Network and Certificate System Security Requirements

Version 2.2

27 September, 2024

Table of Contents

Introduction 2
Overview 2
Document History 2
Definitions 3
Requirements 5
1. CA Infrastructure and Network Equipment Configuration 6
1.1 Network Segmentation 6
1.2 CA Infrastructure Security 6
1.3 Change Management 7
2. Access Control 7
2.1 Trusted roles 7
2.2 Access Management 8
3. Monitoring, Logging, Auditing, and Incident Response 9
3.1 Monitoring and Logging 9
3.2 Audit Log Processing and Alerting 10
4. Vulnerability Management 11
4.1 Inventory of Certificate Systems 11
4.2 Intrusion Detection and Prevention 11
4.3 Vulnerability Management Lifecycle 12
4.4 Vulnerability Management Timeframe 12

Introduction

Overview

Scope and Applicability:

In these Requirements, the CA is responsible for all tasks performed by Delegated Third Parties and Trusted Roles, and the CA SHALL define, document, and disclose to its auditors:

a. the tasks assigned to Delegated Third Parties or Trusted Roles;
b. the arrangements made with Delegated Third Parties to ensure compliance with these Requirements; and
c. the relevant practices, procedures, and/or systems implemented by Delegated Third Parties.

Guiding Principle and Goal:

CAs are expected to maintain a very high level of security for their infrastructure and systems because the certificates they issue play a vital role in the security of the internet, email, and software distribution.

Desired Outcomes:

The following are outcomes that this document seeks to achieve:

- CAs are able to clearly understand the minimum security requirements found in this document and successfully adapt/implement these Requirements to their own infrastructure and architecture.
- Audit and assessment bodies are able to accurately map these Requirements to the specific implementations observed during audit engagements, and judge compliance against these Requirements.
- CA organizations, operations, infrastructure, and CA Private Keys and certificates are not compromised.
- Controls are implemented that protect against external and internal threats, including mistakes.
- Through a combination of credentialing, role management, and training, CA personnel are limited in their ability to negatively impact the CA's operations, whether intentionally or unintentionally.
- Systems provide sufficient artifacts to enable traceability of all events and identification and investigation of anomalous events.
- Continuous monitoring and testing are conducted to identify any vulnerabilities or weaknesses that need to be addressed promptly and to ensure the effectiveness of implemented security controls.
- CA Infrastructure is maintained, including timely patching of software and firmware, and hardware is kept sufficiently up to date to support software and systems running on it.
- A framework is provided for assessment of infrastructure and systems not directly owned or controlled by the CA.
- The use of infrastructure or systems not owned or controlled by the CA is possible, if such use aligns with these Requirements and all other applicable standards, policies, or requirements.

Document History

Ver.	Ballot	Description	Adopted	Effective*
1.0	83	Original Version Adopted	3-Aug-12	01-Jan-13
1.1	210	Misc. Changes to NCSSRs	31-Aug-17	09-Mar-18
1.2	SC3	Two-Factor Authentication and Password Improvements	16-Aug-18	15-Sep-18
1.3	SC21	The Network and Certificate Systems Security Requirements Section 3 (Log Integrity Controls)	26-Sep-19	4-Nov-2019
1.4	SC29	System Configuration Management	7-May-20	8-Jun-2020
1.5	SC28	Logging and Log Retention	10-Sep-2020	19-Sep-2020
1.6	SC39	Definition of Critical Vulnerability	16-Feb-2021	30-Mar-2021
1.7	SC41	Reformatting the BRs, EVGs, and NCSSRs	24-Feb-2021	5-Apr-2021
2.0	NS-003	Restructure NCSSRs	06-May-2024	05-Jun-2024

* Effective Date based on completion of 30-day IPR review without filing of any Exclusion Notices.

Definitions

Air-Gapped: Physically and logically separated, disconnected, and isolated from all other Systems.

CA Infrastructure: Collectively the infrastructure used by the CA or Delegated Third Party which qualifies as a:

- Certificate Management System;
- Certificate System;
- Delegated Third Party System;
- Issuing System;
- Root CA System (Air-Gapped and otherwise); or
- Security Support System.

Certificate Management System: A system used by a CA or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.

