COMMON Certificate Policy Change Proposal Number: 2018-05

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Clarify requirements for virtual implementations under the COMMON Policy
Date: July 21, 2017

Title: Requirements for virtual implementations under the COMMON Policy

X.509 Certificate Policy for the Federal PKI Common Policy Framework Version 1.28 April 4, 2018

Change Advocate's Contact Information:
Name: Jimmy Jung
Organization: The Slandala Company
Telephone number: 703 851 6813
E-mail address: jimmy.jung@slandala.com

Organization requesting change: N/A

Change summary: Update the CP to clarify the requirements in virtual machine environment (VME) implementations.

Background:

A large number of PKI systems in the Federal space are implemented in virtual environments; however, the policy has not been updated to address this change. This update is intended to clarify policy requirements as they relate to virtual implementations, primarily with regard to system auditing and what it means for the system to be dedicated to operating and supporting the CA. Note that extending security requirements for operating CAs in virtual environments does not permit CAs to be operated in cloud environments.

Specific Changes:

Insertions are underlined, deletions are in ~~strikethrough~~:

5.4 AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the CA. For CAs operated in a virtual machine environment (VME)[1], audit logs shall be generated for all applicable events on both the virtual machine (VM) and isolation kernel (i.e. hypervisor).

Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

Computer security controls are required to ensure CA/RA operations are performed as specified in this policy. The following computer security functions pertaining to the Common Policy Root CA may be provided by the operating system, or through a combination of operating system, software, and physical safeguards:

- Require authenticated logins
- Provide discretionary access control
- Provide a security audit capability
- Enforce access control for CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object reuse or require separation for CA random access memory
- Require use of cryptography for session communication and database security
- Archive CA history and audit data
- Require self-test security-related CA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanism for keys and the CA system
- Enforce domain integrity boundaries for security-critical processes.

[1] For the purposes of this policy, the definition of a virtual machine environment does not include cloud-based solutions (e.g. platform-as-a-service) or container-type solutions (e.g. Docker), which are not permitted for any CA operating under this policy.

For those portions of the Common Policy Root CA operating in a VME, the following security functions also pertain to the hypervisor:

- Require authenticated logins
- Provide discretionary access control
- Provide a security audit capability
- Enforce separation of duties for PKI roles
- Prohibit object reuse or require separation for CA random access memory
- Require use of cryptography for session communication and database security
- Archive CA history and audit data
- Require self-test security-related CA services
- Enforce domain integrity boundaries for security-critical processes.

For other CAs operating under this policy, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA and its ancillary parts shall include the following functionality (in a VME, these functions are applicable to both the VM and hypervisor):

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see section 5.4)
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

For certificate status servers operating under this policy, the computer security functions listed below are required (in a VME, these functions are applicable to both the VM and hypervisor):

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

For remote workstations used to administer the CAs, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see section 5.4)

- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

All communications between any PKI trusted role and the CA shall be authenticated and protected from modification.

6.6.1 System Development Controls

…

- The CA hardware and software, including the VME hypervisor, shall be dedicated to ~~performing one task:~~ operating and supporting the CA (i.e., the systems and services dedicated to the issuance and management of certificates). There shall be no other applications, hardware devices, network connections, or component software installed which are not part of the CA operation. Where the CA operation supports multiple CAs, the hardware platform may support multiple CAs. In a VME, a single hypervisor may support multiple CAs and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the CA.
- In a VME, all VM systems must operate in the same security zone as the CA.

…

11. Acronyms and Abbreviations

VME	Virtual Machine Environment

12. Glossary

Hypervisor	Computer software, firmware or hardware that creates and runs virtual machines. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel or virtual machine monitor.
Virtual Machine Environment	An emulation of a computer system (in this case, a CA) that provides the functionality of a physical machine in a platform-independent environment. They provide functionality needed to execute entire operating systems. At this time, allowed VMEs are limited to Hypervisor type virtual

	environments. Other technology, such as Docker Containers, is not permitted.

Estimated Cost: The change would incur the cost associated with physically securing components meeting the criteria.

Implementation Date: For organizations utilizing a VME for PKI Operations, 90 days following publication of this change in the FCPCA CP.

Prerequisites for Adoption: none

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG: October 26, 2017
Date presented to the FPKIPA: November 14, 2017
Date published: May 8, 2018