NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS

Scope and Applicability: These Network and Certificate System Security Requirements (Requirements) apply to all publicly trusted Certification Authorities (CAs) and are adopted with the intent that all such CAs and Delegated Third Parties be audited for conformity with these Requirements as soon as they have been incorporated as mandatory requirements (if not already mandatory requirements) in the root embedding program for any major Internet browsing client and that they be incorporated into the WebTrust Service Principles and Criteria for Certification Authorities, ETSI TS 101 456, ~~and~~ ETSI TS 102 042 and ETSI EN 319 411-1, ~~-~~including revisions and implementations thereof, including any audit scheme that purports to determine conformity therewith. 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, and (b) the arrangements made with Delegated Third parties to ensure compliance with these Requirements, and (c) the relevant practices implemented by Delegated Third Parties.

1. GENERAL PROTECTIONS FOR THE NETWORK AND SUPPORTING SYSTEMS

Each CA or Delegated Third Party SHALL:

a. Segment Certificate Systems into networks ~~or zones~~ based on their functional or ~~,~~ logical relationship, for example separate ~~and~~ physical networks or VLANs ~~(including location) relationship~~;

b. Apply ~~the same~~equivalent security controls to all systems co-located in the same ~~zone~~ network with a Certificate System;

c. Maintain Root CA Systems in a High Security Zone and in an offline state or air-gapped from all other networks;

d. Maintain and protect Issuing Systems, Certificate Management Systems, and Security Support Systems in at least a Secure Zone;

e. Implement and configure Security Support Systems that protect systems and communications between systems inside Secure Zones and High Security 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;

f. Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations;

g. Configure Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's or Delegated Third Party's operations and allowing only those that are approved by the CA or Delegated Third Party;

h. Review configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems on at least a weekly basis to determine whether any changes violated the CA's security policies;

i. Grant administration access to Certificate Systems only to persons acting in Trusted Roles and require their accountability for the Certificate System's security;

j. Implement multi-factor authentication to each component of the Certificate System that supports multi-factor authentication (but see subsection 2.n.(ii) below);

k. Change authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked; and

l. Apply recommended security patches to Certificate Systems within six (6) 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.

2. TRUSTED ROLES, DELEGATED THIRD PARTIES, AND SYSTEM ACCOUNTS

Each CA or Delegated Third Party SHALL:

a. Follow a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them;

b. Document the responsibilities and tasks assigned to Trusted Roles and implement "separation of duties" for such Trusted Roles based on the security-related concerns of the functions to be performed;

c. Ensure that only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones;

d. Ensure that an individual in a Trusted Role acts only within the scope of such role when performing administrative tasks assigned to that role;

e. Require employees and contractors to observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems;

f. Require that each individual in a Trusted Role use a unique credential created by or assigned to that person in order to authenticate to Certificate Systems;

g. 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~~three (3) months, 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 (4) 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.

h. Require Trusted Roles to log out of or lock workstations when no longer in use;

i. Configure workstations with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user (the CA or Delegated Third Party MAY allow a workstation to remain active and unattended if the workstation is otherwise secured and running administrative tasks that would be interrupted by an inactivity time-out or system lock);

j. Review all system accounts at least every three (3) months~~90 days~~ and deactivate any accounts that are no longer necessary for operations;

k. Lockout 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;

l. Implement a process that disables all privileged access of an individual to Certificate Systems within twenty-four (24) hours upon termination of the individual's employment or contracting relationship with the CA or Delegated Third Party;

m. Enforce multi-factor OR multi-party authentication for administrator access to Issuing Systems and Certificate Management Systems;

n. For each Delegated Third Party, (i) require multi-factor authentication prior to the Delegated Third Party approving issuance of a Certificate or (ii) implement technical controls that restrict the Delegated Third Party's ability to approve certificate issuance to a limited set of domain names; and

o. 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.