Certificate System: A system used by a CA or Delegated Third Party to access, process, or manage data or provide services related to performing:

1. identity validation;
2. identity authentication;
3. account registration;
4. certificate application;
5. certificate approval;
6. certificate issuance;
7. certificate revocation;
8. generation and signing of authoritative certificate status; or
9. key escrow.

Critical Security Event: An event, set of circumstances, or anomalous activity that could lead to a circumvention of CA Infrastructure security controls or compromise of CA Infrastructure integrity or operational continuity, including, but not limited to, excessive login attempts, attempts to

access prohibited resources, DoS/DDoS attacks, attacker reconnaissance, excessive traffic at unusual hours, signs of unauthorized access, system intrusion, or physical compromise of component integrity.

Delegated Third Party: A natural person or legal entity that is not the CA and that operates any part of a Certificate System.

Delegated Third Party System: Any part of a Certificate System used by a Delegated Third Party while performing the functions delegated to it by the CA.

Issuing System: A system used to sign certificates or validity status information.

Key Pair: The Private Key and its associated Public Key.

Multi-Factor Authentication: An authentication mechanism consisting of two or more of the following independent categories of credentials (i.e. factors) to verify the user's identity for a login or other transaction:

1. something the user knows (knowledge factor);
2. something the user has (possession factor); and
3. something the user is (inherence factor).

Each factor is independent of the other(s).

Multi-Party Control: An access control mechanism which requires two or more separate, authorized users to successfully authenticate with their own unique credentials prior to access being granted.

Network Equipment: Hardware devices and other components that facilitate communication and data transfer within the CA Infrastructure.

Physically Secure Environment: A controlled and protected physical space consisting minimally of a physical environment which is:

1. protected by security controls which address the topics outlined in section 4.5.1 of RFC 3647; and
2. designed, built, and maintained in accordance with Risk Assessments conducted by the CA.

Principle of Least Privilege: The principle that users, devices, and software should only have the minimum necessary access and privileges to complete their functions.

Private Key: The cryptographic key of an asymmetric Key Pair that is kept secret by the holder of the Key Pair. It may be used to create digital signatures and/or to decrypt data that were encrypted by the corresponding Public Key.

Public Key: The cryptographic key of an asymmetric Key Pair that can be made public without compromising the security of the Key Pair. It may be used to verify digital signatures and/or to encrypt data that can be decrypted by the corresponding Private Key.

Requirements: The Network and Certificate System Security Requirements found in this document.

Risk Assessment: A formal process that:

1. Identifies and documents foreseeable internal and external threats to the CA Infrastucture that could result in:
    - unauthorized access to the CA Infrastructure;

    - disclosure of data stored in the CA Infrastructure;
    - misuse of the CA Infrastructure; or
    - unapproved alteration or destruction of any part of the CA Infrastructure;
2. Assesses and documents the likelihood and potential damage of each identified threat, taking into consideration minimally the sensitivity and criticality of the CA Infrastructure; and
3. Assesses and documents the sufficiency of the policies, procedures, controls, information systems, technology, and other arrangements that the CA has in place to counter each identified threat.

Root CA Certificate: A self-signed and self-issued certificate where:

1. the issuer and subject of the certificate are the same; and
2. the digital signature of the certificate is:
    - generated using the Private Key of a Key Pair whose corresponding Public Key is bound to the certificate; and
    - verified using the Public Key contained in the certificate.

Root CA Private Key: The Private Key associated with a Root CA Certificate.

Root CA System: A system used to:

1. generate a Key Pair whose Private Key is or will be a Root CA Private Key;
2. store a Root CA Private Key; or
3. create digital signatures using a Root CA Private Key.

Security Support System: A system or set of systems supporting the security of the CA Infrastructure, which minimally includes:

1. authentication;
2. network boundary control;
3. audit logging;
4. audit log reduction and analysis;
5. vulnerability scanning;
6. physical intrusion detection;
7. host-based intrusion detection; and
8. network-based intrusion detection.

System: One or more pieces of equipment or software that stores, transforms, or communicates data.

Trusted Role: An employee or contractor of a CA or Delegated Third Party who has authorized access to any component of CA Infrastructure.

