Department of Defense
INSTRUCTION

NUMBER 8520.02
May 24, 2011

ASD(NII)/DoD CIO

SUBJECT: Public Key Infrastructure (PKI) and Public Key (PK) Enabling

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Reissues DoD Instruction (DoDI) 8520.2 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5144.1 (Reference (b)) to establish and implement policy, assign responsibilities, and prescribe procedures for developing and implementing a DoD-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption.

b. Prescribes DoD PKI and PK-enabling activities consistent with the policy established in DoDD 8500.01E (Reference (c)) and DoDI 1000.13 (Reference (d)).

c. Supplements the implementing guidance provided in DoDI 8500.2 (Reference (e)).

d. Prescribes DoD PKI activities on the Secret Internet Protocol Router Network (SIPRNET) consistent with requirements stated in References (c) and (e).

e. Incorporates and cancels DoDD 8190.3 and Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) memorandums (References (f), (g), and (h), respectively).

2. APPLICABILITY

a. This Instruction applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the “DoD Components”).

(2) All unclassified and classified DoD information systems and networks (e.g., Non-classified Internet Protocol Router Network (NIPRNET), SIPRNET, Defense Research and Engineering Network (DREN), Secret Defense Research and Engineering Network (SDREN)), web servers, and e-mail systems).

(3) All users accessing unclassified and classified DoD information systems (e.g., DoD web-based systems, DoD websites, DoD web servers) and networks (e.g., NIPRNET, SIPRNET, DREN, SDREN).

b. This Instruction does NOT apply to sensitive compartmented information and other information systems operated within the DoD that fall under the authority of the Director of National Intelligence in accordance with Intelligence Community Directive 503 (Reference (i)). This Instruction also does not apply to Top Secret collateral systems, special access programs, and stand-alone networks with no connection to the Global Information Grid (GIG).

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. The DoD shall implement a DoD-wide PKI to maintain the certificate lifecycle, including, but not limited to, issuance, suspension, and revocation. The DoD shall issue certificates to DoD PKI Certificate Eligible Users in accordance with "United States Department of Defense X.509 Certificate Policy" (Reference (j)). The DoD PKI also shall support requirements for group, role, information systems, device, and code signing certificates. The DoD PKI shall provide first and third party key recovery for private keys associated with encryption certificates.

b. The DoD shall enable DoD information systems to use PKI for digital signature and encryption as specified in this Instruction. The DoD shall enable DoD information systems to use DoD-approved PKIs for authentication in accordance with DoDI 8520.03 (Reference (k)).

c. The DoD shall only rely on certificates that are issued by the DoD PKI or by a DoD-approved PKI for authentication, digital signature, or encryption. External PKIs are approved for use by the ASD(NII)/DoD CIO. The process for recommending approval for external PKIs is outlined in the DoD External Interoperability Plan (Reference (l)). DoD mission partners shall use certificates issued by the DoD External Certification Authority (ECA) program or a DoD-approved PKI, when interacting with the DoD in unclassified domains. DoD ECA PKI and External PKI certificates are not used in the DoD classified domain.

d. The DoD shall establish and maintain a cross certification with the Federal PKI to comply with Federal Information Processing Standards Publication 201-1 (Reference (m)). The DoD shall facilitate the issuance of any new PKI certificates necessary to comply with Federal or Office of Management and Budget issuances or mandates and be consistent with DoD

implementation plans. DoD PKI shall comply with Reference (m) for mandatory certificates issued on the Common Access Card (CAC).

e. PKIs operating under the purview of the DoD (e.g., DoD ECA, DoD Coalition PKI) are approved for use for their intended purpose and environment. The types of external PKIs that can be approved for use in the DoD are described in this Instruction. Implementation and use of DoD-approved PKI certificates for identity authentication is described in Reference (k).

f. DoD digital signers of mobile code shall use DoD-issued code-signing certificates to allow validation of both the integrity of the code and the authenticity of its source in accordance with DoDI 8522.01 (Reference (n)).

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

8. EFFECTIVE DATE. This Instruction is effective upon its publication to the DoD Issuances Website.

Teri M. Takai
Principal Deputy Assistant Secretary of Defense
For Networks and Information Integration/
DoD Chief Information Officer

Enclosures
1. References
2. Responsibilities
3. Implementation Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Instruction 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," April 2004 (hereby cancelled)
(b) DoD Directive 5144.1, "Assistant Secretary of Defense for Network and Information Integration / DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
(c) DoD Directive 8500.01E, "Information Assurance (IA)," April 23, 2007
(d) DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," May 2, 2011
(e) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(f) DoD Directive 8190.3, "Smart Card Technology," August 31, 2002 (hereby cancelled)
(g) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "Guidance and Provisions for Developing Department of Defense (DoD) Component's Public Key Enabling (PKE) Policy Compliance Waiver Process," August 5, 2002 (hereby cancelled)
(h) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "Approval of Alternate Logon Token," August 14, 2006 (hereby cancelled)
(i) Intelligence Community Directive 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," September 2008
(j) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, "United States Department of Defense X.509 Certificate Policy," current edition
(k) DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 13, 2011
(l) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, "DoD External Interoperability Plan," August 26, 2010
(m) Federal Information Processing Standards Publication 201-1 "Federal Information Processing Standards Publication, Personal Identity Verification of Federal Employees and Contractors," March 2006
(n) DoD Instruction 8552.01, "Use of Mobile Code Technologies in DoD Information Systems," October 23, 2006
(o) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, "Key Recovery Policy for the United States Department of Defense," current edition[1]
(p) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, "External Certification Authority, X.509 Certificate Policy," current edition[2]
(q) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, "Key Recovery Policy for External Certification Authorities," current edition[3]

