DoD Public Key Enablement (PKE) Frequently Asked Questions

DoD Root Certificate Chaining Problem

Contact: PKE_Support@disa.mil
URL: http://iase.disa.mil/pki-pke

Enabling PKI Technology for DoD users

Issue	Department of Defense (DoD) Public Key Enabling (PKE) and the DoD Public Key Infrastructure (PKI) Program Management Office (PMO) have received several reports from DoD services about DoD certificates chaining improperly to cross-certificates or the Common Policy Root Certificate Authority (CA). When this occurs on DoD systems, PKI validation does not work properly and may result in any of 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 Internet Explorer during validation d) DoD users receive a prompt to install the Common Policy Root CA when opening a signed email of a DoD sender whose workstation is misconfigured
Discussion	Several scenarios can cause a workstation to become infected. 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., 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 Microsoft's Root Update Service is not disabled, Microsoft will automatically add the Common Policy self-signed certificates (among others) into the local computer Trusted Root store. This can pose a significant security risk and is a Windows Operating System Security Technical Implementation Guide (STIG) violation.

	c) When a DoD user receives a signed message from a misconfigured workstation, Microsoft Outlook will send the entire undesired certificate chain (e.g. from DoD end user up to Common Policy) in the SMIME payload. This can cause the prompt to install a non-DoD trust anchor and incorrect chaining outside of DoD PKI. d) When valid certificate chains exist to both the DoD Root CA 2 and Common Policy Root CA, Microsoft will prefer the path to the Common Policy Root CA. When trying to validate an end entity, MS 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 user → DoD Intermediate CA → DoD Root CA 2). It is also possible that CAPI cannot construct complete chains – this can happen when intermediate CAs are not available on the client, and the client could not retrieve the certificates (due to server issues, proxy authentication failures, insufficient rights to access the network, and other issues). This process is also affected by certificate discovery – can the client access all certificates in the chain. CAPI starts by calculating the "quality" of each chain. The quality of the chain is derived from a number of factors. If a chain provides more information (i.e. valid policy constraints, revocation check succeeded) 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 MS CAPI path building algorithm is available at http://blogs.technet.com/b/pki/archive/2010/05/13/certificate-path-validation-in-bridge-ca-and-cross-certification-environments.aspx.

Recommendation	1. Administrators should run the Federal Bridge Certification Authority (FBCA) Cross-Certificate Removal Tool v1.06 once as an administrator and once as the current user. The tool is available from the DoD PKE site at http://iase.disa.mil/pki-pke under Tools > Certificate Validation (CAC required for download). Among other things, the tool moves the Interoperability CA (IRCA) → DoD Root CA 2 certificate to Microsoft's Untrusted Certificates store, which makes the local machine treat that certificate as untrusted. 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 the Interoperability Root CA trust anchor (when present in the trust store). Putting the certificate in the Untrusted store provides a permanent fix, as opposed to simply removing it from the trusted CAs store, which leaves open the potential that the certificate could be automatically re-installed during Microsoft path building in the future. 2. DoD root and subordinate/intermediate CA certificates should be installed on all DoD systems in the appropriate locations. Administrators should use InstallRoot or other approved method of distribution (such as Group Policy Object or GPO). This will prevent Microsoft from trying to build a path to a known issuer since all required certificates are present locally. 3. In Microsoft Outlook the check box, "Send these certificates with signed messages" should be unchecked. 4. Microsoft's Root Update service should be disabled on all DoD systems (through GPO when possible) to prevent Common Policy and other certificates from being added to the local computer trusted root store through Microsoft Root Update service.