DEPARTMENT OF WAR
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301 -6000

CHIEF INFORMATION OFFICER

APR 01 2026

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOW FIELD ACTIVITY DIRECTORS

SUBJECT: Updated Criteria for Commercial Public Key Infrastructure Non-Person Entity and Code-signing Certificates on Public-Facing DoW Websites

Reference: DoD Instruction 8520.02, Public Key Infrastructure and Public Key Enabling, May 18, 2023

This memorandum amends paragraphs 3.1.a.(4)(c) and 3.a.(5)(a) of DoD Instruction (DoDI) 8520.02, "Public Key Infrastructure and Public Key Enabling." These paragraphs list the conditions under which DoW system owners may use commercially issued Non-Person Entity (NPE) or code-signing Public Key Infrastructure (PKI) certificates on their unclassified public-facing websites, DoW Enterprise Email Message Security Gateway (EEMSG) mail servers, or DoW Mobile Device Management (MDM) systems.

Attachment A replaces the 8520.02 conditions with a new process for evaluating and approving these NPE or code-signing PKI certificates for use on unclassified DoW public-facing websites, DoW EEMSG mail servers, or DoW MDM systems. Attachment B sets out the specific circumstances under which system owners may use commercially issued NPE and code-signing PKI certificates on DoW systems once they've been approved in accordance with Attachment A. As a transition period, DoD Components may continue accepting PKI certificates approved under the prior reference (a) process for one year from the date of signature of this memorandum. DoW CIO will update reference with the process in this memorandum.

This memorandum does not apply to PKI certificates issued by DoW or DoW External Certificate Authority (ECA) vendors, PKI certificates issued to internal facing DoW websites, or to acceptance of external PKIs for authentication to DoW systems. For information on these topics, see reference (a). This memorandum is solely focused on providing a means to identify DoW systems to external non-DoW browsers, systems, and users that do not recognize the DoW PKI.

DoW is working with the General Services Administration (GSA) to develop a Federal public trust PKI for NPEs. Once a Federal public trust PKI is fully operational, DoW Components operating public-facing .mil websites using commercial PKI certificates must transition to certificates issued by the Federal public trust PKI, as the previously obtained commercial PKI certificates expire.

The DoW CIO retains discretion to modify this memorandum's effective period and to remove a commercial PKI vendor from the approved list due to security or compliance concerns. The point of contact for this memorandum is Dr. Britta Hale, osd.mc-alex.dod-cio.mbx.pki-mfa@mail.mil.

Kirsten A. Davies

Attachment:
As Stated

ATTACHMENT A

Approval Process for Commercial NPE & Code-signing PKIs

This new approval process is expected to be a living document. It will be made available to the DoW community at: https://intelshare.intelink.gov/sites/dodcioicamdocs, and will be updated in response to evolving security risks. This approval process is intended only for NPE and code-signing PKI certificates issued by commercial PKI vendors for installation on unclassified public-facing DoW websites, unclassified DoW Enterprise Email Message Security Gateway (EEMSG) mail servers, or unclassified DoW Mobile Device Management (MDM) systems.

1. To be evaluated for approval, the vendor must have a DoW Component CIO sponsor (GS15/06 equivalent or above). The DoW sponsor will initiate the approval process by sending a request for approval to the DoW CIO Cryptographic Acquisition, Testing, and Licensing Authorization for Security (ATLAS) group distro (osd.pentagon.dod-cio.list.cs-atlas@mail.mil), and providing:[1]

    a. The reason the sponsor needs the commercial PKI certificates from the vendor.

    b. The vendor's System and Organization Controls (SOC)-3 and annual compliance audit reports (as submitted to the Certificate Authority Browser (CA/B) Forum) and an explanation of how any findings are being addressed.

    c. Documentation demonstrating that the vendor's commercial PKI meets the CA/B Forum baseline requirements.

    d. Evidence that the vendor is a member of the Microsoft, Google, Mozilla, Apple, and/or JAVA root programs and has one or more Root Certification Authorities (CA) listed in the corresponding default root store(s).

    e. Evidence that the vendor's PKI meets current DoW PKI algorithm strength standards and is aligned with current DoW planned transition timelines to stronger Post-Quantum Cryptography (PQC) algorithms.

2. At the request of the DoW CIO, the DoW PKI Program Management Office (PMO) and DoW PKI Configuration Control Board (PCCB) will assist in evaluating and validating information, reports, or documentation submitted by the sponsor.

3. At the request of the DoW CIO, the DoW Component CIO Sponsor will work with the vendor, the DoW CIO, and such other DoW organizations which may be tasked by the DoW CIO to facilitate a DoW security review of the commercial PKI vendor. The sponsor will provide any information requested by the DoW CIO in support of the DoW vendor security review.

[1] Information submitted by the sponsor or vendor for review, including any records that contain personal information, will be safeguarded and retained in accordance with applicable DoW records management, privacy, and information security policies.

4. The DoW CIO will determine whether to approve the commercial PKI for use on unclassified public-facing DoW websites, unclassified DoW Enterprise Email Message Security Gateway (EEMSG) mail servers, or unclassified DoW Mobile Device Management (MDM) systems which meet the criteria in Attachment B.

5. If a commercial PKI is approved by the DoW CIO, it will be listed on the Cyber.mil website run by DISA (https://www.cyber.mil/).

6. If a commercial PKI is approved, the DoW sponsor for the commercial PKI will certify annually to the DoW CIO that the commercial PKI still meets the requirements in step 1 of this attachment. The DoW CIO retains the discretion to have approved commercial PKI vendors undergo additional periodic security reviews as a condition of continued approval.

ATTACHMENT B

Instructions For System Owners

DoW System Owners may only use DoW-approved NPE and code-signing PKI certificates issued by commercial PKI vendors for installation on unclassified DoW websites, unclassified DoW Enterprise Email Message Security Gateway (EEMSG) mail servers, or unclassified DoW Mobile Device Management (MDM) systems, or to certify code on unclassified DoW websites, if all the following conditions are met:

1. The DoW website or EEMSG mail server must be unclassified and hosted on an unclassified network.

2. The DoW website or EEMSG mail server must be public facing (the public facing requirement is not applicable to MDM systems).

3. If the DoW website, MDM system, or EEMSG mail server is hosted on a defense information system network, then it must be hosted in an appropriately isolated network segment (e.g., a DoW de-militarized zone).

4. If the DoW website, MDM system, or EEMSG mail server operates in the .gov or .mil top-level domain space, the commercial PKI certificate must meet the criteria for domain validation.