[1] Available on the SIPRNet at http://iase.disa.rel.smil.mil/pki/pki-guidance.html
[2] http://iase.disa.mil/pki/eca/updates.html
[3] http://iase.disa.mil/pki/eca/documents.html

(r) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, "Coalition Public Key Infrastructure, X.509 Certificate Policy," current edition
(s) Combined Communication-Electronics Board, "CCEB Publication 1010 PKI Cross-Certification Between CCEB Nations," current edition
(t) DoD Directive 5100.03, "Support of the Headquarters of Combatant and Subordinate Unified Commands," February 9, 2011
(u) Committee on National Security Systems Policy No. 25, "National Policy for Public Key Infrastructure (PKI) in National Security Systems," March 2009
(v) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
(w) Committee on National Security Systems Instruction No. 1300, "Instruction for National Security Systems PKI X.509 Certificate Policy Under CNSS Policy No. 25," October 2009
(x) Directive-Type Memorandum 08-003, "Next Generation Common Access Card (CAC) Implementation Guidance," December 1, 2008
(y) Federal Public Key Infrastructure Policy Authority, X.509 Certificate Policy for the Federal Bridge Certification Authority, current edition
(z) Federal Public Key Infrastructure Policy Authority, X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, current edition
(aa) Section 3504, et. seq. of title 44, United States Code (also known as the "Government Paperwork Elimination Act")
(ab) Section 7001, et. seq. of title 15, United States Code (also known as the "Electronic Signatures in Global and National Commerce Act")
(ac) DoD 5200.1-R, "Information Security Program," January 1997
(ad) Chairman of the Joint Chiefs of Staff Instruction 6211.02C, "Defense Information System Network (DISN): Policy and Responsibilities," July 9, 2008
(ae) The Internet Society, "RFC 3647-X.509 Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework," November 2003

ENCLOSURE 2

RESPONSIBILITIES

1. ASD(NII)/DoD CIO. The ASD/NII(DoD CIO), in addition to the responsibilities in section 7 of this enclosure, shall:

a. Manage implementation and evolution of the DoD PKI in accordance with this Instruction and References (c), (d), (e).

b. Update and issue PKI and PK-enabling implementation and maintenance guidance as necessary, including but not limited to:

(1) Providing oversight and guidance for digital signature and encryption requirements.

(2) Ensuring DoD-wide interoperability of digital signature solutions.

c. Serve as the Policy Management Authority for the DoD PKI, delegate this authority as appropriate, and approve these documents, as required:

(1) Reference (j).

(2) Key Recovery Policy for the United States Department of Defense (Reference (o)).

(3) DoD External Certification Authority, X.509 Certificate Policy (Reference (p)).

(4) DoD Key Recovery Policy for External Certification Authorities (Reference (q)).

(5) DoD Coalition Public Key Infrastructure, X.509 Certificate Policy (Reference (r)).

d. Designate an individual to serve as the designated accrediting authority (DAA) for the DoD PKI.

e. Approve or disapprove DoD-wide waivers that affect the DoD PKI.

f. Approve DoD use of hardware tokens other than the CAC for identity, authentication, signature, code signing, group/role, and encryption certificates upon the advice and coordination of the Identity Protection and Management Senior Coordinating Group (IPMSCG).

g. Approve external PKIs for use by DoD relying parties, including:

(1) Providing guidance on the use of certificates issued by PKIs that have been cross-certified by the Federal Bridge Certification Authority (FBCA).

(2) Approving all memorandums of agreement (MOAs) with external PKIs or external PKI certificate providers.

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). The Director, DISA, under the authority, direction, and control of the ASD(NII)/DoD CIO and in addition to the responsibilities in section 7 of this enclosure, shall:

a. Operate and maintain the infrastructures for the DoD PKI and Coalition PKI in coordination with the DoD PKI Program Management Office (PMO).

b. Provide technical consultation, best practices, and technical security implementation guidance to the DoD Components implementing the DoD PKI or the Coalition PKI.

c. Operate and maintain the infrastructure necessary for implementing interoperability with DoD-approved PKIs.

d. Provide technical consultation to, and facilitate testing for, the DoD Components conducting PK-enabling activities.

e. Maintain a repository for posting certification authority (CA) certificates and policy object identifiers (OIDs) for approved external PKIs.

f. Coordinate changes to the PKI infrastructure with the Defense Manpower Data Center CAC issuance infrastructure.

g. Ensure personnel supporting the Defense IA Security Accreditation Working Group (DSAWG) Secretariat have competencies to provide risk acceptance recommendations or decisions over a broad range of information assurance topics and subjects.

