Department of Defense
External Interoperability Plan

Version 1.0

The Office of the Assistant Secretary of Defense

for

Networks and Information Integration/DoD Chief Information Officer

Prepared by:

External Interoperability Working Group

Approved:

Cheryl J. Roby
ACTING ASD(NII)/DoD CIO

AUG 26 2010

1 INTRODUCTION

The Department of Defense (DoD) Chief Information Officer (CIO) Memorandum, dated July 22, 2008, "Approval of External Public Key Infrastructures" [DoD CIO Memo] outlines the categories of External Public Key Infrastructures (PKIs) that are approved for use with DoD relying parties. This Public Key Infrastructure (PKI) External Interoperability Plan (EIP) outlines the steps to be accomplished in order for External PKIs to be designated as approved for use with DoD relying parties.

Certificates issued by approved external PKIs can be used within DoD for authentication to DoD private web servers and/or digital signature or encryption. PKI credentials that are DOD-approved can be used for authentication to physical access controls systems. See DOD 5200.8-R, "Physical Security Program", latest version, for policy and details regarding use of identity credentials for physical access to DOD facilities.

The use of the word "system" in this document should be construed to mean any DoD IT system, as defined in Department of Defense Directive 8500.1, "Information Assurance (IA)" [DoDD 8500.1].

The use of the term "external PKI" in this document should be construed to mean any non-DoD PKI, operated in accordance with a published certificate policy and that issues PKI certificates to defined subscriber populations.

System owners are responsible for protecting data accessed or stored in DoD information systems. They should take any necessary actions or precautions to mitigate the risks inherent with using PKI certificates for authentication in logical access control procedures. [Logical Access Memo] identifies DoD policy (Issuances) and security best practices that should be implemented in conjunction with any certificate-based authentication procedures. Access controls/authorization to access (read, change, delete) data must consider data handling caveats, foreign disclosure rules and export control/ITAR restrictions.

1.1 BACKGROUND

[DoDD 8500.1] states that "[t]he use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication shall be in accordance with published DoD policy and procedures. These technologies shall be incorporated in all new acquisitions and upgrades whenever possible. Where interoperable PKI is required for the exchange of unclassified information with vendors and contractors, the Department of Defense shall only accept PKI certificates obtained from a DoD-approved external certificate authority or other mechanisms approved in accordance with DoD policy."

DoD Instruction 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling" [DoDI 8520.2] states that "The Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)), as the DoD Chief Information Officer (CIO), shall...[a]pprove DoD relying party use of certificates issued by external PKIs." It also states that "[t]he Director, DoD PKI Program Management Office, as defined by the Assignment of PMO Responsibilities for the DoD PKI PMO [PKI PMO Responsibilities], shall...[m]anage all tasks involved in the requirements for using external PKIs by the Department of Defense including... [d]eveloping an external interoperability plan for evaluating and recommending external PKIs for approval by the ASD(NII)/DoD CIO."

In March 2007 the Identity Protection and Management Senior Coordinating Group (IPMSCG), chartered the External Interoperability Working Group (EIWG) to review external Public Key Infrastructure requests for interoperability with the DoD and make recommendations about PKI interoperability policy and implementation issues to the DoD PKI Policy Management Authority (PMA).

1.2 PURPOSE

This EIP identifies the actions needed to validate the criteria that are stipulated in the attachment to the [DoD CIO Memo] to support interoperability with External PKIs and to support trust between the DoD PKI and External PKIs. External PKIs shall not be considered approved for use until all steps identified in this EIP have been accomplished.

1.3 DOCUMENT OVERVIEW

This document provides brief descriptions of PKIs operated by the DoD, including the DoD PKI, the ECA PKI, the DoD Interoperability Root, and the CCEB Root. It outlines the process for external PKIs to achieve interoperability with the DoD PKI.

Appendices to this document provide additional information as follows:

Appendix A contains a list of referenced documents.

Appendix B contains the Mission or Business Need Form.

Appendix C contains the MOA template.

2 DOD PKI OVERVIEW

This section provides a brief overview of the DoD PKI, the ECA PKI, and the Interoperability Root that the DoD uses to interoperate with the Federal Bridge.

2.1 DOD PKI

The DoD PKI is a hybrid PKI with Root Certificate Authorities (CA) hosted by NSA and subordinate CAs hosted by DISA. The DoD PKI has centralized management of components and distributed registration. The core components of the DoD PKI are centrally funded using DoD appropriated funds, and registration and other requirements are funded by the Combatant commands, Military Departments, and agencies of the DoD. The DoD PKI provides certificates for subscribers operating on DoD networks, including the NIPRNET and SIPRNET. [DoDI 8520.2] defines users eligible to receive certificates from the DoD PKI as “DoD active duty Uniformed Services personnel, members of the Selected Reserve, DoD civilian employees, and personnel working on site at DoD facilities using DoD network and e-mail services.”

