Department of Defense

INSTRUCTION

NUMBER 8520.2
April 1, 2004

ASD(NII)

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

References: (a) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002
(b) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(c) DoD Directive 8190.3, "Smart Card Technology," August 31, 2002
(d) DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," August 12, 2000 (hereby canceled)
(e) through (t), see enclosure 1

1. PURPOSE

This Instruction:

1.1. Implements policy, assigns responsibilities, and prescribes procedures for developing and implementing a Department-wide Public Key Infrastructure (PKI) and enhancing the security of Department of Defense (DoD) information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption.

1.1. Aligns DoD PKI and PK (Public Key)-Enabling activities with reference (a), as implemented by reference (b), and the DoD Common Access Card (CAC) program, as specified by reference (c).

1.3. Supersedes references (d), (e), (f), and (g).

2. APPLICABILITY AND SCOPE

This Instruction applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff; the Combatant Commands, the Office of the Inspector General of the

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 APR 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Public Key Infrastructure (PKI) and Public Key (PK) Enabling	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense ,1400 Defense Pentagon,Washington,DC,20301-1400**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**18**	

Department of Defense; the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. All active duty military personnel, members of the Selected Reserve, DoD civilian employees, and other DoD eligible users.

2.3. Information-privileged individuals, volunteers, and Reservists accessing personal information held by DoD information systems.

2.4. All DoD unclassified and classified information systems including networks (e.g., Non-secure Internet Protocol Router Network , Secret Internet Protocol Router Network, web servers, and e-mail systems. Excluded are Sensitive Compartmented Information, and information systems operated within the Department of Defense that fall under the authority of the Director of Central Intelligence Directive (DCID) 6/3 (reference (h)).

3. DEFINITIONS

Terms used in this instruction are defined in references (a), (b), CNSS Instruction No. 4009 (reference (i)), and enclosure 2.

4. POLICY

4.1. This Instruction implements the policies established in references (a) and (c) and supplements the implementation guidance provided in reference (b).

4.2. The Department of Defense shall implement a Department-wide PKI to issue identity, signature, and encryption certificates to DoD eligible personnel and provide first and third party key recovery for private keys associated with encryption certificates. The DoD PKI also shall support requirements for group/role, device, and code signing certificates.

4.3. The DoD Components shall enable DoD information systems, including networks, e-mail, and web servers, to use certificates issued by the DoD PKI and approved external PKIs as appropriate to support authentication, access control, confidentiality, data integrity, and nonrepudiation.

4.4. The Department of Defense shall require that DoD Partners get and use certificates issued by approved external PKIs when interacting with DoD PK-Enabled information systems; accessing DoD sensitive information; or engaging in any other transactions requiring data integrity, confidentiality, or nonrepudiation of DoD information.

4.5. The DoD Components that conduct web server-based transactions with information-privileged individuals, volunteers, or Reservists involving the transfer of personal information,

shall use encryption to ensure confidentiality of these transactions, and shall require, at a minimum, that the information-privileged individual present a user-id and password.

4.6. The DoD Components shall ensure that new Commercial-Off-The-Shelf (COTS) software to be used in information systems that require PK-Enabling have passed interoperability testing performed by a DoD PKI Program Management Office (PMO)-approved testing facility prior to procurement.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)), as the DoD Chief Information Officer (CIO), shall:

5.1.1. Manage implementation and evolution of the DoD PKI.

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

5.1.2.1. Providing oversight and guidance for digital signature and encryption requirements.

5.1.2.2. Ensuring Department-wide interoperability of digital signature solutions.

5.1.3. Approve the X.509 Certificate Policy (reference (j)) and the associated Key Recovery Policy (reference (k)), as required.

5.1.4. Approve the DoD Component certification and key recovery practice statements as complying with references (j) and (k).

5.1.5. Serve as the Designated Approving Authority (DAA) for the DoD PKI.

5.1.6. Approve or disapprove Department-wide waivers submitted by the DoD PKI PMO.

5.1.7. Approve DoD use of hardware tokens other than the CAC for identity, signature, and encryption certificates.

5.1.8. Approve DoD relying party use of certificates issued by external PKIs including:

5.1.8.1. Approving the Certificate Policy for External Certification Authorities (reference (l)) and the Key Recovery Policy for External Certification Authorities (reference (m)), as required.

