



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

JUL 22 2003

CHIEF INFORMATION OFFICER

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF
DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF
DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Approval of External Public Key Infrastructures

Use of hardware credentials with public key infrastructure (PKI) certificates for authentication has enhanced the security of information systems and business processes of the Department.

The Federal Bridge Certification Authority (FBCA), overseen by the Federal CIO Council, facilitates trust between disparate PKIs. In accordance with DoD Instruction 8520.2, members of the following PKIs, upon successful completion of interoperability testing as described in attachment 1, are approved for use with DoD information systems:

- FBCA member PKIs cross certified at Medium-Hardware or High Assurance levels
- PKI members of other PKI bridges that are cross certified at FBCA Medium-Hardware or High assurance levels
- PKIs that assert the Federal PKI Common Policy Medium-Hardware or High assurance level

Also approved for use are Foreign, Allied, Coalition partner, and other External PKIs, subject to conditions described in attachment 1.

DoD system, application and portal owners are cautioned to continue to use appropriate access control procedures in conjunction with PKI authentication to ensure



appropriate security. To assist application and portal owners with making appropriate trust decisions, attachment 2 lists operational differences between the DoD PKI and approved external PKIs. The DoD PKI Program Management Office, the DoD Public Key Enabling (PKE) Team and the DoD External Interoperability Working Group will work with DoD system owners and DoD partners to facilitate initial interoperability testing, establishment of the trust paths, and use of DoD-approved PKIs in their logical access control procedures. The DISA PKE team will establish a trusted DoD repository of all DoD approved Root Certification Authority certificates that can be used by DoD relying parties to establish specific trust relationships.

For additional information about this memorandum, contact Ms. Sheron Randolph, 703-604-5522 ext 108, sheron.randolph@osd.mil or Mr. Don Fuller, 703-604-5522 ext 112, donald.fuller.ctr@osd.mil.



John G. Grimes

Attachments:
As stated

A. DoD External Certificate Authority (ECA) PKI

Certificates issued by the DoD ECAs are approved for use within the DoD for authenticating to DoD web sites and for digital signature or encryption. The DoD ECA vendors offer certificates at the following assurance levels (the policy Object Identifiers (OID) are included in parentheses):

- **DoD ECA Medium Assurance** (id-eca-medium-token or 2.16.840.1.101.3.2.1.12.1) certificates are comparable to **DoD Medium Assurance** (id-US-dod-medium or 2.16.840.1.101.2.1.11.5) certificates issued to users in software format (i.e., .p12 files).
- **DoD ECA Medium Token Assurance** (id-eca-medium-token or 2.16.840.1.101.3.2.1.12.2) certificates are also comparable to **DoD Medium Assurance** (id-US-dod-medium or 2.16.840.1.101.2.1.11.5) certificates; however, the ECA vendor ensures that the keys and certificates are generated and stored on a hardware token (smartcard) only. The ECA Vendor relies on third party Trusted Agents for the identity proofing. Medium Token Assurance certificates should be used where the additional security of a certificate on a hardware token is desired by the relying party system.
- **DoD ECA Medium Hardware Assurance** (id-eca-medium-hardware or 2.16.840.1.101.3.2.1.12.3) certificates are comparable to **DoD Medium Hardware Assurance** (id-US-dod-mediumhardware or 2.16.840.1.101.2.1.11.9) certificates issued on the Common Access Card (CAC). These ECA certificates are generated and stored on a hardware token (smartcard) only. This assurance level is greater than the DoD ECA Medium Token Assurance level because the identity proofing is performed by the ECA Vendor versus establishing third party Trusted Agents. Medium Hardware Assurance certificates should be used where the additional security of a certificate on a hardware token is desired by the relying party system.

Application owners should consider what minimum assurance level is acceptable for authentication to their information system. In addition to the particular identifying information in the certificate, the policy OIDs for the assurance level contained in the certificate should be considered when making access control decisions based on the authenticated identity asserted by any DoD ECA certificate.

B. U.S. Federal Agency PKIs cross-certified with the Federal Bridge Certification Authority (FBCA). The FBCA is commonly referred to as the "Federal Bridge".