The DoD PKI supports certificates it issues to DoD eligible users on Common Access Cards (CAC). The DoD PKI also supports software-based certificates it issues to both human users and infrastructure components such as web servers and network components. Finally, the DoD PKI supports certificates it issues on alternative hardware tokens as approved by the DoD CIO.

Certificates issued to human users have three types, identity, signature, and encryption. Private keys associated with encryption certificates are escrowed by the DoD PKI, and can be retrieved, if required, either by the entity identified in the certificate or by an authorized third party.

The DoD PKI provides revocation status information for all of its non-expired certificates. Revocation status is provided by each CA in the form of a Certificate Revocation List (CRL). Because the large size of CRLs issued by DoD PKI CAs, the DoD PKI also provides the Robust Certificate Validation Service (RCVS), which responds to revocation status requests using the On-line Certificate Status Protocol (OCSP).

As stated in the "X.509 Certificate Policy for the United States Department of Defense" [DoD CP], DoD PKI certificates may only be used for transactions related to DoD business. The DoD PKI supports multiple assurance levels, which are intended for use based upon the required level of trust. The DoD PKI supports requirements to use digital certificates for authentication to DoD networks and DoD private web servers, for digitally signing data, documents or messages and for encrypting data that is in transit or at rest..

2.2 DOD EXTERNAL CERTIFICATION AUTHORITY (ECA) PKI

[DoD CIO Memo] states that "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. DoD ECA Medium Hardware assurance certificates are comparable to DoD Medium Assurance Hardware certificates issued on the Common Access Card (CAC). DoD ECA Medium assurance certificates are comparable to DoD Medium Assurance certificates. DoD ECA Medium Token Assurance certificates are comparable to DoD Medium Assurance certificates, and may be used where the additional security of a hardware token is desired even though the keys are generated in software . Application owners should consider the Object ID (OID) of the certificate when making access control decisions based on the authenticated identity asserted by any DoD ECA certificate."

The ECA PKI is a hierarchical PKI with a Root CA managed by NSA and subordinate CAs owned and operated by commercial entities. The requirements of the ECA PKI are contained in the "Certificate Policy for External Certification Authorities" [ECA CP]. The use of ECA certificates by DoD systems is encouraged when communicating with entities outside of the DoD, such as off-site support contractors that don't have access to DoD approved, third party PKI credentials. The ECA program assists system managers in meeting the Defense-In-Depth Strategy by providing a mechanism to identify support contractors and other non-DoD personnel via certificates that are issued and maintained under rigorous practices similar to those used by the DoD PKI itself.

The DoD Certificate Policy Management Working Group has determined that the ECA Medium/Medium Token and Medium Hardware Assurance certificates provide protection equivalent to the DoD Medium and Medium-Hardware Assurance level requirements respectively. This means that DoD systems that can accept DoD Medium and/or Medium Hardware certificates can also accept ECA Medium/Medium Token and/or Medium Hardware certificates used to support any PKI-based capability (user authentication, digital signature or encryption).

Table-1: Assurance Level Mapping from DoD to ECA

DoD CP	ECA CP
Medium Assurance	Medium Assurance
Medium Assurance	Medium Token
Medium Assurance Hardware	Medium Hardware Assurance
High	N/A

Each ECA vendor/operator is required to submit a Certificate Practice Statement (CPS) that is determined to meet the [ECA CP] requirements prior to the issuance of a subordinate CA certificate to that ECA vendor/operator. Root CA operations are managed by the DoD PKI PMO. ECA operations are funded by commercial entities. ECA vendors may charge fees to subscribers. Any commercial entity that successfully completes the ECA application process may become an ECA.

ECA operators are required to meet all the requirements of the ECA CP including the certificate issuance and CRL profile requirements. These profiles have been modeled after the DoD certificate and CRL profiles. ECA operators are also required to publish CRLs. These similarities to the DoD PKI ensure that the use of ECA certificates does not pose technical interoperability issues and provides a mechanism for response to ECA certificate compromise. In addition to ECA vendor repositories, ECA CA certificates and CRLs can be downloaded from the DoD Global Directory Service (GDS) at https://crl.chamb.disa.mil,

The ECA Root CA has been cross-certified with the Federal Bridge at medium assurance. The [ECA CP] is being updated so that it can also cross-certify with the Federal Bridge at medium hardware assurance. This cross-certification is one way, the Federal Bridge has issued a cross-certificate to the ECA Root CA, but the ECA Root CA has not issued a cross-certificate to the Federal Bridge.

2.3 DOD PKI INTEROPERABILITY ROOT

The DoD PKI Interoperability Root, managed by NSA, is a specialized root CA designed for interoperability with members of the Federal Bridge. Figure 1 shows the relationship and cross-certification directions between the Interoperability Root and the Federal Bridge.