5.1.8.2. Approving the compliance of vendor component certification and key recovery practice statements to reference (l) and (m) documents.

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

5.1.9. Oversee the Defense-wide Information Assurance Program (DIAP) office efforts in providing DoD PKI and PK-Enabling policy compliance oversight including:

5.1.9.1. Maintaining and updating the DoD Guidance and Provisions for Developing the DoD Component's Public Key-Enabling Policy Compliance Waiver Process (reference (n)), as required.

5.1.9.2. Producing an annual report that summarizes DoD-wide PKI and PK-Enabling policy compliance status.

5.1.9.3. Analyzing DoD Component PKI and PK-Enabling compliance information and notifying the DoD Components of shortfalls or duplications of effort.

5.2. The Under Secretary of Defense (Personnel and Readiness) (USD(P&R)), under references (a) and (c), shall:

5.2.1. 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 in coordination with the ASD(NII)/DoD CIO.

5.2.2. Maintain the design of the CAC and provide technical support on matters relating to smart card technology about the DoD PKI.

5.2.3. Support the Certification and Accreditation activities of the DoD PKI DAA.

5.3. The Chairman of the Joint Chiefs of Staff, under reference (a) and (c), shall:

5.3.1. Identify, review, and validate PK-Enabling requirements for the Combatant Commands and ensure that the Combatant Commanders coordinate requirements to implement this policy with their host Military Departments in accordance with DoD Directive 5100.3 (reference (o)).

5.3.2. Coordinate requirements for the DoD PKI and for PK-Enabled information systems to support joint, allied, and coalition-based operations.

5.4. The Director, Defense Information Systems Agency shall:

5.4.1. Operate and maintain the DoD PKI in coordination with the DoD PKI PMO.

5.4.2. Provide technical support to the Heads of the DoD Components in implementing the DoD PKI.

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

5.5. The Heads of the DoD Components shall:

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

5.5.2. Designate offices for coordinating PKI and PK-Enabling activities.

5.5.3. Develop and implement policies and procedures for e-mail signature and encryption, and for acceptance of certificates issued by DoD-approved external PKIs to support Component business processes.

5.5.4. Coordinate with the DoD PKI PMO to identify requirements including:

5.5.4.1. Functional requirements supporting the DoD PKI upgrade and maintenance process.

5.5.4.2. Component PKI interoperability testing requirements.

5.5.4.3. Requirements for interoperating with external PKIs.

5.5.5. Establish the Component portion of the infrastructure necessary to support the DoD PKI key recovery service.

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

5.5.7. PK-Enable information systems for Joint programs and systems for which the Component is the executive agent, PMO, or equivalent.

5.5.8. Ensure that PK-Enabled information systems have been tested by a centralized or Component-specific testing facility approved by the DoD PKI PMO in accordance with the PKI interoperability test plan as follows:

5.5.8.1. New COTS PK-Enabled information systems have been tested prior to procurement.

5.5.8.2. New Government-developed information systems that require PK-Enabling are developed and tested prior to Initial Operating Capability.

5.5.8.3. Legacy information systems that are being PK-Enabled undergo testing as part of the PK-Enabling process.

5.5.9. Inform the DoD PKI PMO of information systems that have successfully completed PKI interoperability testing.

5.5.10. Coordinate with other Components and the DoD PKI PMO for interoperability testing and PK-Enabling of information systems used throughout the Department of Defense.

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

5.6. The DoD Component CIOs shall:

5.6.1. Report PKI and PK-Enabling policy compliance status to the DIAP office in accordance with ASD(NII)/DoD CIO reporting requirements.

5.6.2. Approve business case analyses for PK-Enabling of information systems other than network login, e-mail systems, and web servers.

5.6.3. Develop DoD Component waiver process in accordance with reference (n).

5.6.4. Approve or disapprove waiver requests in accordance with the DoD Component waiver process guidance and submit approved waivers to the ASD(NII)/DoD CIO.

5.6.5. Recommend Department-wide waivers to the ASD(NII)/DoD CIO where waivers involving multiple DoD Components are needed.

5.7. The Director, DoD PKI Program Management Office, as defined by the Assignment of PMO Responsibilities for the DoD PKI PMO (reference (p)), shall:

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

5.7.2. Maintain the reference (j) and (k) documents.

5.7.3. Ensure the timely availability of Certificate Authorities, encryption certificates, and Certificate Revocation Lists.