Workstation: A device, such as a phone, tablet, or desktop or laptop computer, which is:

1. connected to the same network as CA Infrastructure and/or Network Equipment; and
2. capable of accessing CA Infrastructure and/or Network Equipment.

Requirements

Prior to 2025-03-12, the CA SHALL adhere to these Requirements or Version 1.7 of the Network and Certificate System Security Requirements. Effective 2025-03-12, the CA SHALL adhere to these Requirements.

1. CA Infrastructure and Network Equipment Configuration

1.1 Network Segmentation

1.1.1

CA Infrastructure MUST be segmented into separate networks based on the functional and/or logical relationships of CA Infrastructure components.

1.1.1.1

Network segmentation MUST be designed and implemented using Network Equipment, such as:

- firewalls
- network switches
- physically separate networks

Network segmentation MAY leverage software, such as:

- virtual LANs (VLANs) and VLAN access control lists
- software-defined networking
- virtual private networks (VPNs)

1.1.1.2

Network segmentation SHOULD be designed and implemented in a manner that:

1. minimizes attack surfaces;
2. limits lateral movement within networks;
3. restricts traffic flow between different network segments; and
4. protects all CA Infrastructure components from unauthorized access.

1.2 CA Infrastructure Security

1.2.1

CA Infrastructure MUST be in a Physically Secure Environment.

1.2.2

Connections to and within the CA Infrastructure MUST be authenticated and encrypted except OCSP and CRL.

CA Infrastructure and Network Equipment MUST be implemented and configured in a manner that minimizes unnecessary active components and capabilities such that:

1. all connections, communications, applications, services, protocols, and ports not used are removed and/or disabled; and
2. only connections, communications, applications, services, protocols, and ports necessary and approved under the Principle of Least Privilege are enabled.

1.2.3

Equivalent security MUST be implemented on all Systems on the same network as any CA Infrastructure component.

1.3 Change Management

The CA MUST establish and maintain a change management process which is minimally:

1. documented comprehensively;
2. authoritative for:
    1. all personnel in Trusted Roles;
    2. management of Network Equipment; and
    3. management of CA Infrastructure;
3. reviewed annually;
4. updated as needed; and
5. approved:
    - with each update;
    - prior to going into effect; and
    - by personnel in applicable Trusted Roles.

The CA MUST ensure the change management process:

1. enables identification, documentation, and remediation of risks associated with introducing, modifying, or removing:
    - Trusted Role definitions;
    - Trusted Role appointments;
    - Network Equipment; or
    - CA Infrastructure;
2. addresses managing exceptions and responding to emergencies; and
3. incorporates procedures for change reversal where applicable.

The CA MUST ensure that all changes are completed in accordance with such a change management process for:

1. Trusted Role definitions;
2. Trusted Role appointments;
3. Network Equipment; and
4. CA Infrastructure.

2. Access Control

Within this Section 2, references to “access” include all physical and logical access, unless otherwise specified.

2.1 Trusted roles

The CA MUST define Trusted Roles for the personnel who design, build, develop, implement, operate, and maintain its CA Infrastructure and Network Equipment.

Each Trusted Role MUST have its responsibilities, privileges, and access documented.

Each Trusted Role MUST be assigned responsibilities, privileges, and access in a manner consistent with:

1. the Principle of Least Privilege; and
2. requirements of Multi-Party Control.

2.1.1

The CA MUST ensure personnel assigned to a Trusted Role act only within the scope of their Trusted Role(s) when performing responsibilities, using privileges, or using access assigned to that Trusted Role.

2.2 Access Management

2.2.1

The CA MUST ensure access to CA Infrastructure and/or Network Equipment is:

1. limited to personnel assigned to applicable Trusted Roles; and
2. based on the Principle of Least Privilege.

2.2.1.1

The CA MUST ensure personnel assigned to Trusted Roles that are authorized to access or authenticate to CA Infrastructure and/or Network Equipment use unique authentication credentials created by or assigned to the authorized individual.

2.2.1.2

The CA SHOULD NOT allow group accounts or shared role credentials to authenticate to or access CA Infrastructure and/or Network Equipment. If group accounts or shared role credentials are used, the CA MUST be able to attribute each use to * an approved activity; and * an individual user or service account.