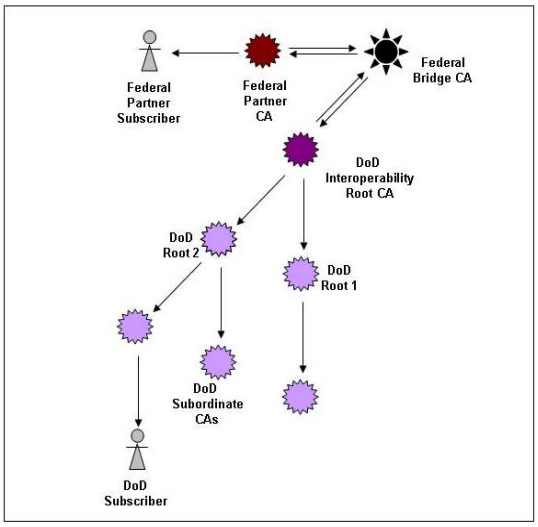

Figure 1 DoD Interoperability Root and the Federal Bridge

The Interoperability Root is two-way cross-certified with the Federal Bridge CA (FBCA) at Medium Hardware level of assurance and will only be used to generate cross certificates. The Interoperability Root issued cross-certificates to DoD Root1 and DoD Root2, and is one-way cross-certified with both DoD Roots.

2.4 CCEB ROOT

DoD has established the Combined Communications Electronics Board (CCEB) Root CA under a separate process from that specified in this EIP. The CCEB Root is designed for interoperability with CCEB partners. The CCEB Root is currently operating using a separate root CA from the DoD Root and a separately negotiated memorandum of agreement (MOA). The CCEB Root is one-way cross-certified with the DoD and has issued cross-certificates to DoD Root1 and DoD Root2. The CCEB Root is two-way cross-certified with the other CCEB partners.

3 PROCESS FOR ESTABLISHING INTEROPERABILITY WITH THE DOD PKI

For purposes of this EIP, entities desiring to use their PKI certificates to interoperate with the DoD will be referenced throughout this document by one of the following categories:

1. **Category I:** U.S. Federal agency PKIs
2. **Category II:** Non-Federal Agency PKIs cross certified with the FBCA or PKIs from other PKI Bridges that are cross certified with the FBCA
3. **Category III:** Foreign, Allied, or Coalition Partner PKIs or other PKIs

3.1 CATEGORY I: U.S. FEDERAL AGENCY PKI

[DoD CIO Memo] states that "Certificates issued by U.S. Federal Agency PKIs are approved for use within DoD for authenticating to DoD web sites and for digital signature or encryption upon successfully completing interoperability testing, and if either of the following are true:

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 and asserts either the Medium Hardware

Assurance (*id-fpki-certpcy-mediumHardware*) or High Assurance. (*id-fpki-certpcy-highAssurance*) Object ID (OID)

2. The certificate was issued by a certified PKI Shared Service Provider (SSP) operating under the x.509 Certificate Policy for the Common Policy Framework and asserts either the *id-fpki-common-hardware* or the *id-fpki-common-authentication* OID.

The process for establishing interoperability with Federal Agency PKIs (Category I) is outlined in the following three sections of this EIP:

Step 1: ***Application Submission (Section 4)***

Step 2: ***Interoperability Testing (Section 6)***

Step 3: ***Acceptance and Implementation (Section 9)***

3.2 CATEGORY II: NON-FEDERAL AGENCY PKIs

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:

1. The certificate was issued by a PKI that has a valid path to the FBCA at the Medium Hardware level of Assurance.
2. A DoD sponsor has established and defined a business or mission need to interoperate with external PKIs.
3. JITC has successfully completed interoperability testing of the PKI.
4. A Memorandum of Agreement (MOA) has been signed by both the DoD and the non-Federal Agency PKI.

The JITC Test Plan is available for review at the following URL:
http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html

Appendix C contains a reference Memorandum of Agreement.

The process for establishing interoperability with Non-Federal Agency PKIs (**Category II**) is outlined in the following four sections of this EIP:

Step 1: ***Application Submission (Section 4)***

Step 2: ***Validate Business or Mission Need (Section 5)***

Step 3: ***Interoperability Testing (Section 6)***

Step 4: ***Acceptance and Implementation (Section 9)***

3.3 CATEGORY III: FOREIGN, ALLIED, COALITION PARTNER, OR OTHER 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:

1. A Combatant Command, DoD Service or DoD Agency system or application has identified that they require interoperability with the identified PKI and has established a business case or mission need to authenticate those external PKI certificates.
2. The PKI Certificate Policy has been mapped to the DoD PKI Certificate Policy in accordance with the DoD process. There is no documented process for mapping, however, previous mappings of the DoD PKI to the Federal Bridge will serve as the model.
3. The DoD Certificate Policy Management Working Group (CPMWG) or its designated authority has not identified critical risks to the EIWG that would prevent certificate validation or authentication at all levels of assurance.
4. JITC has successfully completed 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.
5. The EIWG has reviewed the business or mission need, the results of the CP mapping, the results of the JITC testing, and the PKI Root CA certificate is added to the DoD trusted external PKI repository."
6. A Memorandum of Understanding (MOU) has been signed by the DoD PMA and the Foreign, Allied, Coalition or other PKI.