3. DIRECTOR, DoD PKI PMO. The Director, DoD PKI PMO, under the authority, direction, and control of ASD(NII)/DoD CIO, shall:

a. Manage the definition, development, deployment, integration, training, and acceptance testing of the DoD PKI.

b. Maintain the currency of References (j), (o), (p), (q), and (r) by conducting a formalized change management process .

c. Approve DoD Component certification practice statements and key recovery practice statements for the DoD PKI, as complying with References (j) and (o).

d. Approve vendor Certification Practice Statements and Key Recovery Practice Statements, in accordance with References (p) and (q).

e. Approve DoD Coalition certification practice statements, in accordance with Reference (r).

f. Ensure the timely availability of CA services, including but not limited to: the recovery of private keys associated with encryption certificates, the retrieval of archived encryption certificates, and the provision of certificate revocation information.

g. Coordinate PKI functional requirements input from the Heads of the DoD Components.

h. Provide guidance to the DoD Components regarding the evolving DoD PKI and Coalition PKI implementations and PK-enabling to ensure consistency across the DoD.

i. Facilitate information exchange among the DoD Components regarding lessons learned and best practices in the PK-enabling of information systems, including network login, e-mail systems, and web servers by:

(1) Maintaining and making available a list of DoD Component PKI and PK-enabling coordinating offices.

(2) Maintaining and publishing a list of PK-enabled DoD information systems and COTS products used for PK-enabling that have successfully passed the DoD PKI interoperability testing program.

(3) Establishing and leading a forum for the DoD Components to coordinate, collaborate, and share information and lessons learned.

(4) Providing a collaborative environment for users, developers, and system administrators to collaborate and share information, including configuration guidelines for products commonly used throughout the DoD.

j. Coordinate with the Chairman of the Joint Chiefs of Staff and the other Heads of the DoD Components to ensure that the DoD PKI and deployed PK-enabled information systems are capable of supporting joint-, allied-, and coalition-based operations where required.

k. Coordinate with DoD Components to identify:

(1) Functional requirements supporting the DoD PKI upgrade and maintenance process.

(2) Component PKI interoperability testing requirements.

(3) Requirements for interoperating with external PKIs.

l. Collaborate with the Heads of the DoD Components to establish a DoD PKI interoperability testing program. The purpose of the testing program is to help ensure PK-enabled information systems interoperate with the components of the DoD PKI and comply with DoD PK enabling requirements. The PKI interoperability testing program shall include:

(1) Developing and maintaining a PKI interoperability test plan that includes technical and security requirements, as required for the DoD Components.

(2) Developing and maintaining the PKI interoperability testing capability.

m. Review justification of requests for hardware tokens other than the CAC and provide a recommendation for action to the ASD(NII)/DoD CIO.

n. Manage all tasks involved in the requirements for using DoD-approved PKIs by the DoD including:

(1) Developing an external interoperability plan for evaluating and recommending external PKIs for approval by the ASD(NII)/DoD CIO.

(2) Maintaining a program for performing interoperability testing of external PKIs that supports the approval of external PKIs.

(3) Developing and maintaining a repository for posting the root and intermediate CA certificates of approved external PKIs and commensurate certificate policy OIDs for approved external PKIs.

(4) Maintaining the DoD ECA program.

(5) Coordinating with the DoD Components to identify requirements to interoperate with DoD-approved PKIs.

(6) Collaborating with the Federal PKI community to ensure that DoD PKI and DoD ECA certificates are interoperable with other FBCA member PKIs.

(7) Providing recommendations for action to the ASD(NII)/DoD CIO for approval of external PKIs within the DoD, in coordination with the Office of the General Counsel and the Identity Protection Management Senior Coordinating Group, including certificates issued by other members of the FBCA community.

(8) Negotiating and signing cross-certification agreements (CCA), as described in Combined Communication-Electronics Board (CCEB) Publication 1010 (Reference (s)), with nations that participate in the CCEB activities.

o. Collaborate with standards bodies and vendors to promote implementations compatible with the DoD PKI.

4. DIRECTOR, IDENTITY ASSURANCE AND PKI. The Director, Identity Assurance and PKI, under the authority, direction, and control of ASD(NII)/DoD CIO, shall:

a. After consultation with the Director, DoD PKI PMO, approve incremental changes to References (j), (o), (p), (q), and (r), as required.

b. Approve and release audit compliance letters to Federal or other PKI entities with which the DoD has a relationship, as required.

c. Oversee efforts providing DoD PKI and PK-enabling policy compliance oversight including:

(1) Analyzing DoD Component PKI and PK-enabling compliance information;

(2) Notifying the DoD Components of shortfalls;

(3) Collaborating with United States Strategic Command, National Security Agency, DISA, and the Defense Information Systems Network (DISN)/GIG Flag Panel to understand the causes of non-compliance and to develop business process improvements; and reporting compliance analysis, shortfalls, and recommended improvements.

5. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R), in addition to the responsibilities in section 7 of this enclosure, shall:

a. Upgrade and maintain the required Defense Enrollment and Eligibility Reporting System/Real-time Automated Personnel Identification System infrastructure as required to support the DoD PKI issuing certificates on CACs and other hardware tokens in coordination with the ASD(NII)/DoD CIO.

b. Maintain the design of the CAC in accordance with Reference (m) and provide technical support on matters relating to smart card technology about the DoD PKI.

c. Support the certification and accreditation activities of the DoD PKI DAA.

6. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff, in addition to the responsibilities in section 7 of this enclosure, shall:

a. Identify, review, and validate PK-enabling requirements for the Combatant Commands and ensure that the Combatant Commanders coordinate requirements to implement this Instruction with their host Military Departments in accordance with DoDD 5100.03 (Reference (t)).

b. Coordinate with the DoD PKI PMO and the DoD Components to identify:

(1) PKI interoperability testing requirements.

(2) Requirements for interoperating with external PKIs.

c. Coordinate with the DoD PKI PMO and the DoD Components to ensure that deployed PK-enabled information systems are capable of supporting joint-, allied-, and coalition-based operations, as required.

7. HEADS OF THE OSD AND DoD COMPONENTS. The Heads of the OSD and DoD Components shall:

a. Plan, program, and budget to support the evolution of the DoD PKI program and to PK-enable applicable Component information systems.

b. Designate offices for coordinating PKI and PK-enabling activities.

c. Develop and implement policies and procedures for e-mail signature and encryption using DoD-approved PKIs to support Component business processes.

d. Coordinate with the Director, DoD PKI PMO, and the Chairman of the Joint Chiefs of Staff to identify:

(1) Functional requirements supporting the DoD PKI upgrade and maintenance process.

(2) Component PKI interoperability testing requirements.

(3) Requirements for interoperating with external PKIs.

e. Establish the Component portion of the infrastructure necessary to support the DoD PKI certificate life cycle and key recovery service.

f. Implement the DoD PKI and PK-enabled information systems, including network login, e-mail systems, web servers, and devices to use certificates for authentication, digital signatures, and encryption.

g. PK-enable information systems for joint programs and systems for which the Component is the Program Executive, Lead Agency, PMO, or equivalent.

h. Ensure that PK-enabled information systems have been tested under the PKI interoperability testing program, including:

(1) Commercial off-the-shelf (COTS) products to be used in new PK-enabled information systems and have been tested prior to procurement.

(2) PK-enabled Government-developed information systems that use PKI-based functions (authentication, digital signature or encryption) which should be tested prior to achieving initial operating capability.

(3) Legacy information systems that have undergone modification to use PKI-based functions (authentication, digital signature or encryption) which shall undergo interoperability testing during the enabling process.

i. Inform the Director, DoD PKI PMO, of information systems that have successfully completed PKI interoperability testing in accordance with procedures provided by the DoD PKI PMO.

j. Coordinate with the Heads of the other DoD Components and the Director, DoD PKI PMO, for interoperability testing and PK-enabling of information systems used throughout the DoD.

k. Coordinate with the Chairman of the Joint Chiefs of Staff and the Director, DoD PKI PMO, to ensure that deployed PK-enabled information systems are capable of supporting joint-, allied-, and coalition-based operations, as required.

l. Ensure all DoD contracts require DoD mission partners use certificates issued by the DoD External Certification Authority (ECA) program or a DoD-approved PKI, when interacting with DoD in unclassified domains as specified in Section 4 of this Instruction, above the signature.

m. Ensure that all DoD contracts require DoD mission partners to use certificates issued by the DoD portion of the NSS PKI, when interacting with DoD in classified domains as specified in Enclosure 3, paragraph 1.a. of this Instruction, Committee on National Security Systems Policy No. 25 (Reference (u)), and Reference (k).

n. Ensure the Component CIO provides ASD(NII)/DoD CIO with situational awareness of monitoring and compliance activities within the Component by:

(1) Reporting PKI and PK-enabling policy compliance status to the Director, Identity Assurance and PKI in accordance with ASD(NII)/DoD CIO reporting requirements.

(2) Establishing and implementing a DoD Component waiver process responsible for reviewing Component PKI or PK-enabling waiver requests.

(3) Submitting positively endorsed DoD Component waiver requests, for DISN/FLAG Panel approval, using the established DSAWG waiver review processes.

(4) Recommending DoD-wide waivers to the ASD(NII)/DoD CIO through the Director, Identity Assurance and PKI, where waivers involving multiple DoD Components are needed.

ENCLOSURE 3

IMPLEMENTING PROCEDURES

1. DoD PKI. The DoD implements the DoD PKI, DoD portion of the National Security Systems (NSS) PKI, and the DoD Coalition PKI to satisfy operational needs and requirements. These PKIs are operated by the DoD PKI PMO and shall be certified and accredited in accordance with DoDI 8510.01 (Reference (v)).

a. Certificate Issuance. The DoD PKI can issue certificates to all subscribers identified in Reference (j) to support DoD missions and business operations. The DoD-operated portion of the NSS PKI will issue certificates to DoD SIPRNET users for authentication and logon to SIPRNET resources in accordance with guidance provided in Reference (u), Committee on National Security Systems Instruction No. 1300 (Reference (w)) and Reference (k). The DoD Coalition PKI will issue certificates to coalition partner organizations or individuals conducting business with Combatant Commands in accordance with Reference (r).

b. Certificate Types. The DoD PKI is capable of issuing different types of certificates, including identity, authentication, signature, encryption, group/role, device, and code signing to satisfy DoD Component requirements.

c. Hardware Tokens. In accordance with Directive-Type Memorandum 08-003 (Reference (x)), the CAC shall be the primary hardware token for identifying individuals for logical access to NIPRNET resources and physical access to DoD facilities. The CAC hardware token protects the private keys associated with identity, authentication, signature, and encryption certificates issued by the DoD PKI for use in unclassified environments. DoD personnel shall use and can rely on certificates issued and maintained on the CAC. All hardware tokens used within the DoD must comply with the credential strength requirements stated in Reference (k). While DoD medium assurance (software) certificates are acceptable for use within the DoD, they are primarily intended for use in servers and other non-person entities (e.g., SSL certificates), and their use for identifying people (i.e., issuance of an identity certificate for a person) should be minimized.

