Using Commercial PKI Certificates

How and where commercial PKI certificates may be used within the DoD

Introduction

The DoD PKI provides certificates to support most PKI use cases within DoD, but there are certain scenarios in which commercial PKI certificates are permitted – and in fact encouraged - to be used. This document provides answers to frequently asked questions regarding the use of commercial PKI certificates within DoD.

1. What is the difference between the External Certification Authority (ECA) PKI, DoD-Approved External PKIs, and commercial PKIs?

The major difference is that commercial PKIs are publicly trusted by the major vendor (Microsoft, Mozilla, Apple, Java) root certificate programs, so those certificates will be trusted out-of-the-box by those vendors and their products (operating systems, browsers, etc.). The ECA PKI and DoD-Approved External PKIs generally are not publicly trusted.

The **ECA PKI** is a DoD-sponsored PKI for which DoD owns and operates the root CAs. ECA vendors offer different types of certificates for both users and devices on an individual, fee-for-service basis to support a variety of use cases. ECA PKI credentials are approved for use by DoD systems both to authenticate users and devices. However, the ECA root CAs are not publicly trusted (do not participate in the major vendor root programs).

DoD-Approved External PKIs are non-DoD organizational PKIs that have been evaluated and approved by DoD in accordance with the DoD External Interoperability Plan. These PKIs are divided into three categories: (1) US Federal Agency PKIs, (2) Non-Federal Agency PKIs cross-certified with the Federal Bridge Certification Authority, and (3) Foreign, Allied or Coalition Partner PKIs/Other. DoD-Approved External PKIs have successfully completed PKI interoperability testing with the Joint Interoperability Test Command, and, for Category II/III PKIs, have executed legal Memoranda of Agreement (MoA) or of Understanding (MoU) with DoD CIO. They primarily issue end user credentials such as PIV and PIV-I certificates, and their credentials are approved for acceptance by DoD systems at DoD medium hardware-equivalent and higher assurance levels (as mapped within their policy documentation and cross-certificates with the Federal Bridge). They typically do not offer PKI certificates on an individual, fee-for-service level. They also typically are not publicly trusted (do not participate in the major vendor root programs), although the PKI vendors who operate the DoD-Approved External PKIs in some cases also operate other PKIs that are publicly trusted.

Commercial PKIs, as used within the DoD CIO memo from January 2018 about "Commercial Public Key Infrastructure Certificates on Public-Facing DoD Websites," is a generic term used to refer to PKIs that are operated by vendors on an individual fee-for-service basis (e.g. you can purchase a single certificate for a single web site) and are publicly trusted (participate in the major vendor root programs). As such, purchasing a commercial PKI certificate for a web server results in sites and services hosted by that server being trusted out-of-the-box by the major web browsers and operating systems.

2. **Am I allowed to use a commercial PKI certificate on my public-facing server?**

   Yes. The latest DoD CIO guidance, "Update to Department of Defense Chief Information Officer Memorandum on Commercial Public Key Infrastructure Certificates on Public-Facing DoD Websites" dated 4 October 2018, authorizes the use of commercial PKI TLS (server) and code signing certificates on unclassified public-facing DoD PKI web sites and mobile device management (MDM) systems.

3. **What is the benefit of using a commercial PKI certificate over a DoD PKI certificate?**

   Public-facing DoD web sites and services typically serve user populations that may be accessing those sites and services from systems that are not under DoD enterprise management. As such, those systems do not trust the DoD PKI by default, but would need to be configured to do so. Such configuration requirements place additional burden on users and introduce additional security risk if the users do not follow the proper processes to validate the DoD PKI root certificates prior to installing them. Additionally, on systems that have not been configured to trust the DoD PKI, sites that use DoD PKI certificates will be flagged by browsers and other system components as untrusted, which could make users question their legitimacy or cause connections to the sites to fail.

   Alternatively, using a commercial PKI certificate issued by a PKI that is a member of the major vendor (Microsoft, Mozilla, Apple, Java) root certificate programs means that those certificates will be trusted out-of-the-box by those vendors and their products (operating systems, browsers, etc.) without any additional configuration requirements placed on the user. Each of the vendors has a set of requirements with which member PKIs must comply to ensure a basic level of confidence in certificates issued by those PKIs.