The process for establishing interoperability with Foreign, Allied, or Coalition Partner PKIs or other PKIs (**Category III)** is outlined in the following six sections of this EIP:

Step 1: ***Application Submission (Section 4)***

Step 2: ***Validate Business or Mission Need (Section 5)***

Step 3: ***Interoperability Testing (Section 6)***

Step 4: ***Policy Mapping (Section 7)***

Step 5: ***Compliance Audit Review (Section 8)***

Step 6: ***Acceptance and Implementation (Section 9)***

Note: DoD will interoperate with CCEB partners via the CCEB Root as discussed in Section 2.4.

4 APPLICATION SUBMISSION

Categories I, II, and III

The EIWG will be the primary point of contact for external PKIs requesting interoperability with the DoD.

1. The process is initiated by the submission of a request for interoperability to the EIWG via email to ExternalPKI.Interoperability@osd.mil.

   The application submission from Category I, II, III PKIs must include the following:

3. Name of requesting entity (i.e. Federal Agency for Category I)
4. Name and contact information (phone number, email address, and address) for a primary point of contact (POC), and a secondary POC
5. PKI certificate provider agency name or organization name (i.e. Federal Agency operated, HSPD-12/PIV Shared Service Provider or DoD approved third party credential service provider)
6. PKI certificate provider name of person in charge of issuance and contact information (phone number, email address, and address)

   Category II and Category III PKIs must also provide the following:

7. Status of cross-certification with the Federal Bridge (date, assurance levels)
8. Assurance level(s) supported by the PKI
9. Sponsoring DoD Service or Agency entity or application
10. DoD sponsor's name and contact information (phone number, email address, and address) for a primary POC and a secondary POC
11. Brief description of business case or mission need (see Section 5 for additional details)

    Category III PKIs must also provide the following:

1. The Entity Certificate Policy and Certificate Practice Statement(s)

2. The EIWG will schedule a time on the next EIWG agenda to process the application.

3. The EIWG will review the application and provide DoD's determination about business or mission need to the primary or secondary POC.

5 VALIDATE BUSINESS OR MISSION NEED

Categories II and III

The EIWG must make an initial determination about the validity of the requirement and the capability of the external PKI to meet DoD requirements.

1. Requesting entities from Categories II and III are requested to submit the Business Case or Mission Need Form (Appendix B)
2. The EIWG will review the analysis of the need, status, and risk information supplied in the Business or Mission Need Form and make a preliminary determination of whether a valid need exists to interoperate with the external PKI. A valid need exists if there is a functional community, including systems, that can benefit from using certificates issued by the external PKI and the DoD can potentially be better served by use of this external PKI than by use of already approved PKIs, or there is an overriding mission or business need or other requirement justifying the need to interoperate with the external PKI. The potential level of risk introduced by interoperating with the external PKI must be acceptable.
3. The EIWG will contact the DoD sponsor and request confirmation that they acknowledge and accept the risk associated with accepting the external PKI certificates, and are making the necessary system modifications.

6 INTEROPERABILITY TESTING

Categories I, II, and III

Certificates issued by external PKIs shall be tested by the Joint Interoperability Test Center (JITC) testing to prove that they are technically interoperable with DoD systems, including web servers and email clients, and that certificate revocation information can be obtained by these DoD systems.

The JITC DoD PKI Interoperability Test Plan is located at http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html.

1. Requesting entities from Categories I, II and III must submit the following documentation:
   a. Entity's PKI architecture, including all Certificate Authorities (CAs) within the PKI
   b. List of CAs that have any other trust relationships with the PKI's CAs, such as cross-certificates with other PKIs.
   c. X.500/LDAP directory relationships and hierarchical DN relationships, if any, with other PKIs
   d. Certificate profiles of certificates issued by the PKI, including all certificate object IDs issued by any entity PKI CA
2. The EIWG will initiate the request for interoperability testing. External PKIs will provide the documentation listed in 1a.-1d to JITC.
3. JITC will contact requesting entity's POC to coordinate interoperability testing.

4. JITC will conduct interoperability testing and document results.
5. The EIWG will review the results of the JITC testing.