2.2.1.3

The CA MUST ensure authentication credentials are changed or revoked when associated authorizations are changed or revoked.

The CA MUST ensure access to CA Infrastructure and Network Equipment is disabled for personnel within twenty-four (24) hours of the termination of an individual's employment or contracting relationship.

2.2.1.4

The CA MUST ensure any account capable of authenticating to or accessing CA Infrastructure or Network Equipment is reviewed at a minimum frequency of every three (3) months.

The CA MUST ensure any account that is not necessary for the operation of CA Infrastructure or Network Equipment is deactivated or removed such that the account is no longer capable of authenticating to or accessing CA Infrastructure or Network Equipment.

2.2.1.5

The CA MUST ensure security measures are implemented that minimize the susceptibility of CA Infrastructure to unauthorized access through repeated attempts to authenticate to or access an account that has access to CA Infrastructure. These measures SHOULD prevent brute-force attacks which systematically enumerate authentication credentials such as username and password combinations. These measures SHOULD be based on a Risk Assessment.

2.2.2

The CA MUST ensure Workstations are configured in a manner that prevents continued access to the Workstation after a set period of inactivity, for example by automatically logging off active

users. The allowed and configured duration of inactivity MUST be selected based on the CA's assessment of associated risks.

2.2.3

The CA MUST enforce the use of Multi-Factor Authentication for:

1. accounts on CA Infrastructure; and
2. access to CA Infrastructure.

Authentication based on the possession of a cryptographic key can be used as part of Multi-factor Authentication only if that key is stored in a key storage device that is designed to prevent extraction.

2.2.4

The CA MUST enforce the use of Multi-Party Control for physical access to any Root CA System.

2.2.5

The CA SHOULD ensure passwords used as authentication credentials for accounts on CA Infrastructure, Network Equipment, or Workstations are generated and managed in accordance with NIST 800-63B Revision 3 Appendix A. Access to shared credentials MUST:

- be limited to personnel based on the Principle of Least Privilege; and
- comply with section 2.2.1.2.

2.2.6

The CA MUST ensure any remote connection that enables administration of and/or access to CA Infrastructure:

1. originates from a Workstation owned and/or controlled by the CA;
2. is made through a temporary, non-persistent, and encrypted channel;
3. is authenticated using Multi-Factor Authentication; and
4. is made to a Network Equipment asset which:
    - is located within the CA's network;
    - is secured in accordance with these Requirements; and
    - mediates the remote connection to the CA Infrastructure.

3. Monitoring, Logging, Auditing, and Incident Response

3.1 Monitoring and Logging

3.1.1

The CA MUST identify and document the monitoring and logging capabilities of CA Infrastructure and Network Equipment.

The CA SHOULD establish, evaluate, and maintain policies and procedures for:

1. identifying and utilizing the monitoring and logging capabilities of CA Infrastructure and Network Equipment; and
2. retaining, parsing, securing, and archiving the audit logs output by CA Infrastructure and Network Equipment.

The CA SHOULD review and update such policies and procedures at least annually.

3.1.1.1

The CA MUST ensure the monitoring and logging capabilities of CA Infrastructure and Network Equipment are enabled to the extent necessary to meet:

1. these Requirements; and
2. applicable obligations that depend on such audit logs (such as the requirements in Section 5.4.1 (3) of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates).

3.1.1.2

The CA MUST ensure audit logs produced by the monitoring and logging capabilities of CA Infrastructure and Network Equipment include activities and/or events:

1. necessary to detect possible:
    1. Critical Security Events; and
    2. modifications to CA Infrastructure not authorized through the change management process outlined in Section 1.3; and
2. with sufficient detail to meet
    1. these Requirements; and
    2. applicable obligations that depend on such audit logs (such as the requirements in Section 5.4.1 (3) of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates).

3.1.2

The CA MUST ensure the integrity of logging processes within CA Infrastructure is monitored through:

1. continuous automated monitoring operating within CA Infrastructure; or
2. a review by personnel assigned to applicable Trusted Roles at least once every 31 days.

The CA MUST ensure such integrity monitoring is configured and managed in a manner sufficiently effective to identify possible audit log compromise.