(1) Hardware tokens used for network logon to the SIPRNET will be issued by a credential service provider that is either a member of the NSS PKI, is cross-certified with the NSS PKI in accordance with Reference (u), or has been specifically approved by the ASD(NII)/DoD CIO. DoD Components shall ensure that their infrastructures are capable of using NSS PKI hardware tokens for accessing networks and web-based resources on the DoD SIPRNET.

(2) Other hardware tokens, as approved by ASD(NII)/DoD CIO, may be authorized to facilitate DoD missions where accepting trust in the certificates on the token is consistent with the DoD information assurance requirements. Recommendations for approval of all hardware tokens will include the endorsement of the IPMSCG.

d. Alternate Logon Token (ALT). Use of an ALT with DoD PKI certificates is authorized for specific cases where certificates issued on the CAC cannot be used by various groups of network users. ALTs are approved for use when issued through the alternate login certificate process described in an appropriate Service or Agency certificate practice statement (CPS). Issuance of ALTs to authorized flag officer (FO) and Senior Executive Service (SES) personnel or their staffs shall be in accordance with the implementing procedures in the appendix to this enclosure.

e. Key Recovery. The DoD PKI shall provide a service to support escrow and recovery of private keys associated with encryption certificates.

2. EXTERNAL PKI. DoD information systems and users shall only rely on certificates that are issued by a DoD PKI or by an external PKI that has been approved for use. DoD relying parties will authenticate approved external PKI certificates using either a direct trust mechanism or using a cross-certification mechanism. All external PKI certificates presented from an approved external PKI must be validated via either download of the PKI certificate revocation list associated with the external PKI or use of an on-line certificate status protocol query. The DoD shall maintain a repository for posting CA certificates and policy OIDs for approved external PKIs.

a. DoD ECA PKI. The DoD shall maintain the DoD ECA program in accordance with Reference (p) to support the issuance of certificates to DoD mission partners. Certificates issued by DoD ECAs are approved for use within the DoD at all supported levels of assurance in Reference (p). The DoD shall operate the ECA root CA and shall maintain a repository for posting information regarding the DoD ECA program, including CA certificates and certificate revocation lists. Also, although the DoD ECA is established by the DoD, the identity proofing requirements for ECA certificates are different than the identity proofing and vetting requirements for the DoD PKI certificates on the CAC.

b. Non-DoD Sponsored External PKIs. The DoD will implement and maintain the procedures for approving external PKIs in accordance with Reference (l). The following paragraphs detail the requirements for obtaining approval for categories of external PKIs.

(1) Federal Agency PKIs. Federal agency PKI certificates are approved for use within the DoD if the following requirements are satisfied:

(a) Policy Mapping. Certificates shall assert a policy OID that has been mapped to the medium hardware or high assurance policy OID defined in the FBCA certificate policy (CP) (Reference (y)).

(b) Sponsorship. DoD sponsorship is not required for Federal agency PKIs.

(c) Interoperability Testing. Federal agency PKI certificates shall be tested for technical interoperability with DoD information systems, including web servers and e-mail

clients, to ensure that certificate revocation status information can be obtained by DoD information systems.

(d) Review. Review is not required for Federal agency PKIs.

(e) MOA. An MOA is not required for Federal agency PKIs.

(2) Federal Agencies Using the X.509 Common Policy Framework Under the Federal Shared Service Provider (SSP) Program. (The SSP Program, definition, and more information is available at http://www.idmanagement.gov/fpkipa/drilldown_fpkipa.cfm?action=ssp) PKI certificates issued by SSPs are approved for use within the DoD if the following requirements are satisfied:

(a) Policy Mapping. Certificates are issued by certified SSPs and assert one or more of the following policy OIDs defined in X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (Reference (z)): common-hardware, common-authentication, or common-High.

(b) Sponsorship. DoD sponsorship is not required for certificates issued by SSP PKIs.

(c) Interoperability Testing. Each Federal agency's certificates shall be tested for technical interoperability with DoD information systems, including web servers and e-mail clients, to ensure that certificate revocation status information can be obtained by DoD information systems.

(d) Review. Review is not required for certificates issued by SSP PKIs.

(e) MOA. An MOA is not required for SSP PKIs.

(3) Non-Federal Agency PKIs. Non-Federal agency PKIs are approved for use within the DoD if the following requirements are satisfied:

(a) Policy Mapping. Certificates assert a policy OID that has been mapped to the medium hardware policy OID defined in Reference (y), either directly or through a bridge cross certificate that has itself been issued by the FBCA.

(b) Sponsorship. A DoD Component shall identify a business case or mission need to interoperate with the PKI.