7 POLICY MAPPING

Category III

A policy analysis will be conducted to determine if the external PKI's CP meets DoD requirements as defined in the [DoD CP]. To aid in making these policy comparisons, IETF RFC 3647, "Certificate Policy and Certification Practices Framework" [RFC 3647], provides an outline for certificate policy documents. The external PKI is requested to submit a CP that conforms to [RFC 3647] or provides a mapping showing where the requirements identified in each section of the CP template in [RFC 3647] are addressed.

If the external PKI supports escrow of private keys, policies and procedures related to key escrow and recovery must also be provided. These policies and procedures will be analyzed against the "Key Recovery Policy for the United States Department of Defense" [DoD KRP].

The basic process for policy mapping is as follows:

1. Requesting entities from Category III must submit the following documentation:
   a. Certificate Policy (CP) in [RFC 3647] format,
   b. Policies and procedures related to key escrow and recovery,
   c. Principal CA Certification Practice Statements (CPS),
   d. Signed third party Auditor Letter of Compliance summarizing the results of an audit of its PKI operations that attests to the applicant's claim that its PKI is operated in accordance with its CPS, and that the CPS implements the requirements of the CP,
   e. Other documentation or alternative process as approved by DoD PKI PMA needed to show evidence of comparability between the applicant PKI and the requirements of the DoD PKI.
2. A Certificate Policy Management Working Group (CPMWG) analyst performs an initial compliance analysis of the external PKI CP against the requirements in the DoD CP.
3. The compliance analysis and external PKI CP are provided to the CPMWG membership for review and comment.
4. Comments are collected and consolidated. Comments may also be vetted by the CPMWG analyst and CPMWG co-chair to resolve any that are not compliance-related.
5. CPMWG reviews CPS(s), audit report(s), and any other relevant documentation.
6. Comments are provided to the external PKI for response. The external PKI may choose to modify their CP in response to the comments. If so, the external PKI submits a revised CP and the process is repeated.
7. A final compliance analysis report is prepared by the CPMWG, identifying remaining compliance-related issues with the external PKI CP with a recommendation by the CPMWG as to whether these outstanding comments constitute an unacceptable risk for the DoD to rely on certificates issued by the external PKI at the requested level of assurance.

8. The CPMWG provides the final compliance analysis report to the PKI PMO and the EIWG. The PKI PMO may provide the compliance analysis report to the DoD PKI PMA.

8 COMPLIANCE AUDIT REVIEW

Category III

The purpose of a compliance audit is to verify that the CA has an operating PKI system to assure the quality of the CA services that it provides, and that the system complies with all of the requirements of its CP and its CPS.

1. The requesting entity must submit its Auditor Letter of Compliance completed by an independent third party auditor. The auditor must have competence in the field of security compliance audits of Information Technology (IT) systems, must be thoroughly familiar with the entity's CPS, and have expertise in information security, cryptography and PKI.
2. The Auditor Letter of Compliance will be reviewed by the CPMWG. The CPMWG will verify that the signed third party Auditor Letter of Compliance summarizes the results of an audit of its PKI operations, attests to the applicant's claim that its PKI is operated in accordance with its CPS, which implements the requirements of the CP.
3. If the compliance audit is not sufficient, the CPMWG will provide feedback to the requesting entity.
4. The requesting entity may choose to submit an updated Auditor Letter of Compliance for review.
5. The EIWG makes a final recommendation to the PKI PMO concerning the acceptability the compliance audit.

9 ACCEPTANCE AND IMPLEMENTATION

The ASD (NII)/DoD CIO is responsible for approving the use of external PKIs by DoD relying parties. This decision is made based upon the recommendation of the EIWG in coordination with the DoD PKI PMO and the DoD Office of the General Counsel.

Use of Category I certificates will continue to be approved and accepted by DoD systems as long as the entity PKI has a valid cross-certificate issued from the Federal Bridge.

Use of Category II certificates will continue to be approved and accepted by DoD systems as long as the entity PKI has a valid cross-certificate(s) establishing a trust path to the Federal Bridge and continues to meet the terms of the Memorandum of Agreement (MOA) between the entity PKI and the DoD.

Use of Category III certificates will continue to be approved and accepted by DoD systems as long as an MOU is in place and effective, the entity PKI meets the terms of that MOU, submits an annual compliance audit report that is satisfactory to the EIWG, and submits updated documentation as required.

DoD will maintain a website in the Defense Knowledge On-Line portal that hosts all Principal CA certificates from all approved external PKIs at https/:www.us.army.mil/suite/page/571419.

Note: An external PKI successfully meeting all criteria for obtaining “approved” status, does not imply that all DoD applications will authorize access based on authentication of that PKI’s certificates.

