5.4.5	The RA maintains controls to provide reasonable assurance that its Certificate Verification Process includes: • physical security and environmental controls (see WTCA 2.2.1 Section 3.4); • system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention (see WTCA 2.2.1 Section 3.7); • network security and firewall management, including port restrictions and IP address filtering (see WTCA 2.2.1 Section 3.6); • user management, separate trusted-role assignments, education, awareness, and training (see WTCA 2.2.1 Section 3.3); and • logical access controls, activity logging, and inactivity time-outs to provide individual accountability (see WTCA 2.2.1 Section 3.6).
5.4.6	The RA maintains controls to provide reasonable assurance that: • physical access to RA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control;

[1] For organizations that are undergoing a WebTrust for CA audit (examination), all of the above are required and already tested with the exception of the disclosure of the distance of recovery facilities to the CA's main site.

#	Criterion
	- RA 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. (See Baseline 5.0 (See WTCA 2.2.1 Section 3.4))
5.4.7	The RA maintains controls to provide reasonable assurance that RA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity. (See Baseline 5.0 (WTCA2.2.1 Section 3.7)
5.4.8	The RA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that: - operating system and database access is limited to authorized individuals with predetermined task privileges; - access to network segments housing CA systems is limited to authorized individuals, applications and services; and - CA application use is limited to authorized individuals. Such controls must include, but are not limited to: - network security and firewall management, including port restrictions and IP address filtering; - logical access controls, activity logging (WTCA 2.2.1 Section 3.10), and inactivity time-outs to provide individual accountability. (See Baseline 5.0 (WTCA 2.2.1 Section 3.6))
5.4.9	The RA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations. (See Baseline 5.0 (WTCA 2.2.1 Section 3.3))
5.4.10	The RA maintains controls to provide reasonable assurance that: - significant CA environmental, 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 authorized personnel. (See Baseline 5.0 (WTCA 2.2.1 Section 3.10))

5.5: Network and Certificate System Security Requirements

The RA maintains effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

#	Criterion
5.5.1	The RA maintains controls to provide reasonable assurance that Certificate Systems are segmented into networks or zones based on their functional, logical, and physical (including location) relationship. (See network security 1.a)

#	Criterion
5.5.2	The RA maintains controls to provide reasonable assurance that the same security controls for Certificate Systems apply to all systems co-located in the same zone. (See network security 1.b)
5.5.3	The RA maintains controls to provide reasonable assurance that Certificate Systems, and Security Support Systems are maintained and protected in at least a Secure Zone. (See network security 1.d)
5.5.4	The RA maintains controls to provide reasonable assurance that Security Support Systems are implemented and configured to protect systems and communications between systems inside Secure Zones, and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks. (See network security 1.e)
5.5.5	The RA maintains controls to provide reasonable assurance that networks are configured with rules that support only the services, protocols, ports, and communications that the RA has identified as necessary to its operations. (See network security 1.f)
5.5.6	The RA maintains controls to provide reasonable assurance that Security Support Systems, and Front-End / Internal-Support Systems are configured by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the RA's or Delegated Third Party's operations and allowing only those that are approved by the RA or Delegated Third Party. (See network security 1.g)
5.5.7	The RA maintains controls to provide reasonable assurance that configurations of Certificate Systems, Security Support Systems, and Front-End / Internal-Support Systems are reviewed on at least a weekly basis to determine whether any changes violated the RA's security policies. (See network security 1.h)
5.5.8	The RA maintains controls to provide reasonable assurance that administration access to Verification Systems is granted only to persons acting in Trusted Roles and require their accountability for the Certificate System's security. (See network security 1.i)
5.5.9	The RA maintains controls to provide reasonable assurance that multi-factor authentication is implemented to each component of the Certificate System that supports it. (See network security 1.j)
5.5.10	The RA maintain controls to provide reasonable assurance that authentication keys and passwords for any privileged account or service account on a Certificate System are changed, when a person's authorization to administratively access that account on the Verification System is changed or revoked. (See network security 1.k)
5.5.11	The RA maintains controls to provide reasonable assurance that recommended security patches are applied to Verification Systems within six months of the security patch's availability, unless the RA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch. (See network security 1.l)