(c) Interoperability Testing. Non-Federal agency certificates shall be tested for technical interoperability with DoD information systems, including web servers and e-mail clients, to ensure that certificate revocation status information can be obtained by DoD information systems.

(d) Review. The business case or mission need along with interoperability testing results shall be favorably reviewed, in accordance with Reference (l), as presenting an acceptable risk for use with DoD systems and applications.

(e) MOA. The non-Federal agency PKI shall execute an appropriate MOA with the DoD, in accordance with Reference (l).

(4) CCEB Nation PKIs. CCEB nation PKIs are approved for use within the DoD if these requirements are satisfied:

(a) Policy Mapping. CCEB member nations shall assert that they comply with all requirements specified in Reference (s).

(b) Sponsorship. The DoD PKI PM is the sponsor for all CCEB nation PKIs.

(c) Interoperability Testing. Interoperability testing is not required for CCEB nation PKIs.

(d) Review. Review is not required for CCEB nation PKIs. The DoD PKI PMO is authorized to direct the issuance of DoD PKI cross certificates to CCEB member nations once the DoD and the CCEB member nation have signed a CCA.

(e) MOA. CCEB member nations shall sign a CCA with the DoD.

(5) Other Mission Partner PKIs (e.g., non-CCEB Nation Allies). Other partner PKIs are approved for use within the DoD if these requirements are satisfied:

(a) Policy Mapping. Requested policy OIDs defined by the partner CP shall be mapped to policy OIDs defined in Reference (j). This mapping shall identify any critical risks and potential impact to the DoD.

(b) Sponsorship. A DoD Component shall identify a business case or mission need to interoperate with the PKI.

(c) Interoperability Testing. Partner PKI certificates shall be tested for technical interoperability with DoD information systems, including web servers and e-mail clients, to ensure that certificate revocation status information can be obtained by DoD information systems.

(d) Review. The business case or mission need, policy mapping, and interoperability testing results shall be favorably reviewed, in accordance with Reference (l), as presenting an acceptable risk for use with DoD systems and applications.

(e) MOA. All partner PKIs shall execute an appropriate MOA with the DoD, in accordance with Reference (l).

3. PK-ENABLING. PK-enabling of DoD information systems shall be achieved through adherence to guidelines set forth in this Instruction and Reference (k). Certificates accepted by DoD relying parties must be issued by a PKI approved by the ASD(NII)/DoD CIO at an assurance level appropriate for the information being protected. PK-enabled information systems that include users who are DoD mission partners shall support certificates issued by DoD-approved PKIs. Security services shall be provided to the maximum extent possible via standard security protocols (e.g., secure sockets layer (SSL), transport layer security (TLS), and secure or multipurpose Internet mail extensions) and shall use algorithms and key strengths, as defined in Reference (j), commensurate with the sensitivity level (risk level, confidentiality impact level) of the information being protected (e.g., stored, processed, and/or accessed).

a. Authentication. Refer to Reference (k) for implementing procedures.

b. Digital Signature. PKI provides the capability to implement digital signatures and can be an important enabling tool to comply with Federal law, such as section 3504 of title 44, United States Code (U.S.C.) (also known as "The Government Paperwork Elimination Act" (Reference (aa))), and section 7001 of title 15, U.S.C. (also known as "The Electronic Signatures in Global and National Commerce Act" (Reference (ab))). If an information system uses PKI for digital signatures, then that system shall follow DoD implementation and interoperability standards for digital signatures in the DoD IT Standards Repository. DoD Components shall provide direction to review and assess processes or transactions that would increase information security or improve efficiency or effectiveness by incorporating digital signature capability. DoD Components shall ensure applications, systems, and business processes using digital signatures are identified to and reviewed by the DoD Component's General Counsel for all aspects of digital signature use to ensure legal sufficiency and to prevent conflict with law, regulations, policy, treaties or international agreements. DoD Components should consider contingency, work-around, or back-up signature procedures for any processes that rely upon the use of digital signatures.

(1) E-mail. All DoD e-mail systems shall support sending and receiving e-mail signed by DoD-approved certificates. E-mail shall be digitally signed in accordance with DoD Component digital signature policy and shall be signed using DoD-approved certificates.

(2) Other Information Systems. DoD information systems other than e-mail that incorporate the use of PKI for digital signatures shall follow DoD and DoD Component interoperability guidelines for digital signature solutions.

c. Encryption. PKI provides an encryption capability and can be a tool for complying with encryption requirements in Reference (c) as implemented in Reference (e). If an information system uses PKI for encryption of information in transit or at rest, then that system shall follow DoD Information Security Program policy, DoDI 5200.1-R (Reference (ac)), DoD Component guidelines for protecting information, and other requirements in this Instruction for PK-enabling and interoperability.

(1) Web Servers. All DoD web servers shall require a DoD-approved certificate to initiate SSL/TLS server authentication, support data integrity, and maintain confidentiality as necessary to meet the sensitivity level requirements of the information stored on those web servers.

(2) E-mail. All DoD e-mail systems (including mobile devices) shall support sending and receiving e-mail encrypted using DoD-approved certificates. E-mail shall be encrypted in accordance with DoD Component encryption policy and shall be encrypted using DoD-approved certificates.

(3) Other Information Systems. DoD information systems other than web servers or e-mails that incorporate the use of PKI for encryption of information in transit or at rest shall meet requirements in this Instruction for PK-enabling and interoperability.

