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 software certificates to support devices and other special use cases, and 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 a test CAC?

Test CACs are reserved for DoD (or DoD-sponsored vendor) testing and development activities that require direct interfaces with smart cards. Common examples of such scenarios are mobile devices, network smart card logon, and physical access control systems. 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 #4). Test CAC request forms are processed through the DoD Components' test card approval agents to DMDC's test lab. Submissions and inquiries can be made to DMDC at cacsupport@mail.mil.

2. How do I obtain access to smart card development tools?

The CAC developer's kit (CDK) is owned and managed by DMDC; inquire at cacsupport@mail.mil for access. Please note that all software provided within CDK is provided for sample/reference purposes only and is prohibited from being integrated into operational systems or commercial products.

ActivIdentity provides their software development kit (SDK) free of charge to DOD Components who maintain licenses for ActivClient. Distribution is managed at the DoD Component level. Inquiries for access should be made to your Component PKI lead or help desk. Contact information for various Component PKI support organizations is available under *Combatant Command/Service/Agency Help Desks* on the *Contact Us* page of the DoD PKE web site at http://iase.disa.mil/pki-pke.

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

ActivClient and other third-party middleware is licensed and maintained at the DoD Component level. Inquiries for access to 3rd party middleware licenses for use in internal and properly sponsored vendor development/testing should be made to your Component PKI lead or help desk.

4. 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.

NIPRNet software certificates may be available from your RA Operations office if they have a JITC NIPRNet RA, or can be requested directly from JITC by emailing the JITC PKI team at disa.huachuca.jitc.list.projectpki@mail.mil. A CSV-formatted bulk submission template is available in instances where multiple test certificates are needed. After a JITC RA has processed the request, requestors will be provided with a Certificate Request Information (CRI) form that will allow them to directly download the issued certificate. 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 *Contact Us* page of the DoD PKE web site at http://iase.disa.mil/pki-pke.

5. How do I obtain a test server certificate?

NIPRNet SSL (web server) and domain controller certificates can be requested from JITC at https://ca-27.c3pki.nit.disa.mil and approved by your local JITC NIPRNet RA or by emailing the request ID to the JITC PKI team disa.huachuca.jitc.list.projectpki@mail.mil. However, your local RA may have a preferred site and should be contacted for that information.

Refer to the *Obtaining a PKI Certificate for a DoD Server* guide available on the DoD PKE site under *PKE A-Z* > *Guides* for step-by-step instructions to request a certificate.

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

The JITC PKI Certification Authority (CA) certificates are available in the InstallRoot Windows Installer and InstallRoot-J utility located on the DoD PKE site at http://iase.disa.mil/pki-pke under *Tools* > *Trust Store Management*.

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

7. 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 on the DoD PKE site at http://iase.disa.mil/pki-pke under *PKE A-Z* > *Slick Sheets & White Papers* for more information on the various data available within the certificate.

8. Where does the test infrastructure exist?

The JITC PKI test infrastructure is only available on NIPRNet.

9. Where can I find supplemental usage guidance?

Refer to the DoD PKE site at http://iase.disa.mil/pki-pke for additional policies, memoradums, and implementation documentation regarding DoD PKI operations and PK-enabling.