What type of test material would best serve my development, integration, or testing needs?

The DoD CAC-PKI programs provide identity credentials for several different populations within DoD for different purposes. Most of the infrastructures that provide these credentials have a companion test infrastructure for DoD's development and testing communities. Below is a list of the different available DoD CAC-PKI test material with recommended usages:

#	Test Material	Target Development/Test Audience	Typical Turnaround
A	**DoD PKI Test Software Certificates** • Target population: DoD personnel or affiliates who do not process CACs. • Description: DoD PKI test software certificates are the best test material to be used in development/testing of web-based application, portals or website in which the user interface is a browser. This material is distributed virtually as PKCS#12 files.[1] • DoD Lead: DISA • Location: Instructions on requesting software certificates can requested from DISA at dodpke@mail.mil.	• Web-based applications, portals, and/or websites in which browser is user interface. • Applications that secure cryptographic services from Microsoft Cryptographic Application Interface (API) or Cryptography API: Next Generation (CNG)	**1-2 business days**
B	**DoD External Certificate Authority PKI Test Credentials** • Target population: DoD business partners and individuals needing to interact with DoD who are not direct contract support personnel (e.g., contractor personnel who do not qualify for CACs). Primary usage is to digitally sign/encrypt e-mail, digitally sign forms, and authentication to DoD websites/web-applications. • Description: DoD PKI test certificates that come in the form of software (i.e., PKCS#12 files) or hardware (i.e., smart card) credentials. • DoD lead: DISA • Location: Availability of this test material is limited. Requests for ECA test material should be made directly to the vendors (https://public.cyber.mil/pki-pke/interoperability/)	• Web-based applications, portals, and/or websites in which browser is user interface. • Applications that secure cryptographic services from Microsoft Cryptographic Application Interface (API) or Cryptography API: Next Generation (CNG) • Applications/devices that service non-CAC eligible personnel. • Application/devices that have knowledge of and technical interfaces to smart cards and/or external tokens and need services directly from them. • Application/devices that need services from the ECA smart cards and	**Varies by DoD ECA Vendor**

[1] Note: PKCS#12 file contain both private keys and certificates. For more info: http://www.rsa.com/rsalabs/node.asp?id=2138

		process cryptography from tokens on their own, i.e., without leveraging web browsers or MS cryptographic capabilities	
C	**DoD Test Alternate Tokens** • Target population: Non-CAC eligible populations who require access to UNCLASSIFED networked DoD accounts (e.g., selected volunteers or non-US persons) • Description: DoD PKI test certificates that come on hardware (i.e., smart cards) tokens procure and managed by the DoD Components. These cards do not contain barcode or contactless technologies. • DoD lead: Individual DoD Components • Location: This material is available and identified in the test token request form at https://www.cac.mil/Common-Access-Card/Developer-Resources/, under "Test Material."	• Applications/devices that service non-CAC eligible personnel. • Application/devices that have knowledge of and technical interfaces to smart cards and/or external tokens and need services directly from them. • Application/devices that need services from the alternate tokens and process cryptography from tokens on their own, without leveraging web browsers or MS cryptographic capabilities	**Varies by DoD Component**
D	**DoD Test Common Access Card** • Target population: DoD civilian, military, and selected contract support personnel. • Description: DoD test credential that contains hardware DoD PKI certificates, DoD CAC Data model including FIPS 800-73 interfaces, contactless technology, 2-dimensional barcode (PDF417), linear barcode (Barcode 39), and conforms with FIPS 201. • DoD lead: DMDC • Location: Test CAC request forms are process through the DoD Components test card approval agents. Submissions and inquiries can be made directly to each DoD Component CAC-PKI leads or cacsupport@mail.mil.	• Application/devices that have knowledge of and technical card edge interfaces to smart cards and/or external tokens and need service directly from CACs. • Application/devices that need services from the CAC and process cryptography from tokens on their own, i.e., without leveraging web browsers or MS cryptographic capabilities.	**Approximately 25-30 business days**