4. INTEROPERABILITY TESTING PROGRAM

a. The purpose of the testing program is to ensure PK-enabled information systems interoperate with the components of the DoD PKI and comply with PK-enabling developed by the DoD PKI PMO. The PKI interoperability testing program will include:

(1) Developing and maintaining a PKI interoperability test plan that includes technical and security requirements, as required for the DoD Components.

(2) Developing and maintaining a PKI interoperability testing capability for all DoD Components.

b. Acquisition and development authorities for information systems shall ensure new information systems conform to PK-enabling standards developed by the DoD PKI PMO and are interoperable with all DoD-approved PKIs.

c. PK-enabled information systems shall be tested to ensure conformance to current PK-enabling standards and shall be interoperable with all DoD-approved PKIs.

d. COTS software products using or requiring the use of PK cryptography shall be tested to ensure interoperability with the appropriate DoD PKI and verified against security requirements in Reference (c) prior to procurement. COTS products not passing interoperability testing shall not be procured unless interoperable alternatives providing the requisite functionality are unavailable.

5. WAIVERS

a. The DISN/GIG Flag Panel may authorize waiving compliance with this Instruction for individual information systems on a case-by-case basis. Waivers shall be granted only for the minimum length of time required to achieve compliance. All waiver requests from an

information system, their operational control headquarters, or program office shall include a Component CIO endorsement memorandum that validates the waiver rationale and justification. Information systems applying for a waiver to this policy will follow guidance in Chairman of the Joint Chiefs of Staff Instruction 6211.02C (Reference (ad)) and the DSAWG. System owners granted waivers by the DISN/GIG Flag Panel for their information systems shall report approved waivers to the ASD(NII)/DoD CIO within 15 days of approval. All waivers previously approved under DoDI 8520.02, dated 1 April 2004 by DoD Component CIOs shall be submitted to the DISN/GIG Flag Panel if renewal or extension of any previous waiver is required.

b. For policy compliance issues that are DoD-wide or involve multiple DoD Components, DoD Components may submit DoD-wide waiver recommendations through the Director, Identity Assurance and PKI to the ASD(NII)/DoD CIO. DoD-wide waivers shall be granted for only the minimum length of time required to achieve compliance.

APPENDIX TO ENCLOSURE 3

CRITERIA FOR ISSUANCE OF ALT TO FOs, SES MEMBERS, AND DESIGNATED STAFF

The following are the minimum steps and criteria that must be met when ALTs are issued to FO/SES and authorized staff members.

a. The Head of the DoD Component shall designate, in writing, an approving authority for issuance of ALTs.

b. Participating FO or SES must designate their individual network account as a "group" account.

c. One member of the FO or SES staff shall be named, in writing, as the sponsor for the group account. That individual shall:

(1) Control and designate which personnel are assigned to the group account.

(2) Request one or more ALTs from the supporting Service's Registration Authority. The number of ALTs requested will be limited to the minimum needed to support the mission.

(3) Control and monitor distribution of all authorized and assigned tokens.

d. The local network domain administrator shall change the characterization of the account from an individual account to a group account and provide the value of FO or SES user principal name (UPN) field to the Registration Authority providing the ALTs.

e. The PKI certificate on the ALT which will support smart card logon shall have the value of the supported FO or SES UPN field as an entry in the Subject Alternate Name field of the certificate. Each token will be issued to the individual or role identified in the Common Name field in the PKI certificates.

f. The issuance of ALTs as group authentication tokens will be conducted in accordance with the appropriate CPS. This requires each DoD Component to ensure its CPS allows FO or SES ALT issuance.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ALT	alternate logon token
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer
CA	certification authority
CAC	common access card
CCA	cross-certification agreements
CCEB	Combined Communications-Electronics Board
CC/S/A	Combatant Command, Service or Agency
CNSS	Committee on National Security Systems
COTS	commercial off-the-shelf
CP	certificate policy
CPS	certification practice statement
DAA	designated accrediting authority
DISA	Defense Information Systems Agency
DISN/GIG	Defense Information System Network/Global Information Grid
DoDD	DoD Directive
DoDI	DoD Instruction
DREN	Defense Research and Engineering Network
ECA	External Certification Authority
FBCA	Federal Bridge Certification Authority
FO	flag officer
GIG	Global Information Grid
IPMSCG	Identity Protection and Management Senior Coordinating Group
IT	information technology
MOA	memorandum of agreement
NIPRNET	Non-classified Internet Protocol Router Network
NSS	National Security Systems
OID	object identifier
PK	public key
PKI	public key infrastructure

PMO	program management office
SDREN	Secret Defense Research and Engineering Network
SES	Senior Executive Service
SIPRNET	Secret Internet Protocol Router Network
SSL	secure sockets layer
SSP	Shared Service Provider
TLS	transport layer security
UPN	user principal name
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

assurance level. Defined in Reference (j).

CAC. Defined in Reference (d).

certificate. Defined in Reference (j)

CP. Defined in RFC 3647-X.509 Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework (Reference (ae)).

