

[GDS TESTING AND SUPPORT](#)

The Global Directory Service (GDS) is a Department of Defense (DoD) and National asset. GDS offers a DoD-wide search capability for information regarding DoD personnel (e.g., name, email address, and key encipherment certificate). In addition, GDS provides certificate revocation lists and Certificate Authority certificates to the user community (JITC GDS provides to the test community), an essential ingredient in public key infrastructure and secure email. The JITC GDS directly supports GDS with operational configuration management and independent verification and validation testing of deploying GDS systems and components .

[JEDS TESTING AND SUPPORT](#)

The Joint Enterprise Directory Services (JEDS) is a DISA initiative to build a Global Information Grid (GIG) Directory. JITC JEDS provides the NIPRNET based testing community enterprise directory services that replicates the JEDS operational interfaces (secure HTTP, Lightweight Directory Access Protocol and Web services (SOAP, SAML, and XML)) that supply white pages (NCES People Discovery) and NCES security Services attribute services. The JITC JEDS directly supports JEDS with operational configuration management and independent verification and validation testing of deploying JEDS systems and components

For more information on JITC's PKI Test Facility, please contact JITC at:

JITC PKI/PKE/CAC/GDS /JEDS Project Officer
DSN 879-5481
(520) 538-5481

Websites

<http://jitc.fhu.disa.mil/pki> (PKI/PKE/CAC)
<https://dod411.chamb.disa.mil> (GDS)
<https://jeds.gds.disa.mil> (JEDS)



Defense Information Systems Agency
Department of Defense

Joint Interoperability Test Command

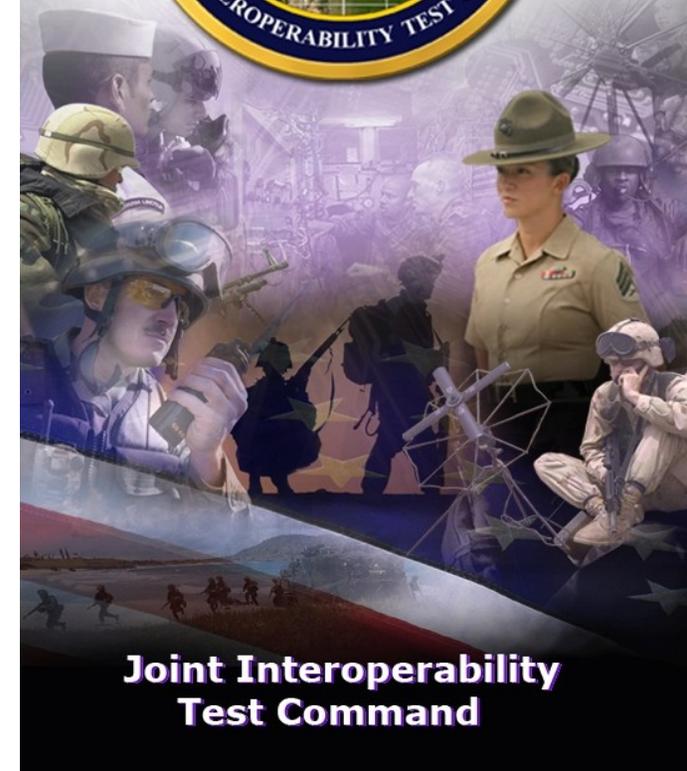
Attn: Visitor Support Center
P.O. BOX 12798
Fort Huachuca, AZ 85670-2798

Phone: 1-800-538-5482
<http://jitc.fhu.disa.mil>

Experts in Testing and Certification
Accelerating the Nation's IT Dominance



THE DOD PUBLIC KEY INFRASTRUCTURE (PKI) TEST FACILITY



**Joint Interoperability
Test Command**

The Joint Interoperability Test Command (JITC) Public Key Infrastructure (PKI) VISION

- ◆ To be the premier Department of Defense (DoD) PKI test organization
- ◆ To provide unequaled PKI support to DoD and its commercial partners
- ◆ To help successfully deploy a fully interoperable PKI

OVERVIEW

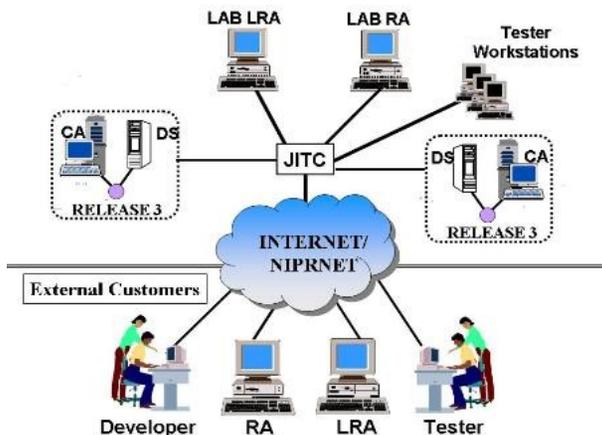
The DoD PKI is the provider of choice for authentication, confidentiality, non-repudiation, and access control to DISA's Enterprise network applications, including Joint Enterprise Email and Defense Enterprise Portal Services.