5.7.4. Provide a key recovery service for private keys associated with encryption certificates.

5.7.5. Coordinate PKI functional requirements inputs from the Heads of the DoD Components.

5.7.6. Provide guidance to the DoD Components regarding the evolving DoD PKI implementation and PK-Enabling to ensure consistency across the Department of Defense.

5.7.7. 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:

5.7.7.1. Maintaining and making available a list of DoD Component PKI and PK-Enabling coordinating offices.

5.7.7.2. Maintaining and publishing a list of PK-Enabled DoD information systems, including COTS products, that have successfully passed DoD PKI interoperability testing.

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

5.7.7.4. Providing a collaborative environment for users, developers, and system administrators to collaborate and share information, including configuration guidelines for products commonly used throughout the Department of Defense.

5.7.8. 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.

5.7.9. Coordinate with the Heads of the DoD Components to establish a DoD PKI interoperability testing program for information system interoperability with the DoD PKI including:

5.7.9.1. Developing and maintaining a PKI interoperability test plan including technical and security requirements, as provided by the DoD Components.

5.7.9.2. Developing and maintaining testing facility requirements.

5.7.9.3. Approving centralized and DoD Component-specific testing facilities in accordance with the PKI interoperability test plan and facility requirements.

5.7.10. Review justification of requests for hardware tokens other than the CAC for identity, signature, and encryption certificates and provide a recommendation for action to the ASD(NII)/DoD CIO.

5.7.11. Manage all tasks involved in the requirements for using external PKIs by the Department of Defense including:

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

5.7.11.2. Establishing and maintaining the External Certification Authority (ECA) program, including updating references (l) and (m), as required.

5.7.11.3. Coordinating with the DoD Components to identify requirements to interoperate with external PKIs other than the ECA and FBCA programs.

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

5.7.11.5. Providing a recommendation for action to the ASD(NII)/DoD CIO for approval of external PKIs within the Department of Defense in coordination with the Office of the General Counsel and the Senior Coordinating Group, including certificates issued by other members of the FBCA community.

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

6. PROCEDURES

Implementation procedures are in enclosure 3.

7. EFFECTIVE DATE

This Instruction is effective immediately.

Linton Wells II
Acting Assistant Secretary of Defense
for Networks and Information Integration

Enclosures - 3
- E1. References, continued
- E2. Definitions
- E3. Implementation Procedures

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Chief Information Officer Memorandum, "Public Key Enabling (PKE) of Applications, Web Servers, and Network for the Department of Defense," May 17, 2001 (hereby canceled)
(f) DoD Chief Information Officer Memorandum, "Public Key Infrastructure (PKI) Policy Update," May 21, 2002 (hereby canceled)
(g) DoD Chief Information Officer Memorandum, "Public Key Infrastructure (PKI) and Public Key Enabling (PKE) Implementation Update," October 7, 2003 (hereby canceled)
(h) DCID 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," June 5, 1999[1]
(i) Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance (IA) Glossary," May 2003[2]
(j) DoD "X.509 Certificate Policy for the United States Department of Defense," current edition[3]
(k) DoD "Key Recovery Policy for the United States Department of Defense," current edition[4]
(l) DoD "Certificate Policy for External Certification Authorities," current edition[5]
(m) DoD "Key Recovery Policy for External Certification Authorities," current edition[6]
(n) 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

---

[1] http://www.fas.org/irp/offdocs/dcid.htm
[2] http://www.nstissc.gov/html/library.html
[3] http://www.iase.disa.mil/policy.html#pki
[4] http://www.iase.disa.mil/policy.html#pki
[5] http://www.iase.disa.mil/pki/eca/documents.html
[6] http://www.iase.disa.mil/pki/eca/documents.html

(o) DoD Directive 5100.3, "Support of the Headquarters of Combatant and Subordinate Joint Commands," November 15, 1999
(p) Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) Memorandum, "Assignment of Program Management Office Responsibilities for the Department of Defense Public Key Infrastructure (PKI)," April 9, 1999[7]
(q) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996
(r) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 6, 1999
(s) Section 3504 of title 44, United States Code, "Government Paperwork Elimination Act (Public Law No. 105-277)," October 21, 1998
(t) Section 7001 of title 15, United States Code, "Electronic Signatures in Global and National Commerce Act (Public Law No. 106-229)," June 30, 2000

[7] http://www.iase.disa.mil/policy.html#pki

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Assurance Level. The level of assurance associated with a certificate is an assertion by a Certificate Authority of the degree of confidence that others may reasonably place in the binding of a public key to the identity and privileges asserted in the certificate. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a certificate management system. Assurance levels are defined in reference (j).