TRUSTED ROLES, DELEGATED THIRD PARTIES, AND SYSTEM ACCOUNTS

#	Criterion
5.6.1	The RA maintains controls to provide reasonable assurance that a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them is followed. (See network security 2.a)
5.6.2	The RA maintains controls to provide reasonable assurance that the responsibilities and tasks assigned to Trusted Roles are documented and “separation of duties” for such Trusted Roles based on the risk assessment of the functions to be performed is implemented. (See network security 2.b)
5.6.3	The RA maintains controls to provide reasonable assurance that only personnel assigned to Trusted Roles have access to Secure Zones. (See network security 2.c)
5.6.4	The RA maintains controls to provide reasonable assurance that individuals in a Trusted Role act only within the scope of such role when performing administrative tasks assigned to that role. (See network security 2.d)
5.6.5	The RA maintains controls to provide reasonable assurance that employees and contractors observe the principle of “least privilege” when accessing, or when configuring access privileges on, Certificate Systems. (See network security 2.e)
5.6.6	The RA maintains controls to provide reasonable assurance that Trusted Roles use a unique credential created by or assigned to that person for authentication to Certificate Systems. (See network security 2.f)
5.6.7	The RA maintains controls to provide reasonable assurance that Trusted Roles using a username and password to authenticate shall configure accounts to include but not be limited to: • For accounts accessible only within Secure Zones: ○ Passwords have at least twelve (12) characters for accounts not publicly accessible • For accounts accessible from outside a Secure Zone: ○ Passwords to have at least eight (8) characters, be changed at least every three months, use a combination of at least numeric and alphabetic characters, not be one of the user’s previous four passwords; and implement account lockout for failed access attempts; OR ○ Implement a documented password management and account lockout policy that the RA has determined provide at least the same amount of protection against password guessing as the foregoing controls. (See network security 2.g)
5.6.8	The RA maintains controls to provide reasonable assurance that Trusted Roles log out of or lock workstations when no longer in use. (See network security 2.h)
5.6.9	The RA maintains controls to provide reasonable assurance that workstations are configured with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user. (See network security 2.i)
5.6.10	The RA maintains controls to provide reasonable assurance that it reviews all system accounts at least every three months and deactivates any accounts that are no longer necessary for operations. (See network security 2.j)

#	Criterion
5.6.11	The RA maintains controls to provide reasonable assurance that it revokes account access to Certificate Systems after no more than five (5) failed access attempts, provided that this security measure is supported by the Certificate system and does not weaken the security of this authentication control. (See network security 2.k)
5.6.12	The RA maintains controls to provide reasonable assurance that it disables all privileged access of an individual to Certificate Systems within 24 hours upon termination of the individual's employment or contracting relationship with the RA. (See network security 2.l)
5.6.13	The RA maintains controls to provide reasonable assurance that it enforces multi-factor authentication for administrator access to Certificate Systems. (See network security 2.m)
5.6.14	The RA maintains controls to provide reasonable assurance that it restricts remote administration or access to a Certificate System, or Security Support System except when: ● The remote connection originates from a device owned or controlled by the RA, and from a pre-approved external IP address; ● The remote connection is through a temporary, non-persistent encrypted channel that is supported by multi-factor authentication; and ● The remote connection is made to a designated intermediary device meeting the following: ○ Located within the RA's network; ○ Secured in accordance with the Network and Certificate System Security Requirements; and ○ Mediates the remote connection to the Issuing System. (See network security 2.o)

LOGGING, MONITORING, AND ALERTING

#	Criterion
5.7.1	The RA maintains controls to provide reasonable assurance that Security Support Systems under the control of RA or Delegated Third Party Trusted Roles are implemented to monitor, detect, and report any security-related configuration change to Certificate Systems. (See network security 3.a)
5.7.2	The RA maintains controls to provide reasonable assurance that Certificate Systems under the control of RA capable of monitoring and logging system activity are configured to continuously monitor and log system activity. (See network security 3.b)
5.7.3	The RA maintains controls to provide reasonable assurance that Automated mechanisms under the control of RA or Delegated Third Party Trusted Roles are configured to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events. (See network security 3.c)
5.7.4	The RA maintains controls to provide reasonable assurance that Trusted Role personnel follows up on alerts of possible Critical Security Events. (See network security 3.d)
5.7.5	The RA maintains controls to provide reasonable assurance that a human review of application and system logs is performed at least monthly and includes:

#	Criterion
	• Validating the integrity of logging processes; and • Testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly. (See network security 3.e)
5.7.6	The RA maintains controls to provide reasonable assurance that it maintains, archives, and retains logs in accordance with its disclosed business practices. (See network security 3.f)

VULNERABILITY DETECTION AND PATCH MANAGEMENT

#	Criterion
5.8.1	The RA maintains controls to provide reasonable assurance that detection and prevention controls under the control of RA or Delegated Third Party Trusted Roles are implemented to protect Certificate Systems against viruses and malicious software. (See network security 4.a)
5.8.2	The RA maintains controls to provide reasonable assurance that a formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities. (See network security 4.b)
5.8.3	The RA maintains controls to provide reasonable assurance that a Vulnerability Scan is performed on public and private IP addresses identified by the RA or Delegated Third Party as the RA's or Delegated Third Party's Certificate Systems based on the following: • Within one week of receiving a request from the CA/Browser Forum; • After any system or network changes that the RA determines are significant; and • At least once per quarter (See network security 4.c)
5.8.4	The RA maintains controls to provide reasonable assurance that a Penetration Test is performed on the RA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the RA determines are significant. (See network security 4.d)
5.8.5	The RA maintains controls to provide reasonable assurance that it documents that Vulnerability Scans and Penetrations Tests were performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test. (See network security 4.e)
5.8.6	The RA maintains controls to provide reasonable assurance that it performs one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the RA's vulnerability correction process: • Remediate the Critical Vulnerability; • If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: ○ Vulnerabilities with high CVSS scores, starting with the vulnerabilities the RA determines are the most critical (such as those with a CVSS score of 10.0); and

#	Criterion
	○ Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; OR ● Document the factual basis for the RA's determination that the vulnerability does not require remediation because of one of the following: ○ The RA disagrees with the NVD rating; ○ The identification is a false positive; ○ The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or ○ Other similar reasons. (See network security 4.f)

6.0 RA Additional EV Controls (where applicable)

6.1 RA Extended Validation SSL Business Practices Disclosure

The Registration Authority

- discloses its Extended Validation (EV) SSL Certificate practices and procedures (meaning, the identification and authentication process related to binding the individual subscriber to the certificate) in reference to the relevant provisions of the CA's EV business practices disclosures in the CA's Certification Practice Statement; and
- discloses its EV Business Practices in compliance with the relevant provisions of the CA's business practices disclosures in the CA's Certificate Policy (if applicable).
- Where applicable, discloses any additional business practices that it undertakes that are not contained in the CA's business practice disclosure that are relevant activities performed on behalf of the CA.

#	**RA's Business Practices:**
6.1.1	The RA discloses, for each CA that it provides EV registration services for, • a summary of the services performed; • direct references to the relevant sections of the CA's CPS addressing the control requirements for the services it performs • a link to the publicly available CPS for CA in scope for the RA.
6.1.2	Where applicable, for each CA that it provides EV registration services for, • direct references to the relevant sections of the CA's CP addressing the control requirements for the services it performs • a link to the publicly available CP for CA in scope for the RA..

#	**Additional Business Practices**
6.1.3	Where applicable, for each CA that it provides EV registration services for, • discloses any business practices that are not contained in the RA's business practice disclosure that are relevant activities performed on behalf of the CA in a publicly available document.

6.2 RA Extended Validation SSL Service Integrity

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

- EV SSL subscriber information was properly collected, authenticated (for the registration activities performed by the Registration Authority (RA)) and verified.

There are a number of verification and personnel requirements that are set out for EV certificates. Where the RA undertakes the verification activities on behalf of the RA, these requirements need to be met by the external RA.

