Southern New Hampshire University

CA Server Root Certificate Requirements Checklist (CA-1)

Andree Salvo
Southern New Hampshire University
CYB 300-14668
Instructor: Jason Keltner

Requirements

A. Identify information systems that support organizational missions/business functions

B. Identify and select the following types of information system accounts that support organizational missions/business functions: [*administrative, service*]

C. Identify authorities from each department for root certificate assignment approval

D. Secure protocols used, TLS v1.2

E. Client renegotiation disabled

F. Account notification to CA authorities:

   a. When user or system accounts are terminated
   b. When individual information system usage changes
   c. When account inactivity is for a period of 90 days

G. Authorize root certificate assignment for information systems based on:

   a. A valid access authorization
   b. Other attributes as required by the organization or associated missions/business functions

H.

- Certificates need to be revoked automatically when its no longer valid
- OCSP or CRL updates will be used to track which certificates are still trusted.
- Monitoring and logging will be in place to confirm that revocation works properly.

I.

- All certificate-related data must be encrypted using strong encryption standards like AES-256
- TLS 1.3 will be required for all communication between systems.
- Private keys must be stored in encrypted containers to prevent unauthorized access.

J.

- The IT team will set how long certificates stay valid.
- Certificates will be valid for more than 12 months.

CA-1 Root Certificate Requirements

Requirements
Support organizational missions: <*IT defined*>
Parameter CA-1(D): <*IT-defined transport layer security*>
Parameter CA-1(E): <*IT-defined client renegotiation policy*>
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
Control Origination (check all that apply): ☐ Organization ☒ IT system specific ☐ Hybrid (organization and IT system specific)

Control Overview

Part	Description
Part A	*<The IT department will be responsible for identifying and selecting the types of accounts required to support the application. Examples of account types include individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. A successful control response will need to address the specific requirements fulfilled by each account type in use.>*
Part B	*<The IT department will be responsible for select information systems, and who will have responsibilities related to the management and maintenance. A successful control response will need to discuss how information systems are defined within the organization.>*
Part C	*<The IT department will be responsible for identification of individuals responsible for CA assignment approval. A successful control response will need to identify the person responsible for CA assignments.>*
Part D	*<The IT department will be responsible for identifying the transport layer security. A successful control response will need to ensure that the proper communication security is in place.>*
Part E	*<The IT department will be responsible for verifying that the certificate renegotiation is disabled from the client machine. The certificate renegotiation will be initiated only from the server. A successful control response will need to identify that a policy is in place to be audited and maintained.>*
Part F	*<The IT department will be responsible for defining the role of an individual to be notified if any criterion [a, b, or c] is met. A successful control response will identify the individuals and procedures used to enforce those conditions.>*
Part G	*<The IT department will be responsible for the assignment of a certificate if any criterion [a or b] is met. This may include the assignment and revocation of certificates. The individual will be responsible for notifying the person responsible for the certificate authorization. A successful control response will outline the procedure and the communication needed to properly report the issue.>*
Part H	*<The IT team's job here is to make sure certificates get revoked automatically when they're no longer valid. For example, if someone leaves the company, a device is taken offline, or a cert gets compromised. This means setting up stuff like OCSP or regular CRL updates, so the system knows which certs to trust and which ones not to trust. This should all be automated through our identity system or scripts, so we're not heavily relying on someone remembering to do it manually. A good setup will also include monitor logging and checks to make sure everything's working how it's supposed to do.>*

Part I	*<The IT team needs to make sure all certificate-related data is encrypted using strong algorithms — like RSA with at least 2048-bit keys or Elliptic Curve Cryptography (ECC) with SHA-256. This includes the certificates themselves and any data being sent between systems. All of it should be encrypted using TLS 1.3 (Cloudflare, n.d.), and private keys need to be stored securely in encrypted key containers. The goal here is to make sure that if anything ever gets intercepted, it's basically useless without the right key.*
Part J	*<The IT team will handle setting and maintaining how long certificates stay valid. No certificate will be issued for more than 12 months unless the Chief Information Officer gives written approval. If we need to set a shorter validity period, a report explaining why will need to be sent to the CIO or whoever they assign.>*

Resources: Cloudflare. (n.d.). *Why use TLS 1.3?* Cloudflare Learning. https://www.cloudflare.com/learning/ssl/why-use-tls-1.3/