4. **Which commercial PKI certificates am I allowed to use?**

   The DoD CIO memo attachment details specific conditions and requirements applicable to the use of commercial PKI certificates. In terms of selecting a PKI vendor, that vendor is required to be included in the list of DoD-Approved External PKIs published at https://iase.disa.mil/pki-pke/interoperability. This does not mean that the certificate must be issued by an existing DoD-Approved External PKI or the ECA PKI; rather it should be issued by a PKI that is "publicly trusted," meaning that it is a member of the Microsoft/Mozilla/Apple/Java root programs, whose operating vendor also operates a DoD-Approved External PKI or an ECA issuing CA.

   As of October 2018, the PKI vendors that meet both requirements include:

   DigiCert - https://www.digicert.com/ssl-certificate/

   Entrust - https://www.entrustdatacard.com/products/categories/ssl-certificates

   IdenTrust - https://identrust.com/certificates/website-security

   Current lists of major vendor root program participants can be found at:

   https://social.technet.microsoft.com/wiki/contents/articles/31634.microsoft-trusted-root-certificate-program-participants.aspx - Microsoft Trusted Root Certificate Program Participants

   https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReport - Mozilla CA Certificate Program

   https://ccadb-public.secure.force.com/mozilla/CACertificatesInFirefoxReport - Firefox Trusted Certificates (Mozilla)

   https://support.apple.com/en-us/HT207189 - macOS Trusted Roots (Apple)

   https://support.apple.com/en-us/HT204132 - iOS Trusted Roots (Apple)

   The Federal PKI also maintains information on the various vendor trust stores and root programs at https://fpki.idmanagement.gov/truststores.

   Prior to procuring a commercial PKI certificate, ensure that the Terms of Service and End-User License Agreement (EULA) from the vendor conform to DoD standards and applicable laws.

5. What kind of certificate do I need?

The DoD CIO memo requires SSL/TLS certificates that meet Domain Validation (DV) requirements for sites with .MIL or .GOV top-level domains (TLDs). PKI vendors may also offer Organization Validated (OV) and Extended Validation (EV) certificates; these are levels of validation higher than DV, and as such meet DV requirements.

Beyond that distinction, the domain name or names used by your server will drive whether you need a single domain certificate, one that supports multiple domains, or a wildcard certificate. You will want to ensure that all names by which users or systems might address the site(s) and/or service(s) hosted by your server are included in the certificate to avoid certificate name mismatch errors that will result in browser warnings for users and failed connections for systems. Typically, additional names will be listed within the certificate's Subject Alternative Name, or SAN, extension.

SSL/TLS certificates are typically software-based certificates (as opposed to stored in a hardware security module (HSM) like those on the CAC) and carry software-level assurance.

6. How do I obtain a certificate?

Each vendor will have their own process for issuing certificates, and vendor-specific information can be found at the URLs listed for each vendor. Typically, a public/private key pair and Certificate Signing Request (CSR) will need to be generated on the system where the certificate will be installed; instructions for generating key pairs and CSRs on various web servers can be found in the PK-enabling guides available in the Web Servers table at https://iase.disa.mil/pki-pke/Pages/admin.aspx . The CSR, which contains the public key, can then be submitted to the commercial PKI vendor for signing; the signing process certifies the certificate and public key of the key pair under the publicly-trusted root. Once the certificate has been signed, it can be downloaded and installed on the target system. The installation process associates the certificate with the private key, which never leaves the target system during the process, and allows the system to use the certificate to prove its identity to users and other entities.

7. Do I need a separate certificate for each server supporting my site's load-balanced or high-availability (DR/COOP) configuration?

For multiple servers or instances supporting the same site or service, a single key pair (and corresponding public certificate) can be shared amongst the various servers/instances as long as the private key is appropriately protected in all locations as well as in transit.

NIST Special Publication (SP) 800-133 section 6.3 provides requirements for the protection of the private key. Among other things, it requires that "the confidentiality and integrity protection for the private key uses a cryptographic mechanism that is at least as strong as the (maximum) security strength that must be supported by the asymmetric algorithm that will use the private key." For example, the private key could be transported from the server where it was generated to other servers via a TLS connection utilizing the strongest of the NIST-approved cipher suites (see NIST SP 800-131A) supported by the servers and secured with a server key pair at least as strong (e.g. RSA-2048/SHA-256) as the private key being transferred.

NIST SP 800-57 Part 1 section 6 provides more detailed key protection requirements and sections 8.1.5.1.3 and 8.1.5.2.2 specifically address requirements and acceptable methods for key distribution (a.k.a., transporting a private key from one location to another).