10 CONTACT INFORMATION

This External Interoperability Plan (EIP) is maintained by the DoD External Interoperability Working Group (EIWG).

Email: ExternalPKI.Interoperability@osd.mil

APPENDIX A

REFERENCES

DoD Chief Information Officer (CIO) Memorandum dated, “Approval of External Public Key Infrastructures”, July 22, 2008 [DoD CIO Memo]

Department of Defense Directive 8500.1, “Information Assurance (IA)” [DoDD 8500.1]

ASD(C3I) Memorandum, “Assignment of Program Office Responsibilities for the Department of Defense Public Key Infrastructure (PKI)”, April 9, 1999, [PKI PMO Responsibilities]

DoD Chief Information Officer (CIO) Memorandum, “Compliance and Review of Logical Access Control in Department of Defense (DoD) Processes”, January 24, 2007, [Logical Access Memo]

DoD Instruction 8520.2, “Public Key Infrastructure (PKI) and Public Key (PK) Enabling” [DoDI 8520.2]

“X.509 Certificate Policy for the United States Department of Defense” [DoD CP]

“Certificate Policy for External Certification Authorities” [ECA CP]

IETF RFC 3647, “Certificate Policy and Certification Practices Framework” [RFC 3647]

“Key Recovery Policy for the United States Department of Defense” [DoD KRP]

Test Plan for Department of Defense (DoD) Public Key Infrastructure (PKI) Interagency/Partner Interoperability, Version 1.0.3,, 27 August 2008,
(available at: http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html)

APPENDIX B

BUSINESS OR MISSION NEED FORM

The EIWG will base the preliminary mission or business need decision on the cumulative answers to the following questions. These questions are included in the interoperability request template. The EIWG will also evaluate the information and answers provided during briefings from representatives of an external PKI and their DoD sponsor.

1. Does the DoD need to interoperate with this external PKI to meet DoD operational requirements?
2. Should the DoD PKI interoperate with the external PKI at a CA to CA level or would including the external PKI in application trust lists or via gateways be more appropriate?
3. Does the benefit garnered from interoperability with the external PKI warrant the interoperability?

Need for DoD to Interoperate

Identify the need for DoD interoperability with the external PKI by requiring answers to the following questions.

- What system(s) have been identified that will benefit near-term from interoperability with the external PKI?
- Are these systems sponsoring the external PKI?
- What is the timeline for the systems to be able to rely on certificates issued by the external PKI?
- Are there other potential systems that can benefit in the future from interoperability with the external PKI?
- How many users have or will be obtaining certificates from the external PKI for piloting activities? For the fully approved (production) environment?
- Can these users obtain certificates from a currently approved external PKI, such as the ECA PKI?

Status of the External PKI

The status of the external PKI will be determined by answering the following questions.

1. What is the community served or intended to be served by the external PKI (note this is the entire community served, not just members of the community that have a need to interoperate with the DoD)?
2. What is the operational status of the external PKI (including whether the PKI is operational, when the PKI became operational, and how many current subscribers it has)?
3. Has the external PKI undergone an independent compliance audit within the past year with results that indicate overall compliance with its documentation?

4. How is the external PKI governed (who is the PMA, what authority does the PMA have, what bodies within the organization provide governance, monitoring and oversight of the PKI operation)?

Risks to the DoD

Approving interoperability with an external PKI creates risk for the DoD. Determining the risk includes answering the following questions.

1. What does the DoD sponsor or external PKI expect will be the estimated cost to the DoD to implement interoperability with the external PKI?
2. Is this PKI new, or has this PKI established credibility with other PKIs through bridges or other cross-certification agreements that exhibit trust relationships for a period of time?
3. What is the impact to the DoD PKI if the external PKI is approved?
4. What is the impact, if any, to existing approved external PKIs if this external PKI is approved?
5. What are the long-term requirements for maintaining interoperability with the external PKI?

APPENDIX C

MEMORANDUM OF AGREEMENT (MOA)

MEMORANDUM OF AGREEMENT

BETWEEN

THE DEPARTMENT OF DEFENSE

POLICY MANAGEMENT AUTHORITY

AND

<Insert the company or organization name here>

THE EXTERNAL PKI

WHEREAS, the External PKI desires to supply Certificates to non-Department of Defense (DoD) entities and personnel desiring to use those certificates to interact with DoD Relying Parties; and

WHEREAS, the DoD Policy Management Authority (PMA) recognizes the need for non-DoD entities and personnel to interoperate with DoD Relying Parties for the purpose of conducting business electronically with the DoD.

NOW, THEREFORE, THE PARTIES HEREBY AGREE AS FOLLOWS:

1) Purpose.