3. LOGGING, MONITORING, & ALERTING

Certification Authorities and Delegated Third Parties SHALL:

a. Implement a Security Support System under the control of CA or Delegated Third Party Trusted Roles that monitors, detects, and reports any security-related configuration change to Certificate Systems;

b. Identify those Certificate Systems under the control of CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity and enable those systems to continuously monitor and log system activity;

c. Implement automated mechanisms under the control of CA or Delegated Third Party Trusted Roles to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events;

d. Require Trusted Role personnel to follow up on alerts of possible Critical Security Events;

e. Conduct a human review of application and system logs at least ~~every 30 days and~~once a month to validate the integrity of logging processes and ensure that monitoring, logging, alerting, and log-integrity-verification functions are operating properly (the CA or Delegated Third Party MAY use an in-house or third-party audit log reduction and analysis tool); and

f. Maintain, archive, and retain logs in accordance with disclosed business practices and applicable legislation.

4. VULNERABILITY DETECTION AND PATCH MANAGEMENT

Certification Authorities and Delegated Third Parties SHALL:

a. Implement intrusion detection and prevention controls under the control of CA or Delegated Third Party Trusted Roles to protect Certificate Systems against common network and system threats~~viruses and malicious software~~;

b. Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities;

c. Undergo or perform a Vulnerability Scan (i) within one (1) week of receiving a request from the CA/Browser Forum, (ii) after any system or network changes that the CA determines are significant, and (iii) at least every three (3) months~~once per quarter~~, on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems;

d. Undergo a Penetration Test on the CA'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 CA determines are significant;

e. Record evidence that each Vulnerability Scan and Penetration Test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test; and

f. Do one of the following within ninety-six (96) hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process:

   i. Remediate the Critical Vulnerability;

   ii. If remediation of the Critical Vulnerability within ninety-six (96) hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to (1) vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0) and (2) 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

   iii. Document the factual basis for the CA's determination that the vulnerability does not require remediation because (a) the CA disagrees with the NVD rating, (b) the identification is a false positive, (c) the exploit of the vulnerability is prevented by compensating controls or an absence of threats; or (d) other similar reasons.

DEFINITIONS

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 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.

Common Vulnerability Scoring System (CVSS): A quantitative model used to measure the base level severity of a vulnerability (see http://nvd.nist.gov/home.cfm).

Critical Security Event: Detection of an event, a set of circumstances, or anomalous activity that could lead to a circumvention of a Zone's security controls or a compromise of a Certificate System's integrity, including 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 an actual compromise of component integrity.

Critical Vulnerability: A system vulnerability that has a CVSS score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating (see http://nvd.nist.gov/home.cfm), or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum.

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.

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.

High Security Zone: A physical location where a CA's or Delegated Third Party's Private Key or cryptographic hardware is located.

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

National Vulnerability Database (NVD): A database that includes the Common Vulnerability Scoring System (CVSS) scores of security-related software flaws, misconfigurations, and vulnerabilities associated with systems (see http://nvd.nist.gov/home.cfm).

OWASP Top Ten: A list of application vulnerabilities published by the Open Web Application Security Project (see https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

Penetration Test: A process that identifies and attempts to exploit openings and vulnerabilities on systems through the active use of known attack techniques, including the combination of different

types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.

Root CA System: A system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.

SANS Top 25: A list created with input from the SANS Institute and the Common Weakness Enumeration (CWE) that identifies the Top 25 Most Dangerous Software Errors that lead to exploitable vulnerabilities (see http://www.sans.org/top25-software-errors/).

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

Security Support System: A system used to provide security support functions, which MAY include~~such as~~ authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and intrusion detection (Host-based intrusion detection, Network-based intrusion detection)~~anti-virus~~.

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 or control over a Secure Zone or High Security Zone.

Vulnerability Scan: A process that uses manual or automated tools to probe internal and external systems to check and report on the status of operating systems, services, and devices exposed to the network and the presence of vulnerabilities listed in the NVD, OWASP Top Ten, or SANS Top 25.

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