3.1.2.1

The CA MUST ensure audit logs are retained and/or archived for the amount of time necessary to meet:

1. these Requirements; and
2. applicable obligations which depend on such audit logs (such as the requirements in Section 5.4.1 (3) of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates).

The CA SHOULD ensure retained and/or archived audit logs are kept and managed in a manner sufficiently effective to prevent unapproved alteration or access.

3.2 Audit Log Processing and Alerting

3.2.1

The CA MUST ensure audit logs are processed:

1. through automated mechanisms under the control of personnel assigned to applicable Trusted Roles; and
2. in a manner sufficiently effective to minimally identify possible:
    1. Critical Security Events; and
    2. unauthorized changes to CA Infrastructure.

3.2.2

The CA MUST ensure personnel assigned to applicable Trusted Roles are alerted via multiple mechanisms and/or communication channels of identified possible:

1. audit log compromise;
2. Critical Security Events; and
3. unauthorized changes to CA Infrastructure.

3.2.3

The CA MUST ensure personnel assigned to applicable Trusted Roles commence an initial response to alerts of Section 3.2.2 within twenty-four (24) hours of the alert being generated.

3.2.3.1

The CA MUST ensure the initial response confirms whether the alert identifies a legitimate

1. audit log compromise;
2. Critical Security Event; and/or
3. unauthorized change to the CA Infrastructure.

The CA MUST ensure personnel assigned to applicable Trusted Roles create and follow an incident response plan for all legitimate alerts.

3.2.3.2

The CA SHOULD ensure incident response plans minimally include:

1. identification of the potential impact, scope, and severity of the incident;
2. containment of the incident to minimize further impact; and
3. identification and mitigation or eradication of the incident root cause(s).

4. Vulnerability Management

The CA MUST implement the policies and procedures in this Section for identifying, evaluating, and resolving security vulnerabilities.

These policies and procedures MUST apply to all Certificate Systems.

These policies and procedures SHOULD apply to Security Support Systems.

4.1 Inventory of Certificate Systems

The CA MUST define an inventory of Certificate Systems.

4.2 Intrusion Detection and Prevention

The CA MUST protect the systems in the inventory of Certificate Systems against common network and system threats using intrusion detection and prevention controls.

4.3 Vulnerability Management Lifecycle

The CA MUST document and follow a vulnerability correction process that includes:

1. identification;
2. review;
3. response; and
4. remediation.

4.3.1 Vulnerability Identification

The CA's vulnerability identification process MUST include monitoring for relevant security advisories and penetration testing.

4.3.1.1 Penetration Testing

As part of the identification component of the CA's vulnerability correction process, the CA MUST define and follow a program for performing penetration tests that ensures:

1. penetration tests are performed:
    - at least on an annual basis; and
    - after infrastructure or application changes that are organizationally defined as significant; and
2. penetration tests are performed by a person or entity (or collective group thereof) with the requisite skills, tools, proficiency, code of ethics, and independence; and
3. vulnerabilities identified during the penetration test are remediated using the vulnerability correction process in Section 4.3.

4.3.2 Vulnerability Remediation

A vulnerability is remediated when the CA has:

- fixed the vulnerability such that the vulnerability is no longer present; or
- confirmed the impact of the vulnerability and documented why the vulnerability does not impact the CA's security posture.

4.4 Vulnerability Management Timeframe

The CA MUST establish one or more timeframes for reviewing, responding to, and remediating all identified vulnerabilities.

Each timeframe MUST be established based on a risk assessment performed by the CA.

The risk assessment MUST be based on a documented security analysis. The security analysis SHOULD take into account and address the following principles:

- criticality of assets;
- maintaining confidentiality, integrity, and availability of assets;
- regulatory requirements;
- likelihood and impact of exploitation;
- dependencies and interdependencies;

- remediation resource requirements;
- historical data; and
- present threat landscape.

The CA MUST ensure vulnerabilities are reviewed, responded to, and remediated in accordance with their established timeframe(s).

The CA MUST document in Section 6.7 of their Certificate Policy and/or Certification Practices Statement each timeframe established for responding to and remediating vulnerabilities.