Definitions

Air-Gapped CA System: A system that is

a. kept offline or otherwise air-gapped, b. physically and logically separated from all other CA systems, and c. is used by a CA or Delegated Third Party to store and manage CA private keys and to sign CA certificates, CRLs, or OCSP responses.

"**Kept offline or otherwise air-gapped**" means that the CA hardware is powered off, and if powered on, is not connected to any other system at any time. Export of data (e.g. CA public keys, signed CA certificates, CRLs, or OCSP responses) from an Air-Gapped CA System would only occur briefly and temporarily with the use of a non-persistent unidirectional mechanism, such as an external drive or unidirectional diode or gateway.

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/vuln-metrics/cvss).

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 v2.0 score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating (see https://nvd.nist.gov/vuln-metrics/cvss), 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.

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: something you know (knowledge factor), something you have

(possession factor), and something you are (inherence factor). Each factor must be independent. Certificate-based authentication can be used as part of Multifactor Authentication only if the private key is stored in a Secure Key Storage Device.

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/).

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 Key Storage Device: A device certified as meeting at least FIPS 140-2 level 2 overall, level 3 physical, or Common Criteria (EAL 4+).

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 physical and logical security support functions, which MAY include authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and intrusion detection (physical intrusion detection, Host-based intrusion detection, 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 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.

---

1. General Protections for the Network and Supporting Systems

Each CA or Delegated Third Party SHALL:

a. Segment Certificate Systems into networks based on their functional or logical relationship, for example separate physical networks or VLANs;

b. Apply equivalent security controls to all systems co-located in the same 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~~ as Air-Gapped CA Systems, in accordance with Section 5;

...

---

5. General Protections for Air-Gapped CA Systems

This Section 5 separates requirements for Air-Gapped CA Systems into two categories -- logical security and physical security.

5.1. Logical Security of Air-Gapped CA Systems

Certification Authorities and Delegated Third Parties SHALL implement the following controls to ensure the logical security of Air-Gapped CA Systems:

1. Review configurations of Air-Gapped CA Systems at least on an annual basis;
2. Follow a documented procedure for appointing individuals to those Trusted Roles that are authorized to operate Air-Gapped CA Systems;
3. Grant logical access to Air-Gapped CA Systems only to persons acting in Trusted Roles and implement controls so that all logical access to Air-Gapped CA Systems can be traced back to an accountable individual;
4. Document the responsibilities assigned to Trusted Roles based on the security principle of multi-person control and the security-related concerns of the functions to be performed;
5. Ensure that an individual in a Trusted Role acts only within the scope of such role when performing administrative tasks assigned to that role;
6. Require employees and contractors to observe the principle of "least privilege" when accessing, or when configuring access privileges on, Air-Gapped CA Systems;
7. Require that all access to systems and offline key material can be traced back to an individual in a Trusted Role (through a combination of recordkeeping, use of logical and physical credentials, authentication factors, video recording, etc.);
8. If an authentication control used by a Trusted Role is a username and password, then, where technically feasible require that passwords have at least twelve (12) characters;

9. Review logical access control lists at least annually and deactivate any accounts that are no longer necessary for operations;
10. Enforce Multi-Factor Authentication OR multi-party authentication for administrator access to Air-Gapped CA Systems;
11. Identify those Air-Gapped CA Systems capable of monitoring and logging system activity and enable those systems to continuously monitor and log system activity. Back up logs to an external system each time the system is used or on a quarterly basis, whichever is less frequent;
12. On a quarterly basis or each time the Air-Gapped CA System is used, whichever is less frequent, check the integrity of the logical access logging processes and ensure that logging and log-integrity functions are effective;
13. On a quarterly basis or each time the Air-Gapped CA System is used, whichever is less frequent, monitor the archival and retention of logical access logs to ensure that logs are retained for the appropriate amount of time in accordance with the disclosed business practices and applicable legislation.

5.2. Physical Security of Air-Gapped CA Systems

Certification Authorities and Delegated Third Parties SHALL implement the following controls to ensure the physical security of Air-Gapped CA Systems:

1. Grant physical access to Air-Gapped CA Systems only to persons acting in Trusted Roles and implement controls so that all physical access to Air-Gapped CA Systems can be traced back to an accountable individual;
2. Ensure that only personnel assigned to Trusted Roles have physical access to Air-Gapped CA Systems and multi-person access controls are enforced at all times;
3. Implement a process that removes physical access of an individual to all Air-Gapped CA Systems within twenty-four (24) hours upon termination of the individual's employment or contracting relationship with the CA or Delegated Third Party;
4. Implement video monitoring, intrusion detection, and intrusion prevention controls to protect Air-Gapped CA Systems against unauthorized physical access attempts;
5. Implement a Security Support System that monitors, detects, and alerts personnel to any physical access to Air-Gapped CA Systems;
6. Implement a process that prevents physical access of an individual to an Air-Gapped CA within twenty-four (24) hours of removal from the relevant authorized Trusted Role, and review lists of holders of physical keys and combinations to doors and safes as well as logical accounts tied to physical access controls at least every three (3) months, and;
7. On a quarterly basis or each time the Air-Gapped CA System is used, whichever is less frequent, monitor the archival and retention of the physical access logs to ensure that logs are retained for the appropriate amount of time in accordance with the disclosed business practices and applicable legislation.
8. On a quarterly basis or each time the Air-Gapped CA System is used, whichever is less frequent, check the integrity of the physical access logging processes and ensure that logging and log-integrity functions are effective.