E2.1.2. Business Case Analysis. An extended form of cost-benefit analysis that considers factors beyond financial metrics. Other factors to be considered might include security needs, business needs, associated risks, and qualitative benefits resulting from the investment. Business case methodology examines investment worthiness and its technical and programmatic feasibility.

E2.1.3. Certificate. A digital representation of information that, at a minimum, identifies the certification authority issuing it, names or identifies its subscriber, contains the subscriber's public key, identifies its operational period, and is digitally signed by the certification authority issuing it.

E2.1.4. Certificate Policy (CP). A named set of rules that indicates the applicability of a certificate to a particular community and/or class of information system with common security requirements. A certificate policy may be used by a certificate user to help in deciding whether a certificate and the binding therein, is sufficiently trustworthy for a particular information system.

E2.1.5. Certification Practice Statement (CPS). A statement of the practices that a Certificate Authority, Registration Authority, or other PKI component employs in issuing, revoking, and renewing certificates and providing access to them, in accordance with specific requirements specified in a CP.

E2.1.6. Committee on a National Security Systems (CNSS). The CNSS, chaired by the Secretary of Defense, provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems. The Secretary of Defense and the Director of Central Intelligence are responsible for developing and overseeing the implementation of Government-wide policies, principles, standards, and guidelines for the security of systems with national security information. As a standing committee of the President's Critical Infrastructure Protection Board, the CNSS reports fully and regularly on its activities to the Board.

E2.1.7. Common Access Card (CAC). A Department-wide smart card used as the identification card for active duty Uniformed Services personnel (to include the Selected Reserve), DoD civilian employees, eligible contractor personnel, and eligible foreign nationals; the primary platform for the public key infrastructure authentication token used to access DoD computer networks and systems in the unclassified environment and, where authorized by governing security directives, the classified environment; and the principal card enabling physical access to buildings, facilities, installations, and controlled spaces as described in reference (c).

E2.1.8. DoD-Approved External PKI. A PKI approved by the ASD(NII)/DoD CIO for use by DoD relying parties for assurance levels appropriate for the information being protected.

E2.1.9. DoD Eligible Users. DoD eligible users are 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.

E2.1.10. DoD Partners. DoD partners are Government or non-Government entities that process electronic transactions with the Department of Defense, or exchange e-mail containing DoD sensitive information.

E2.1.11. DoD PKI Interoperability. PKI interoperability refers to the ability of relying parties, such as web servers and e-mail users, to accept certificates issued by DoD-Approved External PKIs, and to the ability of information systems to correctly accept and use certificates issued by the DoD PKI.

E2.1.12. DoD Private Web Server. For unclassified networks, a DoD private web server is any DoD-owned, operated, or controlled web server providing access to sensitive information that has not been reviewed and approved for release in accordance with DoD Directive 5230.9 (reference (q)) and DoD Instruction 5230.29 (reference (r)). For Secret Internet Protocol Router Network and other classified networks that are not accessible to the public, a DoD private web server is any server that provides access to information that requires need-to-know control or compartmentation.

E2.1.13. External Certification Authority (ECA). A certification authority owned and operated by an entity outside the Department of Defense that has been approved as meeting the 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.

E2.1.14. Hardware Token. A portable, user-controlled, physical device used to generate, store, and protect cryptographic information, and to perform cryptographic functions.

E2.1.15. Information-Privileged Individual. For purposes of this Instruction, an information-privileged individual is a person whom the Department of Defense has authorized access to specified DoD information systems to provide them information about, or access to, benefits, entitlements or services, which may be available to them. The information may include information protected by the Privacy Act or Health Insurance Portability and Accountability Act, which may be lawfully displayed to them. Information-privileged individuals include retirees and dependents. These individuals are provided access to these systems to facilitate the delivery of benefits, entitlements and services. Information-privileged individuals will not be provided access to other DoD sensitive systems, unless they are otherwise authorized such access.