#	Criterion
6.2	When acting on behalf of a CA in performing RA verification procedures, the RA performs the procedures contracted with the CA to meet the verification requirements set out by the CA/Browser Forum

#	Illustrative Controls:
6.2.1	A contract exists setting out the verification procedures that are to be undertaken by the RA for EV.
6.2.2	The RA maintains controls to provide reasonable assurance that the information provided by the Applicant is verified directly by performing the steps established by the EV SSL Guidelines in sections 11.1, 11.2, 11.3, 11.12.3.
6.2.3	The RA maintains controls to provide reasonable assurance that it verifies the physical address provided by Applicant is an address where Applicant or a Parent /Subsidiary company conducts business operations (e.g., not a mail drop or P.O. box, or 'care of' C/O address, such as an address of an agent of the Organization), and is the address of Applicant's Place of Business using a method of verification established by the EV SSL Guidelines in section 11.4.1.
6.2.4	The RA maintains controls to provide reasonable assurance that it verifies a telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant by performing the steps set out in the EV SSL Guidelines in section 11.5.1.
6.2.5	The RA maintains controls to provide reasonable assurance that it verifies the Applicant has the ability to engage in business by verifying the Applicant's, or Affiliate/Parent/Subsidiary Company's, operational existence by performing the steps set out in the EV SSL Guidelines in section 11.6.
6.2.6	The RA maintains controls to provide reasonable assurance that for each Fully-Qualified Domain Name listed in a Certificate, other than a Domain Name with .onion in the rightmost label of the Domain Name, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company, or Affiliate, collectively referred to as "Applicant") either is the Domain Name Registrant or has control over the FQDN by using the guidance out in the EV SSL Guidelines in section 11.7.1.
6.2.7	The RA maintains controls to provide reasonable assurance that for a Certificate issued to a Domain Name with .onion in the right-most label of the Domain Name, the RA confirms that, as of the date the Certificate was issued, the Applicant's control over the .onion Domain Name in accordance with Appendix F of the EV SSL Guidelines.
6.2.8	The RA maintains controls to provide reasonable assurance that it identifies "High Risk Applicants" and undertakes additional precautions as are reasonably necessary to ensure that such Applicants are properly verified using a verification method below: • the RA may identify high risk requests by checking appropriate lists of organization names that are most commonly targeted in phishing and other fraudulent schemes, and by automatically flagging certificate requests that match these lists for further scrutiny before issuance; and • the RA shall use information identified by the relevant RA's high-risk criteria to flag suspicious certificate requests. The RA shall follow a documented procedure for performing additional verification of any certificate request flagged as suspicious or high risk. See EV SSL Guidelines 11.12.1

#	Illustrative Controls:
6.2.9	The RA maintains controls to provide reasonable assurance that provides verification for Contract Signer and Approver, using a method of verification established by the EV SSL Guidelines by performing the steps set out in the EV SSL Guidelines in section 11.8.
6.2.10	The RA maintains controls to provide reasonable assurance, using a method of verification established in the EV SSL Guidelines that: • subscriber Agreements are signed by an authorized Contract signer; • the EV SSL Certificate Request is signed by the Certificate Requester submitting the document; • if the Certificate requester is not also an authorized Certificate Approver, an authorized Certificate Approver independently approves the EV SSL Certificate Request unless pre-authorized; and • signatures have been properly authenticated. See EV SSL Guidelines Sections 11.9 and 11.10.
6.2.11	The RA maintains controls to provide reasonable assurance that it verifies information sources prior to placing reliance on them using a verification procedure set out in the EV SSL Guidelines. The verification includes legal opinions, accountants' letters, face-to-face vetting documents, independent confirmation from applicant, Qualified Independent Information Sources (QIIS), Qualified Government Information Sources (QGIS), and Qualified Government Tax Information Source (QGTIS). See EV SSL Guidelines sections 11.11, 11.11.5, 11.11.6, 11.11.7, 11.14.
6.2.12	For existing subscribers, the RA maintains controls to provide reasonable assurance that in conjunction with an EV SSL Certificate Request placed by an Applicant who is already a customer of the RA, the RA performs all authentication and verification tasks required by the Guidelines to ensure that the request is properly authorized by the Applicant and that the information in the EV SSL Certificate will still be accurate and valid, subject to any exceptions as outlined in Section 11.14.1 and re-issuance requests in Section 11.14.2. See EV SSL Guidelines sections 11.14, 11.14.1, 11.14.2

#	Criterion
6.3	When acting on behalf of a CA in performing RA verification procedures, the RA maintains proper segregation of duties and ensures its employees are properly screened and trained.