After interoperability testing described below is successfully completed, certificates issued by U.S. Federal Agency PKIs are approved for use within the DoD for authenticating to DoD web sites and for digital signature or encryption if either of the following are true:

- B.1. The certificate was issued by a PKI that is operated by a U.S. Federal Agency and is cross certified with the Federal Bridge at Medium Hardware Assurance (id-fpki-certpcy-mediumHardware) or High Assurance (id-fpki-certpcy-highAssurance).

Attachment 1 to Approval of External PKIs memorandum

B.2. The certificate was issued by a certified PKI Shared Service Provider¹ (SSP) operating under the x.509 Certificate Policy for the Common Policy Framework and asserts either one of the following OIDs: id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-High.

Certificates issued by U.S. Federal Agency PKIs are subject to limited Joint Interoperability Test Center (JITC) testing only to ensure that certificates are technically interoperable with DoD systems, including web servers and email clients, and that certificate revocation information can be obtained by these DoD systems. DISA will immediately commence testing.

Upon completion of testing, the Federal Agency Root CA certificates will be posted to the DoD repository for DoD application owners to retrieve, install and configure in their information systems.

C. Non-Federal Agency PKIs cross certified with the FBCA or PKIs from other PKI Bridges that are cross certified with the FBCA.

Certificates issued by non-Federal Agency PKIs will be recognized as approved for use within the DoD for authenticating to DoD web sites and for digital signature or encryption if all of the following are true:

C.1. The certificate was issued by a PKI that is cross-certified with the FBCA at the Medium Hardware level of Assurance.

C.2. The PKI has a DoD sponsor that has established a business or mission need.

C.3. JITC has successfully completed reasonable interoperability testing of the PKI to ensure that certificates are technically interoperable with DoD systems, including web servers and email clients, and that certificate revocation information can be obtained by DoD systems. To ensure that DoD users can exchange secure email with approved external PKIs, DISA will expedite testing of secure email exchange mechanisms.

Upon completion of testing, the appropriate PKI Root CA certificates will be posted to the DoD repository for DoD application owners to retrieve, install and configure in their information systems.

D. Foreign, Allied, or Coalition Partner PKIs or other PKIs not covered under A, B or C above seeking a trust relationship with DoD PKI

Certificates issued by Foreign, Allied, or Coalition partner PKIs will be recognized as approved for use within the DoD for authenticating to DoD web sites and/or digital signature or encryption if all of the following are true:

D. 1. A DoD Service or Agency system or application has identified that they require interoperability with the PKI and has established a business case or mission need to authenticate external PKI certificates.

D.2. The PKI Certificate Policy has been mapped to the DoD PKI Certificate Policy in accordance with the DoD process. The DoD Certificate Policy Management Working

¹ <http://www.cio.gov/fpkipa/cpl.htm>

Attachment 1 to Approval of External PKIs memorandum

Group (CPMWG) or its designated authority has not identified critical risks to the External Interoperability Working Group (EIWG) that would prevent certificate validation or authentication at all levels of assurance.

D.3. JITC has successfully completed reasonable interoperability testing of the PKI to ensure that certificates are technically interoperable with DoD systems, including web servers and email clients, and that certificate revocation information can be obtained by DoD systems.

D.4. The EIWG has favorably reviewed the certificate policy mapping performed by the CPMWG and the results of the JITC testing.

Upon completion of the EIWG review, the appropriate PKI Root CA certificates will be posted to the DoD repository for DoD application owners to retrieve, install and configure in their information systems

E. Approved External PKI Root CA certificates

The EIWG will work closely with DISA and JITC to ensure all appropriately tested external PKI Root CA certificates are posted in the DoD repository for DoD application owners to retrieve, install and configure in their information systems.

Attachment 2 to Approval of External PKIs memorandum

The following table highlights similarities and differences between the following approved PKIs.

- DoD – Information describes certificates issued at the Medium Assurance Hardware
- External Certification Authority (ECA) – Information describes certificates issued at the Medium Hardware and Medium Token assurance levels. Differences between these two levels are noted.
- FBCA – Information describes certificates mapped to the Medium Hardware assurance level. Note that information reflects minimum requirements to be a member of the Federal Bridge. Some members may have more stringent requirements. Certificates issued to First Responders or to industry as part of a PIV compatible program meet FBCA Medium Hardware assurance.
- PIV – Information describes certificates issued by Federal Agencies in compliance with FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*.

