COMMON Certificate Policy Change Proposal Number: 2024-02

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Updates to clarify Remote Workstation definition
Date: January 9, 2024

Title: Remote Workstation Clarification

X.509 Certificate Policy For The Federal PKI Common Policy Framework Version 2.6 November 3, 2023

Change Advocate's Contact Information: fpki@gsa.gov

Organization requesting change: CPWG

Change summary: Clarify the definition of a "remote workstation used to administer the CA" in order to accommodate current secure practices.

Background: The use of "Remote Workstation used to administer the CA" was first used in Section 5.1 in the Common CP in versions prior to version 2.0. Upon update to version 2.0 the term was included in a practice note in Section 5.1; however, during the update process to version 2.1 (CP 2023-02) this term was moved to the glossary for ease of reference and was slightly updated to remove technical controls from the definition in favor of simply referencing the relevant sections within a note in the definition.

This definition has caused some concerns with FPKI audits due to a generic reference to "external networks," contained within the definition.

Additionally, the CPWG noted that the associated technical controls for remote workstations in Section 6.7 specifically calls out VPN which is too specific for the intent of ensuring mutual authentication and confidentiality between the remote workstation and the CA being administered.

Specific Changes:

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

6.7 NETWORK SECURITY CONTROLS

…

Any remote workstation used to administer the CA must ~~use a Virtual Private Network (VPN) to access the CA. The VPN must~~ be configured for mutual authentication. The remote workstation to CA communications, to include CA boundary control devices, must incorporate data integrity and confidentiality services. The remote workstation to CA network communications must be encrypted~~ion~~ and must not be vulnerable to replay or machine-in-the-middle attacks~~, and integrity~~. If mutual authentication is shared secret based, the shared secret must be changed at least annually, must be randomly generated, and must have entropy commensurate with the cryptographic strength of certificates issued by the PKI being administered.

Once the connection is established between the remote workstation and the CA or boundary control devices, the CA must permit remote administration only after successful multi-factor authentication of the Trusted Role at a level of assurance commensurate with that of the CA.

APPENDIX D: GLOSSARY

…

Remote Workstation	In the context of FPKI, "remote workstation" refers to a system used to access either the system hosting the CA or the CA itself through ~~external~~ a network or networks that are not dedicated to the maintenance and administration of the CA. Note: Reference Sections 5.1, 6.5, 6.6.1, and 6.7 for additional technical controls required of remote workstations. This term does not refer to consoles within the CA's security perimeter or to Registration Authority workstations.

Estimated Cost: None

Implementation Date: Immediate upon publication

Prerequisites for Adoption: None

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to CPWG:	9/26/2023
Date change released for comment:	10/20/2023
Date comment adjudication published:	11/28/2023