#	Illustrative Controls:
6.3.1	The RA maintains controls to provide reasonable assurance that ensure the system used to process and approve EV SSL Certificate Requests requires actions by at least two trusted persons before the EV SSL Certificate is created. See EV SSL Guidelines section 16.
6.3.2	The RA maintains controls to provide reasonable assurance that with respect to employees, agents, or independent contractors engaged in the EV process, the RA: • verifies the identity of each person; • performs background checks of such person to confirm employment, checks personal references, confirms the highest or most relevant educational degree obtained and searches criminal records where allowed in the jurisdiction where the person will be employed; and

#	**Illustrative Controls:**
	• for employees at the time of the adoption of the EV SSL Guidelines by the RA (or contracting the RA), verifies the identity and perform background checks within three months of the date of the adoption of the EV SSL Guidelines. See EV SSL Guidelines section 14.1.1.
6.3.3	The RA maintains controls to provide reasonable assurance that: • the RA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the RA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements; • the RA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily; • the RA documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task; • the RA requires all Validation Specialists to pass an examination provided by the RA on the information verification requirements outlined in the Baseline Requirements; and • all personnel in Trusted Roles maintain skill levels consistent with the relevant RA's training and performance programs. See EV SSL Guidelines section 14.1.2.

7.0 RA Additional EV Code Signing Controls (where applicable)

7.1 RA Extended Validation Code Signing Business Practices Disclosure

The Registration Authority discloses:

- Extended Validation (EV) Code Signing (CS) Certificate practices and procedures and its commitment to provide EV CS Certificates in conformity with the relevant provisions of the CA's EV business practices disclosures in the CA's Certification Practice Statement.
- Where applicable, discloses any additional business practices that it undertakes that are not contained in the CA's business practice disclosure that are relevant activities performed on behalf of the CA.

#	**RA's Business Practices:**
7.1.1	The RA discloses, for each CA that it provides EV Code Signing registration services for, • a summary of the services performed; • direct references to the relevant sections of the CA's CPS addressing the control requirements for the services it performs • a link to the publicly available CPS for CA in scope for the RA.
7.1.2	Where applicable, for each CA that it provides EV Code Signing registration services for, • direct references to the relevant sections of the CA's CP addressing the control requirements for the services it performs • a link to the publicly available CP for CA in scope for the RA

#	**Additional Business Practices**
7.1.3	Where applicable, for each CA that it provides EV registration services for, • discloses any business practices that are not contained in the CA's business practice disclosure that are relevant activities performed on behalf of the CA in a publicly available document.

7.2 RA Extended Validation Code Signing Service Integrity

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

- EV SSL subscriber information was properly collected, authenticated (for the registration activities performed by the Registration Authority (RA)) and verified.

There are a number of verification and personnel requirements that are set out for EV certificates. Where the RA undertakes the verification activities on behalf of the CA, these requirements need to be met by the external RA.

#	Criterion
7.2	When acting on behalf of a CA in performing RA verification procedures, the RA performs the procedures contracted with the CA to meet the verification requirements set out by the CA/Browser Forum