Category	DoD Med HW	ECA Med HW (Med Token)	FBCA Med HW ¹	PIV Common HW
Identity Proofing	In-person identity proofing with agent of PKI. Two forms of identification (ID), including a photo ID issued by a Federal or State government.	In-person identity proofing with agent of PKI for Med HW; notary for Med Token. Two forms of ID, including a photo ID issued by a Federal or State government.	In-person identity proofing with agent of PKI or notary, or existence of antecedent relationship. One photo ID issued by a Federal Government, or two non-Federal IDs, one of which must include a photo.	In-person identity proofing with agent of PKI. Two forms of ID from Form I-9 list, including a photo ID issued by a Federal or State government. Confirmation of validity of ID documents.
Background Investigation	No.	No.	No.	Yes – National Agency Check with Inquiries (NACI), full set of fingerprints checked against FBI database).
Citizenship Verification	Yes – country of Citizenship will be embedded in certificates beginning June 2008.	Yes – country of citizenship embedded in certificates.	No.	No – country of citizenship may be determined as part of NACI, information is not included in certificates.

¹ Note that FBCA information reflects minimum requirements to be a member of the Federal Bridge. Some members may have more stringent requirements.

Attachment 2 to Approval of External PKIs memorandum

Category	DoD Med HW	ECA Med HW (Med Token)	FBCA Med HW ¹	PIV Common HW
Foreign Nationals	Can issue to foreign nationals with DoD sponsorship.	Can issue to foreign nationals in US or who are citizens of Australia, Canada, New Zealand, or United Kingdom. Can issue to other foreign nationals with DoD sponsorship.	No restrictions regarding issuance to foreign nationals. No confirmation of nationality.	Can issue to foreign nationals with federal agency sponsorship and successful completion of background investigation comparable to NACL.
Biometric Capture	Yes – facial image and fingerprint capture.	No.	No.	Yes – facial image and full set of fingerprints, (checked vs FBI database) Bios stored as digitally-signed objects on card.
Audit	DoD review and approval that Certificate Practice Statement (CPS) meets Certificate Policy (CP) requirements. Annual audit of Certification Authorities (CA) performed by DoD.	DoD review and approval that CPS meets CP. Initial audit performed by DoD. Annual audit results submitted and reviewed by DoD.	Annual audit including statement that CPS meets CP provided as part of application and annually after acceptance. For bridge to bridge, audit report of bridge only.	Federal Government review and approval that CPS meets CP. Annual audit summary provided to Federal PKI Policy Authority.
Architecture	Root CA operated by DoD as trust anchor, one or more levels of subordinate CAs operated by DoD.	Root CA operated by DoD as trust anchor, single level of subordinate CAs operated by industry.	No stipulation.	Single CA operated by Federal Government as trust anchor CA, no more than two levels of subordinate CAs operated by Government or industry.
Oversight and Validation	DoD ownership of CP, CPSs, and operations.	DoD ownership of CP, DoD oversight of CPSs and oversight of audit of operations.	Federal Government mapping of CP. For bridge to bridge, Federal Government mapping of bridge CP only.	Federal Government ownership of CP, Federal Government oversight of CPSs, and operations.

Attachment 2 to Approval of External PKIs memorandum

Category	DoD Med HW	ECA Med HW (Med Token)	FBCA Med HW ¹	PIV Common HW
Assurance Levels Supported by Single CA	Medium Hardware	Medium Medium Token Medium Hardware	No stipulation. Federal Bridge assesses requirements for assurance levels being mapped, CAs can also issue other assurance levels.	Multiple assurance levels, requirements correlate to FBCA Medium, Medium HW, and High assurance as defined by Federal Bridge, except for cardAuth which does not require activation of private key.
Revocation	Process revocation within one hour of receipt. Publish Certificate Revocation List (CRL) within 24 hours. Process to provide notification of need to revoke part of normal out-processing. Process to provide notification of need to revoke upon determination that certificate is being used improperly. DoD controls revocation requests.	Process revocation within one hour of receipt. Publish CRL within 24 hours. Process to provide notification of need to revoke upon determination that certificate is being used improperly. DoD can request revocation.	Process revocation as quickly as practical upon receipt. Publish CRL within 24 hours.	Process revocation as quickly as practical upon receipt. Publish CRL within 18 hours. Federal Government can request revocation.