This Memorandum of Agreement (MOA) describes the terms and conditions by which certificates issued by the External PKI can be used to interact with DoD Relying Parties. The External PKI shall operate a PKI defined by a Certificate Policy (CP) governing the External PKI's operation which has been mapped as complying with the requirements defined in the Federal Bridge Certification Authority (FBCA) Certificate Policy (CP) at Medium Hardware Assurance, or mapped to another Bridge, which itself has been mapped as complying with the requirements defined in the FBCA CP at Medium Hardware Assurance.

2) References.

a) X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)

b) Criteria And Methodology For Cross-Certification With The U.S. Federal Bridge Certification Authority (FBCA) or Citizen and Commerce Class Certification Authority (C4CA)

c) External PKI Certificate Policy (CP)
< insert title, date and version number of applicable external PKI CP and URL if available>

d) External PKI Certificate Practice Statements (CPS)
< insert title, date and version number of applicable external PKI CPS(s) and URL is available>

e) ASD(NII)/DoD CIO memo, "Approval of External PKIs", dated 22 July 2008
URL:
http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html

3) Authority.

The Electronic Signatures in Global and National Commerce Act (Public Law 106-229) and the Government Paperwork Elimination Act (title XVII of Public Law 105-277).

4) Background.

The FBCA facilitates trust between disparate PKIs by allowing the creation of trust paths between entity-specific PKI domains, so that digital certificates issued by CAs in one domain can be honored with an appropriate level of trust in a different domain. DoD cross-certified with the FBCA at Medium Hardware Assurance in June 2007. The External PKI named in this MOA
<cross-certified with the FBCA at Medium Hardware Assurance in <insert Month and Year>>
Or
< is cross-certified with the <insert the PKI Bridge Certification Authority name> which itself has been mapped as complying with the requirements as defined in the FBCA CP at Medium Hardware assurance in <insert Month and Year>>

In accordance with the procedure set forth in Reference (e), the Parties intend to facilitate a trust relationship as outlined in this MOA.

5) Responsibilities.

a) By entering into this MOA, the External PKI will**:**

i) Operate in accordance with its CP and CPS.

ii) Maintain its mapping status with regards to the Federal Bridge at Medium Hardware Assurance.

iii) Successfully complete technical interoperability testing by the DoD Joint Interoperability Test Command (JITC).

iv) Make all CA certificates available to the DoD for posting in the approved CA certificate store.

v) Make all Certificate Revocation Lists (CRLs) available to DoD Relying Parties, preferably via HTTP.

vi) Give notice of any changes in the External PKI CA architecture or change in status of any CAs within the External PKI to DoD PMO and DoD Relying Parties, to the extent possible.

b) By entering into this MOA, the DoD PMA will:

i) Operate in accordance with its CP and CPS(s).

ii) Publish the External PKI's CA certificates in the approved DoD CA certificate store.

iii) Maintain, to the extent possible, its mapping status to the Federal Bridge at the Medium Hardware Assurance level or higher.

iv) Make all DoD CA certificates available to the External PKI for posting.

v) Make CRLs available to the External PKI.

vi) Give notice of any changes in the DoD CA architecture or change in status of any CAs within the DoD PKI to the External PKI, to the extent possible.

6) <u>Agreements</u>.

a) This MOA is enforceable only by the parties and is binding upon the parties, by and through their officials, agents, employees, and successors. No person or entity is intended to be a third party beneficiary of the provisions of this MOA for purposes of any civil, criminal, or administrative action, and accordingly, no person or entity may assert any claim or right as a beneficiary or protected class under this MOA in any civil, criminal, or administrative action. Similarly, this MOA does not authorize, nor shall it be construed to authorize, access to any documents by persons or entities not a party to this MOA.

b) The External PKI understands that neither DoD nor the Federal Government will compensate it for the operation of its PKI (unless a specific Federal agency sponsors a subscriber, in which case compensation may be owed in accordance

with the operable subscriber agreement).

7) Termination For Cause.

This MOA may be terminated for cause by the DoD PMA. Should the External PKI not comply with its obligations under its CP and CPS, should the External PKI's relationship with the Federal Bridge or other Bridge be terminated, should the External PKI fail an audit or should the DoD PMA become aware of any other issue that places the security of the security of the External PKI in question, DoD PMA may remove the External PKI CA from the approved DoD CA certificate store and suspend use of the External PKI certificates. Justification for such action includes material violations of this MOA or the External PKI's CP or CPS, such as misrepresenting required identity verifications or intentionally failing to comply with the Responsibilities listed in Section 5 of this document. The written notification will be provided and include the reason(s) for the removal of the External PKI CA from the trust store and provide the External PKI with one hundred and twenty (120) calendar days to cure any alleged violation or non-compliance before this MOA is terminated. If the DoD PMA determines that the issues that led to the removal of the External PKI CA from the DoD trust store have been resolved, the External PKI CA must be replaced in the DoD CA certificate store. In the event that the issues cannot timely be resolved, termination of this MOA is the sole remedy of DoD PMA for any alleged violation or non-compliance by the External PKI of the terms of this MOA.

