Southern New Hampshire University

CA Server Root Certificate Requirements Checklist (CA-1)

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. Certificate will be revoked for the following reasons

   a. Attempts to login to a restricted area of the network.
   b. User is terminated and access needs to be deleted ASAP.
   c. Three failed login attempts on a workstation.

I. Implement PKI (Public Key Infrastructure) for both symmetrical and asymmetrical encryption.

J. The validity period for certificates should range from 1 to 3 years, depending on security requirements.

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*>
Parameter CA-1(H): <*IT-defined client revocation of certificates* >
Parameter CA-1(I): <*IT-defined PKI*>
Parameter CA-1(J): <*IT-defined validity period*>

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	*< IT and System Administrators will manage automated revocation settings and manual controls. >*
Part I	*< IT is responsible for encrypting certificates and managing their validity periods using PKI. >*
Part J	*< IT sets the validity period of certificates based on the organization's policy and certificate usage.>*