To help ensure the long-term success of the DoD PKI and programs which rely on PKI services, the JITC offers the following PKI services:

- ◆ DoD PKI test certificate services
- ◆ Coalition PKI test certificate services
- ◆ Non-Person-Entity test certificate services
- ◆ SIPRNet Token Management System services
- ◆ Interoperability certification of Public Key Enabled (PKE) applications
 - ◇ Online Certificate Status Protocol (OCSP) Responders testing
 - ◇ External Certification Authority (ECA) certifications
- ◆ Common Access Card (CAC) end-to-end testing and support
- ◆ Global Directory Service (GDS) testing and support
- ◆ Joint Enterprise Directory (JEDS) testing and support

DOD PKI TEST CERTIFICATE SERVICES

The JITC PKI Test Certificate Lab provides test certificate services in support of DoD and commercial partners to help successfully deploy a fully interoperable PKI. The lab was established by the Defense Information Systems Agency and the PKI Program Management Office (PMO) as the official test facility for the issuance of DoD PKI test certificates.



The JITC PKI enclave replicates the configuration of the operational PKI enclave at the Defense Enterprise Computer Center (DECC) Chambersburg, PA. This allows testing, development, and training to occur in an environment separate from the operational infrastructure yet with the same functionality. All software used by DoD PKI is tested at JITC before being installed at a DECC.

PKE APPLICATIONS

DoD policy states that enabled applications will be tested to ensure interoperability and compatibility with the DoD PKI. To support this policy, the DoD PKI PMO established the JITC DoD PKE Certification Lab as an independent testing facility to perform interoperability testing on PKE applications.

The certification process is based on a master test plan containing all DoD PKE requirements and associated tests. Each PKE application is different and takes advantage of various DoD PKI services; therefore all the DoD PKE requirements may or may not be applicable to every application.

OCSP Responders Testing

Currently the DoD PKI uses Certificate Revocation Lists (CRLs) to check the status of issued certificates. An alternative to CRL checking is to use OCSP. OCSP is a request-response protocol used for obtaining online certificate revocation information from a trusted entity, referred to as an OCSP Responder. OCSP Responders provide immediate revocation information on specific

certificates rather than a list of certificate revocation information in the form of a CRL.

JITC conducts OCSP Responder testing by using DoD Class 3 PKI test certificates and CRLs issued from the JITC PKI test Certificate Authority (CA).

ECA Certifications

The DoD has established an accreditation process to create trust relationships with CAs outside of the DoD domain. These ECAs will provide non-DoD personnel with certificate services that interoperate with the DoD PKI. Contractors, vendors, and other interested parties may use certificates obtained from an accredited ECA to transact electronic business with DoD entities.

As part of the accreditation process, ECAs must achieve an assurance level equivalent to or greater than the DoD PKI Medium Assurance Policy. JITC performs standards compliance testing of ECA-issued certificates, CRLs and online certificate status protocol request and response formats (collectively ECA-issued objects), and interoperability testing of ECA-issued certificates and CRLs in order to ensure ECAs achieve this assurance level.

CAC END-TO-END TESTING AND SUPPORT

The DoD PKI supports both hardware certificates placed on CACs as well as software certificates. The DoD issues CACs with PKI certificates to all active duty military personnel, DoD civilians and eligible contractor personnel. Several systems are involved in the CAC issuance process, namely the Real-time Automated Personnel Identification System (RAPIDS), the Defense Enrollment Eligibility Reporting System (DEERS), the Issuance Portal (IP) system, and the DoD PKI. JITC provides the necessary technical services to perform enterprise testing of the end-to-end issuance process of the CAC as it relates to each of the systems involved in the process. This includes testing various hardware certificate issuing CAs. JITC tests and supports the Robust Certificate Validation Services (RCVS), enclave monitoring system, and other components as necessary, to verify their functionality with the DoD PKI.