8) Voluntary Termination.

a) The External PKI may choose to terminate this MOA and discontinue operation of its PKI for its convenience and in its sole discretion, or may choose to no longer have its certificates approved for use by DoD Relying Parties, at any time, by giving written notice to the DoD PMA not less than one hundred (120) calendar days prior to the date such termination is to be effective.

b) The DoD PMA, for its convenience and in its sole discretion, may choose to terminate this MOA and terminate approval for DoD Relying Parties accepting certificates issued by the External PKI at any time by giving written notice to the External PKI not less than one hundred (120) calendar days prior to the date such termination is to be effective.

c) Notwithstanding anything herein to the contrary, any termination of this MOA shall not provide a cause of action against any party to this Agreement. Neither the DoD PMA nor the External PKI shall be liable for any costs or damages that may result from a termination of this MOA.

9) Term.

This MOA will remain in effect for a period of six (6) years from the last date of signature of this agreement. The parties shall perform an annual review of the terms

of this MOA to assure that all information is current.

10) Modification and Renewal.

If at any time, any party to this MOA desires to modify it for any reason, that party shall notify the other Party in writing of the proposed modification and the reasons for said modification(s). No modification shall occur unless there is written acceptance by both parties hereto.

11) Liability.

Termination is the sole remedy for violation of the terms of this MOA. Each Party to this MOA shall hold the other harmless with respect to any liability arising out of the operation of the External PKI. This MOA is entered into for the convenience of the Parties and shall not give rise to any cause of action by the Parties hereto or by any third party, such as subscribers of private keys. In no event shall the DoD PMA be liable for the payment of any subscription or service fees paid to the External PKI.

12) Disputes.

The Parties agree to resolve all claims, disputes, and other matters in question arising out of this MOA, by good faith negotiations. Initial negotiations shall begin at the lowest level capable of problem resolution. In the event that the parties cannot resolve the dispute at a lower level, the final arbiter of the dispute will be the DoD PMA. The External PKI agrees to be bound by the DoD PMA's final decision.

13) Governing Law.

The construction, validity, performance and effect of this Agreement shall be governed by United States Federal law.

14) Disclaimer.

This MOA shall constitute the entire Agreement of the parties. No prior or contemporaneous communications, oral or written, or prior drafts shall be relevant for purposes of determining the meaning of any provisions herein in any dispute or any other proceeding.

15) Severability.

If any terms or provisions of this MOA prove to be invalid, void, or illegal, they shall in no way impair or invalidate any other terms or provisions herein, and the remaining terms and provisions shall remain in force.

16) Successors.

In the event that either Party reorganizes or merges with another organization, or otherwise operates under new organizational control, this MOA shall not apply to the succeeding organization(s) unless amended in writing.

17) Effective Date.

This MOA is effective upon signature by both parties hereto and shall remain in effect until termination or expiration.

18) **Confidentiality.**

The Parties shall keep in confidence and shall not disclose to any person or entity not bound by this MOA, or make unauthorized use of, any business confidential or proprietary information provided by the External PKI. The DoD PMA shall use the same degree of care to protect the External PKI's information as it uses to protect its own similar class of information. Termination of this MOA shall not relieve the Parties from obligations to continue to protect against the disclosure of such confidential or proprietary information provided by the External PKI.

19) **Nature of Agreement**– This agreement does not express or imply any commitment to purchase or sell goods or services or conduct of any business transaction.

20) Signatures

_____	_____
(PMA of the External PKI)	(DoD PMA)
_____	_____
(Date)	(Date)
_____	_____
(Printed Name)	(Printed Name)
_____	_____
(Title)	(Title)

APPENDIX D

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

JUL 2 2 2003

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 <u>either</u> 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).

B.2. The certificate was issued by a certified PKI Shared Service Provider[1] (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

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.

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.

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 NACI.
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.

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.

GLOSSARY

ASD(NII/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/ DoD Chief Information Officer
CA	certification authority
CAC	common access card
CCEB	Combined Communications Electronics Board
CP	certificate policy
CPMWG	Certificate Policy Management Working Group
CPS	certificate practice statement
CRL	certificate revocation list
EIP	External Interoperability Plan
EIWG	External Interoperability Working Group
FBCA	Federal Bridge Certification Authority
GDS	Global Directory Service
IPMSCG	Identity Protection and Management Senior Coordinating Group
JITC	Joint Interoperability Test Center
MOA	memorandum of agreement
PKI	public key infrastructure
PMA	Policy Management Authority
OID	object identifier
OCSP	on-line certificate status protocol
RCVS	Robust Certificate Validation Service
SSP	Shared Service Provider