E2.1.16. Key Recovery. The capability for authorized entities to retrieve keying material from a key backup or archive.

E2.1.17. Key Recovery Policy (KRP). 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.

E2.1.18. Key Recovery Practice Statement (KRPS). 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 KRP.

E2.1.19. Personal Information. Information such as medical records, credit card numbers, job applications, and training reports, which are considered sensitive because of their personal nature.

E2.1.20. Public Key (PK) Enabling. The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and nonrepudiation. PK-Enabling involves replacing existing or creating new user authentication systems using certificates instead of other technologies, such as userid and password or Internet Protocol filtering; implementing public key technology to digitally sign, in a legally enforceable manner, transactions and documents; or using public key technology, generally in conjunction with standard symmetric encryption technology, to encrypt information at rest and/or in transit.

E2.1.21. Public Key Infrastructure. The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates.

E2.1.22. 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 public key contained in the certificate.

E2.1.23. Selected Reserve. Those units and individuals within the Ready Reserve designated by their respective Services and approved by the Chairman of the Joint Chiefs of Staff as 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.

E2.1.24. 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.

E2.1.25. Web Server. An automated information system that manages a web site 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.

E3. ENCLOSURE 3

IMPLEMENTATION PROCEDURES

E3.1. INTRODUCTION

Public key cryptography is a critical element of the Department of Defense net centric goals as well as Information Assurance (IA) Defense-in-Depth technical strategy. The DoD PKI provides a foundation for interoperable security services including authentication, data integrity, and confidentiality, and also supports digital signature, access control and nonrepudiation. Integrating PKI into DoD information systems through PK-Enabling achieves these security services through digital signature and encryption.

E3.2. PUBLIC KEY INFRASTRUCTURE

The Department of Defense shall implement a Department-wide PKI capable of providing security management services for certificates in accordance reference (j). The PKI shall be certified and accredited in accordance with reference (a).

E3.2.1. Certificate Issuance. All DoD eligible users shall be issued certificates from the DoD PKI. Users not eligible for DoD PKI certificates, but requiring certificates to communicate with DoD relying parties, must get certificates from external PKIs approved in accordance with subparagraph 5.1.8.

E3.2.2. Certificate Types. The DoD PKI shall be capable of issuing different types of certificates, including identity, signature, encryption, group/role, device, and code signing.

E3.2.3. Assurance Levels. The DoD PKI shall evolve to higher assurance levels, as defined in reference (j)) in response to enhanced capabilities of PKI technology and increased capabilities of the DoD Components. During this evolution process, the DoD PKI shall continue to support lower assurance level certificates as required.

E3.2.4. Hardware Tokens. In accordance with reference (c), the CAC shall be the primary token for protecting private keys associated with identity, signature, and encryption certificates issued by the DoD PKI. Alternative hardware tokens may be approved by the ASD(NII)/DoD CIO where justified.

E3.2.5. Key Recovery. The DoD PKI shall provide a scalable key recovery service to support first-party and third-party key recovery. This service shall be used to store and recover private keys associated with encryption certificates and shall conform to reference (k).

E3.3. EXTERNAL PKI

PK-Enabled information systems shall interoperate with external PKIs approved in accordance with subparagraph 5.1.8., where the DoD functional community requires such interoperability and where accepting trust in external PKIs is consistent with DoD IA requirements, as outlined in reference (a). External entities include other Federal Agencies, State and local governments, allied and coalition partners, industry partners, DoD-affiliated personnel, and unaffiliated individuals. Interoperability with external PKIs may be accomplished through a combination of cross-certification, trust lists, or other mechanisms, as defined in the external interoperability plan.

E3.3.1. External Certification Authorities (ECA). The Department of Defense shall establish and maintain the ECA program in accordance with reference (l) to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations.

E3.3.2. Federal Bridge Certification Authority (FBCA). The Department of Defense shall provide guidance on the use of certificates issued by FBCA member PKIs.

E3.4. PK-ENABLING

PK-Enabling of DoD information systems shall be achieved through adherence to guidelines set forth in this policy, with unclassified networks hosting Mission Assurance Category I information systems being given highest priority. 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, as defined in reference (j). Information systems requiring PK-Enabling that include users who are DoD Partners not eligible for DoD PKI certificates shall support certificates issued by DoD-approved external PKIs, as defined in section E3.3. Security services shall be provided to the maximum extent possible via standard security protocols (e.g., Secure Sockets Layer, Transport Layer Security, and Secure/Multipurpose Internet Mail Extensions) and shall use algorithms and key strengths as defined in reference (j).