#	Illustrative Controls:
7.2.1	A contract exists setting out the verification procedures that are to be undertaken by the RA for EV.
7.2.2	The RA maintains controls to provide reasonable assurance that the information provided by the Applicant is verified directly by performing the steps established by the EV CS Guidelines in sections 11.1, 11.2, 11.3, 11.11.
7.2.3	The RA maintains controls to provide reasonable assurance that it verifies the physical address provided by Applicant is an address where Applicant or a Parent /Subsidiary company conducts business operations (e.g., not a mail drop or P.O. box, or 'care of' C/O address, such as an address of an agent of the Organization), and is the address of Applicant's Place of Business using a method of verification established by the EV CS Guidelines.
7.2.4	The RA maintains controls to provide reasonable assurance that it verifies a telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant by performing the steps set out in the EV CS Guidelines.
7.2.5	The RA maintains controls to provide reasonable assurance that it verifies the Applicant has the ability to engage in business by verifying the Applicant's, or Affiliate/Parent/Subsidiary Company's, operational existence by: • verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years, as indicated by the records of an Incorporating Agency or Registration Agency; • verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company is listed in either a current QIIS or QTIS; • verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's, Affiliate's, Parent Company's, or Subsidiary Company's Demand Deposit Account directly from a Regulated Financial Institution; or • relying on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.
7.2.6	The RA maintains controls to provide reasonable assurance that it identifies "High Risk Applicants" and undertakes additional precautions as are reasonably necessary to ensure that such Applicants are properly verified using a verification method below: • the CA may identify high risk requests by checking appropriate lists of organization names that are most commonly targeted in phishing and other fraudulent schemes, and by automatically flagging certificate requests that match these lists for further scrutiny before issuance • the RA shall use information identified by the CA's high-risk criteria to flag suspicious certificate requests. The RA shall follow a documented procedure for performing additional verification of any certificate request flagged as suspicious or high risk.

#	Illustrative Controls:
7.2.7	The RA maintains controls to provide reasonable assurance that provides verification for Contract Signer and Approver, using a method of verification established by the EV CS Guidelines by performing the steps set out in the EV CS Guidelines in section 11.7
7.2.8	The RA maintains controls to provide reasonable assurance, using a method of verification established in the EV SSL Guidelines that: • subscriber Agreements are signed by an authorized Contract signer; • the EV SSL Certificate Request is signed by the Certificate Requester submitting the document; • if the Certificate requester is not also an authorized Certificate Approver, an authorized Certificate Approver independently approves the EV CS Certificate Request unless pre-authorized; and • signatures have been properly authenticated. See EV CS Guidelines Sections 11.8 and 11.9
7.2.9	The RA maintains controls to provide reasonable assurance that it verifies information sources prior to placing reliance on them using a verification procedure set out in the EV CS Guidelines. The verification includes legal opinions, accountants' letters, face-to-face vetting documents, independent confirmation from applicant, Qualified Independent Information Sources (QIIS), Qualified Government Information Sources (QGIS), and Qualified Government Tax Information Source (QGTIS). See EV CS Guidelines sections 11.10, 11.13
7.2.10	For existing subscribers, the RA maintains controls to provide reasonable assurance that in conjunction with an EV CS Certificate Request placed by an Applicant who is already a customer of the CA, the RA performs all authentication and verification tasks required by these Guidelines to ensure that the request is properly authorized by the Applicant and that the information in the EV CS Certificate will still be accurate and valid, subject to any exceptions as outlined in EV SSL Guidelines Section 11.14.1 and re-issuance requests in EV SSL Guidelines Section 11.14.2.See EV CS Guidelines sections 11.13

#	Criterion
7.3	When acting on behalf of a CA in performing RA verification procedures, the RA maintains proper segregation of duties and ensures its employees are properly screened and trained.

#	Illustrative Controls:
7.3.1	The RA maintains controls to provide reasonable assurance that ensure the system used to process and approve EV CS Certificate Requests requires actions by at least two trusted persons before the EV CS Certificate is created. See EV CS Guidelines section 16.
7.3.2	The RA maintains controls to provide reasonable assurance that with respect to employees, agents, or independent contractors engaged in the EV process, the RA: • verifies the identity of each person; • performs background checks of such person to confirm employment, checks personal references, confirms the highest or most relevant educational degree obtained and searches criminal records where allowed in the jurisdiction where the person will be employed; and

#	Illustrative Controls:
	• for employees at the time of the adoption of the EV SSL Guidelines by the RA (or contracting the RA), verifies the identity and perform background checks within three months of the date of the adoption of the EV SSL Guidelines. See EV CS Guidelines section 14.1.
7.3.3	The RA maintains controls to provide reasonable assurance that: • the RA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the RA’s Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements; • the RA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily; • the RA documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task; • the RA requires all Validation Specialists to pass an examination provided by the RA on the information verification requirements outlined in the Baseline Requirements; and • all personnel in Trusted Roles maintain skill levels consistent with the relevant RA’s training and performance programs. See EV SSL Guidelines section 14.1.