Common Certificate Policy Change Proposal Number: 2021-03

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the Common Certificate Policy
Date: October 26, 2021

Title: Remove Exclusion of Containers from Common Policy

Version and Date of Certificate Policy requested to be changed: X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.1, May 18, 2021; recommended changes have also been included for Draft Common Policy, Version 2.2 which is currently in the approval process.

Change Advocate's Contact Information:

Name: Shelley Brewer
Organization: DigiCert
Telephone number: 801-390-8224
E-mail address: shelley.brewer@digicert.com

Organization requesting change: DigiCert

Change summary:
Remove the policy exclusion for using containers or container-type technology and include higher level language to accommodate future technologies compliant with the CP.

Background:
Excluding the use of containers or container-type technology is widely accepted as an outdated requirement from the formative days of cloud technology stacks. Containers or container-type technology is currently ubiquitous in many on-prem datacenters and should not constitute a special exclusion from programs governed by this Certificate Policy. The FPKI CPWG meeting August 24, 2021 emphasized the need from the community of agencies and CAs that implementations must be compliant, but the CP could be updated to allow for higher level language to guide that evolution.

Please Note: Section 5.4 is referenced twice in this change proposal, first for the change to the current version of policy (v2.1) and second for the expected integration into the on-going draft updates to the audit and archive sections (tentatively v2.2). It is expected that the v2.2 will be relevant by the time this proposal is presented to the FPKIPA.

Specific Changes:
Insertions are underlined; deletions are in ~~strikethrough~~.

1.3.2. Certification Authorities (add the following at the end of the sub-section)

…

CA and related applications (e.g., OCSP, CMS, and KRS) may be hosted on one or more system software layers. Operational and technical security controls including audit logging requirements specified in this CP shall apply to all system software layers, where appropriate and applicable.

5.4. AUDIT LOGGING PROCEDURES (Current Version 2.1)

Audit logs ~~files~~ must be generated for all events relating to the security of the CA. For CAs, KEDs, and DDSs ~~operated in a virtual machine environment (VME)[2]~~ audit logs must be generated for all applicable events on application software and all system software layers as appropriate ~~both the virtual machine (VM) and isolation kernel (i.e.,hypervisor)~~.

~~[2] 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.~~

5.4. AUDIT LOGGING PROCEDURES (Draft Version 2.2)

At a minimum, audit records~~,~~ must be generated for all events identified in Section 5.4.1 of this policy, and must be available during audit reviews and third-party audits. For CAs operated in a virtual ~~machine~~ environment, audit records must be generated for ~~both the Virtual Machine ("VM")[2] and hypervisor~~ all applicable events on application software and all system software layers. Where possible, the audit records must be automatically collected. Where this is not possible, a logbook, paper form, other physical or electronic mechanism must be used.

~~[2] 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.~~

6.5.1 Specific Computer Security Technical Requirements

For CAs, KEDs, and DDSs 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 must include the following functionality (~~in a VME,~~ these functions are applicable to all system software layers where applicable ~~both the VM and hypervisor~~):

…

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

6.6.1 System Development Controls

…

- The CA hardware and software, including all system software layers ~~the VME hypervisor~~, must be dedicated to operating and supporting the CA (i.e., the systems

and services dedicated to the issuance and management of certificates). There must be no other applications, hardware devices, network connections, or component software installed that are not parts of the CA operation, administration, monitoring and security compliance of the system. ~~Where the CA operation supports multiple CAs, the hardware platform may support multiple CAs. In a VME, a single hypervisor~~ CA hardware and system software layers may support multiple CAs and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of ~~the~~ CAs in compliance with this CP.

- ~~If a CA operates in a VM, all VM systems in that VMS must operate in the same security zone as the CA.~~

Appendix C: Acronyms and Abbreviations

~~VM~~	~~Virtual Machine~~
~~VME~~	~~Virtual Machine Environment~~

Appendix D: Glossary

Containerization	A form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS).
System Software Layer	A layer of software that manages lower layer hardware and software resources and provides services through well-defined interfaces to the higher layers of software. Examples of system software layers are virtual machines, hypervisors, operating systems, and any containerized architectures.
~~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.~~

Delta Mapping:
It is unlikely there are specific requirements in a mapped CP/CPS that would need to change.

Estimated Cost:
There is no cost expected to implement this change.

Implementation Date:
This change will be effective immediately upon approval by the FPKIPA and incorporated into the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

Not Applicable.

Approval and Coordination Dates:

Date presented to CPWG:	9/28/2021
Date change released for comment:	10/7/2021
Date comment adjudication published:	10/26/2021