E3.4.1. Identity. Networks and web servers accessed by DoD eligible users and DoD Partners shall be enabled to use certificates for authenticating users and to support access control decisions. Web servers protecting access to personal information for information-privileged individuals, volunteers, and Reservists do not require client certificate authentication, but shall at a minimum require userid and password-based

authentication. Other information systems shall consider the use of certificates for authenticating users.

E3.4.1.1. Network Login. All DoD networks required by reference (a) to authenticate users shall perform this authentication using certificates issued by the DoD PKI on hardware tokens (e.g., the CAC or an equivalent assurance level DoD PKI token).

E3.4.1.2. Web Server Authentication. DoD private web servers providing access to DoD sensitive information except those protecting access to personal information by information-privileged individuals shall be PK-Enabled to rely on certificates for client authentication issued by DoD-approved PKIs. Information systems residing behind web servers requiring authorization based on individual identity shall use the identity provided by certificate-based authentication to support access control decisions.

E3.4.1.3. Other Information Systems. For information systems requiring authentication other than network login or web servers, the system owner shall perform a business case analysis to determine if PK-Enabling is warranted. The business case analysis shall be submitted to the DoD Component CIO for review and approval. If warranted, the information system shall be PK-Enabled.

E3.4.2. Digital Signature. PKI provides the capability to implement digital signatures and can be an important enabling tool to comply with Federal regulations, such as the Government Paperwork Elimination Act (reference (s)) and the Electronic Signatures in Global and National Commerce Act (reference (t)). If an information system uses PKI for digital signatures then that system shall follow ASD(NII) guidelines for digital signature requirements and Department-wide interoperability, and other requirements in this Instruction for PK-Enabling and interoperability.

E3.4.2.1. E-mail. All DoD e-mail systems shall support sending and receiving e-mail signed by DoD-approved certificates. E-mail requiring data integrity, message authenticity, or nonrepudiation of DoD sensitive information, other than personal information sent by information-privileged individuals, volunteers, or Reservists, shall be signed using DoD-approved certificates.

E3.4.2.2. Other Information Systems. Information systems other than e-mail that incorporate the use of PKI for digital signatures shall be interoperable with the DoD PKI and shall follow Department-wide interoperability guidelines for digital signature solutions.

E3.4.3. Encryption. PKI provides an encryption capability and can be a tool for complying with encryption requirements in reference (a) as implemented in reference (b). If an information system uses PKI for encryption of information in transit or at rest, then that system shall follow ASD(NII) guidelines for encryption requirements, and other requirements in this Instruction for PK-Enabling and interoperability.

E3.4.3.1. Web Servers. All DoD private web servers shall be PK-Enabled to use a DoD-approved certificate for server authentication, data integrity, and confidentiality.

E3.4.3.2. E-mail. All DoD e-mail systems shall support sending and receiving e-mail encrypted using DoD-approved certificates.

E3.4.3.3. Other Information Systems. Information systems other than web servers or e-mail 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.

E3.5. INTEROPERABILITY TESTING

E3.5.1. Development authorities for information systems using or requiring the use of public key cryptography shall ensure interoperability with the DoD PKI in accordance with standards developed by the DoD PKI PMO.

E3.5.2. All PK-Enabled information systems shall be tested to ensure interoperability with the DoD PKI and verified against security requirements in reference (a) in accordance with guidance provided by the DoD PKI PMO.

E3.5.3. COTS software products using or requiring the use of public key cryptography shall be tested to ensure interoperability with the evolving DoD PKI and verified against security requirements in reference (a) prior to procurement. COTS products not passing interoperability testing shall not be procured unless interoperable alternatives providing the requisite functionality are unavailable.

E3.6. WAIVERS

E3.6.1. DoD Component CIOs may authorize waiving compliance to 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. Approved waivers shall be reported to the ASD(NII)/DoD CIO within 15 days of approval.

E3.6.2. For policy compliance issues that are Department-wide or involve multiple Components, DoD Components may coordinate Department-wide waiver requests to the ASD(NII)/DoD CIO. Department-wide waivers shall be granted for only the minimum length of time required to achieve compliance.