NIPRNet Test Material FAQ

How and where to obtain DoD PKI test materials

Introduction

In order to provide strong authentication, data integrity and confidentiality on NIPRNet, the DoD PKI offers PKI certificates and associated services. The Common Access Card (CAC) contains PKI certificates for user authentication and secure e-mail. The DoD PKI also issues Alternate Logon Tokens (ALTs) via the NIPRNet Enterprise Alternate Token System (NEATS) as well as software certificates to support devices and other special use cases. Additionally, the DoD PKI provides infrastructure services, such as Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responses, to support systems' use of PKI.

The Joint Interoperability Test Command (JITC) hosts a test PKI on the NIPRNet which mirrors the operational DoD PKI. This document details the NIPRNet test materials that are available and how to obtain them.

1. How do I obtain unclassified test tokens (i.e., CAC/NEATS)?

Test tokens are reserved for DoD (or DoD-sponsored vendor) testing and development activities that require direct interfaces with smart cards or assertion of specific card-associated policy OIDs (e.g. hardware assurance, administrator) within the test certificates. Common examples of such scenarios are network smart card logon, system administration use cases, and physical access control systems (PACS) functions. Most web browser-based systems or web client authentication use cases are abstracted from details about smart cards and can be tested using software certificates (see question #3). Test token request forms are processed through the DoD Components' test card approval agents to DMDC's test lab. Test token request instructions and forms can be found on DMDC's CAC Developer Resources page at https://www.cac.mil/Common-Access-Card/Developer-Resources/ under *Test Material*.

2. How do I obtain card reader middleware for testing?

In many instances, native operating system capabilities such as Microsoft's native PIV mini-driver can be used to interact with the card and third-party middleware is not required. However, certain capabilities such as PIN caching require third-party middleware.

Third-party card reader middleware such as HID ActivClient and 90meter Smart Card Manager is licensed and maintained at the DoD Component level. Inquiries for access to third-party middleware licenses for use in internal and properly sponsored vendor development/testing should be made to your Component PKI lead or help desk.

3. How do I obtain a test user software certificate?

User software certificates can be suitable for testing in instances where the application being tested does not need to interact directly with the smart card, but only with the PKI certificate. A common example of such a scenario would be testing user authentication to a web-based application. Software certificates can be issued and delivered more quickly than test CACs due to the lack of cost and shipping requirements associated with hardware tokens.

JITC software user certificates should be requested through your Component RA Operations office. Once a JITC-provisioned RA has submitted and approved the request, the RA will work with the requestor to transfer the credentials through a secure channel. If revoked test certificates are desired, users may self-revoke certificates for which they possess the private keys from the revocation tab of the web site of the CA that issued the certificate.

Contact information for various Component RA Operations offices is available under *Combatant Command/Service/Agency Registration Authority Operations Offices* on the *Help* page of the DoD PKE web site at https://public.cyber.mil/pki-pke.

4. How do I obtain a test server certificate?

JITC SSL (web server) and domain controller certificates can be requested from the JITC Non-Person Entity (NPE) Portal at https://npe-portal.c3pki.nit.disa.mil/ and approved by your local NIPRNet JITC-provisioned RA. Refer to the *Obtaining a PKI Certificate for a DoD Server* guide available from the DoD PKI/E Document Library at https://cyber.mil/pki-pke/pkipke-document-library/ (PKI-protected) for step-by-step instructions to request a certificate.

5. Where can I obtain the NIPRNet test trust anchors?

The JITC PKI Certification Authority (CA) certificates are available in the InstallRoot NIPR Windows Installer and JITC PKCS#7 CA Certificate Bundle located in the DoD PKI/E Document Library at https://public.cyber.mil/pki-pke/pkipke-document-library/.

Refer to the *InstallRoot User Guide* available in the same location for InstallRoot instructions.

6. What revocation checking options are available?

The JITC test PKI offers CRLs and an OCSP responder infrastructure that mirrors what is available in production. The URLs for CRL Distribution Points (CDPs) and the JITC OCSP responder are available within the CRLDP and AIA OCSP values, respectively, of the test certificates. See the *Anatomy of a Certificate* slick sheet located in the DoD PKI/E Document Library at https://cyber.mil/pki-pke/pkipke-document-library/ (PKI-protected) for more information on the various data available within the certificate.

7. Where does the test infrastructure exist?

The JITC PKI test infrastructure is only available on NIPRNet. Revocation data for JITC PKI certificates is publicly available from the commercial internet.

8. Where can I find supplemental usage guidance?

Refer to the DoD PKE site at https://cyber.mil/pki-pke (PKI-protected) or https://public.cyber.mil/pki-pke (publicly accessible, more limited content) for additional policies, memorandums, and implementation documentation regarding DoD PKI operations and PK-enabling.