CPS. Defined in Reference (ae).

credential service provider. An organization or vendor that proffers a service that issues any type of identity credential or identification card. Normally, the credentialing service is used to outsource the production of identity credentials for an organization or entity that does not operate their own credentialing capability.

cross-certification. The act or process by which two CAs each certify a PK of the other, issuing a PK certificate to that other CA. Cross-certification enables users to validate each other's certificate when the users are certified under different certification hierarchies. Cross-certification with the FBCA asserts that the DoD PKI operates in accordance with the standards, guidelines, and practices of the Federal PKI Policy Authority.

direct trust. A simple interoperating mechanism used by an application to take advantage of trust relationships between CAs in different PKIs. An application installs the Root CA certificate and any intermediate CA certificates into the application server's Certificate Trust store, creating a

path from a CA within a PKI that the application trusts directly to the CA that issued the certificate that is being presented to the application.

DoD-approved PKI. A PKI approved by the ASD(NII)/DoD CIO for use by DoD relying parties consistent with the processes in Reference (l). A listing of DoD-approved PKIs is located at: https://www.us.army.mil/suite/page/571419.

DoD mission partners. Federal, State, local, tribal, and coalition partners; foreign governments and security forces; international organizations; non-governmental organizations; private sector companies or organizations; and educational institutes. These entities may process electronic transactions with the DoD, or exchange e-mail or other data containing DoD relevant information.

DoD PKI certificate eligible users. DoD uniformed and civilian personnel and eligible contractors; DoD volunteers or interns; Selected Reserve personnel; Executive department and agency personnel; State or local or tribal government employees; foreign government and foreign organization personnel, and foreign contractors.

DoD PKI interoperability. The ability of DoD-relying parties, such as web servers and e-mail users, to accept certificates issued by DoD-approved PKIs for authentication and to rely upon the authenticated identity as a basis for rules-based system or data authorization or access control decisions.

ECA. The program established by the DoD to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. The DoD has established and controls the governing ECA certificate policy; the issuing CAs are owned and operated by a commercial entity that has been approved as meeting the DoD ECA Certificate Policy and is authorized to create, sign, and issue certificates to external entities that DoD relying parties may use for authentication, signature, and encryption.

External PKI. Any PKI established and sponsored by an entity outside of the DoD. The PKI may be operated by a commercial PKI vendor.

hardware token. A portable, user-controlled, physical device used to generate, store, and protect cryptographic information, and to perform cryptographic functions.

key recovery. The capability for authorized entities to retrieve keying material from a key backup or archive. Recovery of an individual's escrowed encryption key (keying material) initiated by the individual issued that encryption key is considered a first party key recovery process. The individual is always authorized to recover their own escrowed private key(s). Recovery of an individual's escrowed encryption key initiated by other than the individual that the key was issued to is considered third party key recovery. Third parties must obtain authorization to obtain someone else's escrowed private key.

key recovery policy. A named set of rules that specify the conditions under which key recovery information must be created, and conditions under which and to whom escrowed keys may be

released; it also indicates who are allowable key recovery agent(s) and key recovery officials and how or where escrowed keys must be maintained.

key recovery practice statement. A statement of the practices that a key escrow database, key recovery authority, or other PKI component employs in escrowing private keys associated with encryption certificates and recovering them, in accordance with specific requirements specified in a key recovery policy.

non-Federal agency. An entity that is a State, local, or tribal government, commercial organization, or non-governmental organization. For example, the State of Illinois Department of Transportation, a State-level Bureau of Indian Affairs, the Boeing Company, and the Red Cross are considered non-Federal agencies.

PK-enabling. The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and non-repudiation. PK-enabling involves replacing existing or creating new user authentication systems using certificates instead of other technologies, such as user identification and password or Internet protocol filtering; implementing PK technology to digitally sign, in a legally enforceable manner, transactions and documents; or using PK technology, generally in conjunction with standard symmetric encryption technology, to encrypt information at rest or in transit.

PKI. The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of PK certificates.

policy OID. A specific piece of information asserted in the certificate extensions of all DoD and DoD-approved PKI certificates. A policy OID designates the set of rules identified in an associated CP. A policy OID allows a relying party to differentiate between two or more sets of rules for issuing certificates within a single CP.

relying party. Any entity that uses a digital certificate to identify the creator of digitally signed information, verify the integrity of digitally signed information, or establish confidential communication with the holder of a certificate by relying on the validity of the binding the subscriber's name to the PK contained in the certificate.

Selected Reserve. Those units and individuals within the Ready Reserve designated by their respective Service and approved by the Chairman of the Joint Chiefs of Staff as so essential to initial wartime missions that they have priority over all other Reserves. All Selected Reservists are in an active status. The Selected Reserve also includes persons performing initial active duty for training. See Reference (d) for further information.

smart card. A credit card-size device containing one or more integrated circuits and may employ one or more of the following technologies: magnetic stripe, bar code (linear or two-dimensional), non-contact and radio frequency transmitters, biometric information, encryption and authentication information, and photo identification.

SSP. An organization that provides PKI services and digital certificates for use by Federal agency employees and selected contractors as required by Reference (m). The PKI SSP program, which is administered by the General Services Administration, was established to assist agencies with the decision of selecting a PKI service provider.

web server. An automated information system that manages a Website by passing web pages to web browsers over a network. The web server may provide information stored locally on the server or may act as a portal to access information from other linked information systems.