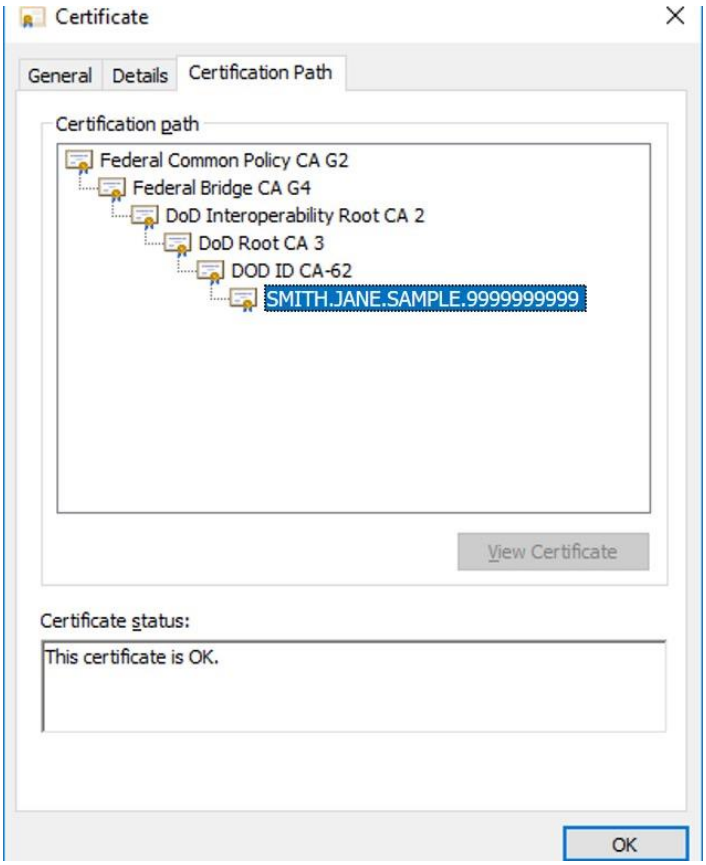
DoD Public Key Enablement (PKE) Frequently Asked Questions

DoD Cross-Certificate Chaining Problem

Contact: dodpke@mail.mil
URL: https://cyber.mil/pki-pke

Enabling PKI Technology for DoD Users

Issue	The Department of Defense (DoD) Public Key Enabling (PKE) team and the DoD Public Key Infrastructure (PKI) Program Management Office (PMO) have received several reports from DoD services about DoD certificates chaining improperly to root Certification Authorities (CAs) other than the DoD root. User certificate chains on workstations experiencing this issue may look similar to the following:



When this occurs on DoD systems, PKI validation does not work properly and may result in the following:

a) DoD user denied access to DoD web sites
b) DoD signed emails in Microsoft Outlook appear invalid

	c) DoD users experience extensive delays with Outlook or Edge during validation d) DoD users receive a prompt to install the Federal Common Policy CA G2 or other Federal Bridge cross-certified root CAs when opening a signed email
Discussion	Several scenarios can cause a workstation to experience this problem. Due to DoD information sharing initiatives with Federal and commercial partners, cross-certificates are essential for our partners to be able to validate DoD credentials but can cause problems on DoD systems when one or more of the following conditions exist: a) When the DoD PKI CA certificates are not installed locally in the correct locations, Microsoft CAPI will attempt to build a path to a known issuer (e.g., Federal Common Policy) and will automatically install cross-certificates obtained during path-processing into the user trust store. In addition to an incorrect or failed path, this can also cause significant delays. b) When valid certificate chains exist to both a DoD Root (e.g. DoD Root CA 3 or DoD Root CA 6) and other root CAs cross-certified with the Federal Bridge (e.g. Federal Common Policy), Microsoft will prefer the path with more information, which typically will be the longer path through the bridge. This situation can be exacerbated by DoD users receiving signed messages from misconfigured workstations. Microsoft Outlook will send the entire undesired certificate chain (e.g. from DoD end user up to Common Policy) in the S/MIME payload, causing the recipient to be prompted to install the non-DoD trust anchor. The user's workstation will then have a Federal Bridge member CA in its trust store, and prefer paths built to that external CA rather than those stopping at the DoD root. When trying to validate an end entity certificate, Microsoft CAPI will attempt to select the best quality chain leading up to a certificate that the user trusts. Where multiple valid chains exist, this may not be the shortest chain found (normally DoD Root CA → DoD Issuing CA → DoD user). CAPI starts by calculating the "quality" of each chain. Microsoft derives the quality of the chain from a number of factors. If a chain provides more information (i.e. valid policy constraints, name constraints) its quality increases; conversely, if it encounters errors (certificate is revoked / revocation status unknown, invalid name constraints) its quality decreases. Once these factors are evaluated, CAPI makes the decision to build a chain to a specific root certificate. More information on the Microsoft CAPI path building algorithm is available at

	https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/certificate-path-validation-in-bridge-ca-and-cross-certification/ba-p/1128610.
Recommendation	1. Administrators should run either the DoD PKE Federal Bridge Certification Authority (FBCA) Cross-Certificate Removal Tool or the DoD PKE InstallRoot tool once as an administrator and once as the current user to ensure that (1) relevant DoD root CAs are trusted, (2) relevant cross-certificates (i.e. certificates issued by DoD Interoperability Root CAs to DoD Root CAs) are untrusted, and (3) problematic certificates are deleted in both the Local Computer and Current User certificate stores. **Note:** These tools are available from the Tools page of the DoD PKE site at https://cyber.mil/pki-pke/tools-configuration-files/. Moving certificates to Microsoft's Untrusted Certificates store makes the local machine treat those certificate as revoked. This prevents the machine from building paths from DoD end entity certificates to roots outside of the DoD PKI, while still allowing paths to be built from other federal bridge members back to a DoD Interoperability Root CA trust anchor (when present in the trust store). Putting the cross-certificates in the Untrusted store provides a permanent fix, as opposed to simply removing them from the trusted Intermediate CAs store, which leaves open the potential that the certificates could be automatically re-installed during Microsoft path building in the future. 2. In Microsoft Outlook Email Security settings, the "Send these certificates with signed messages" check box should be unchecked. This will cause only the end entity signing and encryption certificates, rather than the full certificate chains, to be sent with signed messages. 3. Web server administrators with users experiencing denial-of-service due to this issue should explore options for forcing the web server to discard the presented certificate chain and attempting to build a valid path from the end user certificate on the server side. The Trust Anchor Constraints Tool (TACT), available from the DoD PKE Tools page at https://cyber.mil/pki-pke/tools-configuration-files/, is one such option.