NetSec Document Structuring Sub-Group

CABF F2F Update - Berlin, October 2022

DEFINITIONS

Define “Air-Gapped”

Replace “Zones”

Redefine “Certificate Systems”?

Use “more traditional PKI terms - NIST (CSRC), ETSI TR 119 001, IETF (RFC 4949) - these don’t always work

New Definitions and Glossary Working Group

1. General Protections for Network and Supporting Systems

Replace “Secure Zone” with “Physically Secure Environment”

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

1.c. (paraphrased) “Maintain Root CA Keys and associated equipment physically secured in an offline state, and when powered on, then Air-Gapped from all other networks.”

1.i. Move to Trusted Roles, subsection 2.e.

2. Trusted Roles, Delegated Third Parties, and System Accounts

Consolidate Trusted Roles here (move most of 5.1 of the draft up here to section 2.) and make it clear where, when, and how it applies to Air-Gapped Systems:

> “Define and document the responsibilities assigned to Trusted Roles, taking into account the principles of least-privilege and dual control;”
>
> “Assign tasks to Trusted Roles and follow a documented procedure for appointing authorized individuals to those Trusted Roles;”
>
> Update subsection g. Trusted Role authentication (passwords)
>
> Several others

3. Logging, Monitoring, and Alerting

Maybe revisit “**systems**” - “3.a. Implement a System under the control of CA or Delegated Third Party Trusted Roles that continuously monitors, detects, and alerts personnel to any modification to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems unless the modification has been authorized through a change management process.”

Remove cross-reference dependencies to the Baseline Requirements, e.g. in 3.b?

4. Vulnerability Detection and Patch Management

Add “Annually review system designs to determine updates that need to be made to ensure that they meet current security threats and best practices”

5. Protections for Air-Gapped CA Systems

Logical Security of Air-Gapped CA Systems

Identify those Air-Gapped CA Systems capable of logging system activity and enable those systems to continuously log system activity (and backup);

Review logging integrity and backups on a quarterly basis, or whenever used, whichever is less frequent, and determine whether there were any unauthorized procedures; …

Physical Security of Air-Gapped CA Systems

Implement a process that removes physical access of an individual to all Air-Gapped CA Systems when: (a) a person’s responsibility changes and their access is no longer necessary, or (b) within twenty-four (24) hours upon termination …;

Implement video monitoring, intrusion detection, and intrusion prevention controls to protect Air-Gapped CA Systems against unauthorized physical access attempts; …