Network and Certificate System Security Requirements

Network and Certificate System Security Requirements (NCSSR)

- Effective 1 January 2013
  - No amendments since passed

- Included in WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0
  - For audit periods starting on or after 1 July 2014
  - All CAs audited under WebTrust criteria should have at least one full cycle now with this criteria version

    For period 30 June 2015 to 29 June 2016 – reports were due by end of September 2016

- ETSI?

Definitions and Scope

Certificate Systems: The system used by a CA or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.

Security Support System: A system used to provide security support functions, such as authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and antivirus.

Front End/Internal Support System: A system with a public IP address, including a web server, mail server, DNS server, jump host, or authentication server

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.

Specificity variance

Restrict remote administration or access to an Issuing System, Certificate Management System, or Security Support System

except when: (i) the remote connection originates from a device owned or controlled by the CA or Delegated Third Party and from a pre-approved external IP address, (ii) the remote connection is through a temporary, non-persistent encrypted channel that is supported by multi-factor authentication, and (iii) the remote connection is made to a designated intermediary device (a) located within the CA's network, (b) secured in accordance with these Requirements, and (c) that mediates the remote connection to the Issuing System.

Exception variance

Apply recommended security patches to Certificate Systems within six months of the security patch’s availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

Implement multi-factor authentication to each component of the Certificate System that supports multi-factor authentication

Conflicting requirements

Zone: A subset of Certificate Systems created by the logical or physical partitioning of systems from other Certificate Systems.

Secure Zone: An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of Certificate Systems

1(a) Segment Certificate Systems into *networks* or zones based on their functional, logical, and physical (including location) relationship

If an authentication control used by a Trusted Role is a username and password, then, where technically feasible, implement the following controls :

i. For accounts that are not publicly accessible (accessible only within Secure Zones or High Security Zones), require that passwords have at least twelve (12) characters;

ii. For accounts that are accessible from outside a Secure Zone or High Security Zone, require that passwords have at least eight (8) characters, be changed at least every 90 days, use a combination of at least numeric and alphabetic characters, that are not a dictionary word or on a list of previously disclosed human-generated passwords, and not be one of the user's previous four passwords; and implement account lockout for failed access attempts in accordance with subsection k; OR

iii. Implement a documented password management and account lockout policy that the CA has determined provide at least the same amount of protection against password guessing as the foregoing controls.