



HEALTH AFFAIRS

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-1200

OCT 10 2008

MEMORANDUM FOR: TRICARE MANAGEMENT ACTIVITY
PROGRAM EXECUTIVE OFFICER, JOINT MEDICAL
INFORMATION SYSTEMS OFFICE
TRICARE REGIONAL OFFICE – NORTH
TRICARE REGIONAL OFFICE – SOUTH
TRICARE REGIONAL OFFICE – WEST

SUBJECT: Military Health System (MHS) Information Assurance (IA) Policy Guidance
and MHS IA Implementation Guides

In accordance with Assistant Secretary of Defense (Health Affairs) (ASD (HA)) memorandum, "Military Health System (MHS) Information Assurance (IA) Implementation Guides," dated July 19, 2005, this office has completed a review of the MHS IA Implementation Guides. As a result, the following documents have been updated:

- Implementation Guide No. 1, "Governance"
- Implementation Guide No. 2, "Sanitization"
- Implementation Guide No. 3, "Incident Reporting"
- Implementation Guide No. 4, "Employee Behavior"
- Implementation Guide No. 7, "Data Integrity"
- Implementation Guide No. 9, "Configuration Management"
- Implementation Guide No. 10, "System Life Cycle Management"
- Implementation Guide No. 11, "Public Key Infrastructure (PKI) and PK Enabling"
- Implementation Guide No. 12, "IAVM Program"
- Implementation Guide No. 13, "IA Training, Education and Awareness"
- Implementation Guide No. 14, "INFOCON"

The MHS IA Implementation Guides were developed in collaboration with the MHS IA Working Group, and staffed, coordinated, and approved by the Enterprise Architecture Board.

The provisions of the MHS IA Implementation Guides are policy for all TRICARE Management Activity (TMA) Directorates, TRICARE Regional Offices (TROs), and the Joint Medical Information Systems (JMIS) Office.

For TRICARE Contractors, these documents are policy if required by contract; otherwise, they serve as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate these documents into their information assurance policies and procedures.

For additional information, please contact Ms. Dorothy S. Williams, Chief, MHS IA Program at (703) 681-7735 or via e-mail at dorothy.williams@tma.osd.mil.



Charles M. Campbell
Chief Information Officer
Military Health System

Attachments:
As stated

cc:
Deputy Surgeon General of the Army
Deputy Surgeon General of the Navy
Deputy Surgeon General of the Air Force

 <p>MILITARY HEALTH SYSTEM (MHS)</p> <p>INFORMATION ASSURANCE (IA)</p> <p>IMPLEMENTATION GUIDE</p>	IMPLEMENTATION GUIDE No. 11	
	EFFECTIVE DATE 07/19/05	REVISED DATE xx/xx/xx
<p>Subject:</p> <p>DoD PUBLIC KEY INFRASTRUCTURE (PKI) AND PUBLIC KEY ENABLING (PKE)</p>		

1 PURPOSE AND SCOPE

The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (TRICARE Management Activity (TMA) Directorates; TRICARE Regional Offices (TRO), and the Program Executive Office (PEO), Joint Medical Information Systems Office (JMISO)) (hereafter referred to as the TMA Component(s)). For TRICARE Contractors, this document is policy if required by contract; otherwise it serves as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance polices and procedures.

- 1.1 Public Key Infrastructure (PKI) is a technology consisting of a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances that are important in protecting sensitive communications and transactions. PKI brings to the electronic world the security and confidentiality features provided by the physical documents, hand-written signatures, sealed envelopes, and established trust relationships of traditional, paper-based transactions. These features are:
 - a. Confidentiality – ensures that only intended recipients can read files (sealed envelope).
 - b. Data Integrity – ensures that files cannot be changed without detection (hand-written signature and sealed envelope).
 - c. Authentication – ensures that participants in an electronic transaction are who they claim to be (hand-written signature).
 - d. Non-repudiation – prevents participants from denying involvement in an electronic transaction (established trust relationships and registered mail).
- 1.2 This implementation guide provides guidance for accomplishing DoD PKI/Public Key Enabling (PKE) activities within the MHS and supplements that provided in reference (b).
- 1.3 This guide is applicable to all TMA Centrally Managed ISs and networks and ISs and networks developed and operated by TMA, including contracted services.

2 POLICY

MHS shall follow current DoD PKI and PKE policy. Current DoD PKI/PKE policies may be newer than the references contained in this guide. Service managed ISs and networks are governed by individual Service policy and guidance.

3 PROCEDURES

3.1 Program Managers (PMs) are responsible for:

3.1.1 Ensuring DoD PKI/PKE requirements for private Web servers are met. Procedures include:

- a. Identifying DoD private Web servers under their cognizance.
- b. Requesting, installing, and maintaining the DoD PKI server certificate, and enabling its use to identify the server and to protect the transmissions between the server and the client's browser.
- c. Ensuring that DoD certificates are used for their intended Web server and are not placed on any other server or system.
- d. Relying on DoD-approved PKI certificates for client authentication to the DoD private Web server per DoD PKI/PKE policy. PKI user authentication includes validating that the certificate is from a trusted source, has not expired, or has not been revoked.
- e. Providing a transition period for Web server users to be able to move from the current authentication method to use of PKI.

3.1.2 Ensuring DoD PKI requirements are included in contracts and met by the contractor.

3.1.3 Ensuring DoD PKI is employed when the application requires a service that DoD PKI supports (e.g., strong authentication, digital signature, and data integrity). PMs should complete a Business Case Analysis (BCA) to substantiate the use of a PKI service before committing to PK enabling an application.

3.1.4 Verifying application/system compatibility with DoD PKI by conducting interoperability and compatibility testing except for commercial off-the-shelf (COTS) products already tested by DoD or a Component.

3.1.5 Ensuring that applications and systems that are PK-enabled as a result of a BCA meet the DoD policy requirements for PKI and PKE, and these are met by the DoD-set milestone dates. Lack of time, planning, or resources are usually not an acceptable justification for missing a milestone date.

3.2 Managers of MHS government networks are responsible for:

3.2.1 Enabling their network(s) to rely on DoD-approved PKI certificates contained on a DoD-approved hardware token (e.g., Common Access Card (CAC)) for user authentication and access control to the network per DoD PKI/PKE policy. PKI user authentication includes

validating that the certificate is from a trusted source, has not expired, and has not been revoked.

- 3.2.2 Ensuring DoD PKI/PKE requirements for private Web servers on their network(s) are met. Procedures include:
 - a. Identifying DoD private Web servers under their cognizance.
 - b. Requesting, installing, and maintaining the DoD PKI server certificate, and enabling its use to identify the server and to protect the transmissions between the server and the client's browser.
 - c. Relying on DoD-approved PKI certificates for client authentication to the DoD private Web server per DoD PKI/PKE policy. PKI user authentication includes validating that the certificate is from a trusted source, has not expired, and has not been revoked.
 - d. Ensuring that DoD certificates are used for their intended Web server, system, device, etc., and are not placed on any other server or system.
- 3.2.3 Verifying network-provided application/system compatibility with DoD PKI by conducting interoperability and compatibility testing except for COTS products already tested by DoD or a Component.
- 3.2.4 Ensuring e-mail, including Web-based e-mail, is capable of using DoD PKI certificates for digital signature and encryption. This includes relying on DoD-approved PKI certificates for user authentication to the e-mail private Web server.
- 3.2.5 Ensuring network workstations and network provided remote access laptops have CAC readers and middleware installed to support PKI per DoD PKI/PKE policy.
- 3.2.6 Providing personnel training on the correct use and protection of the PKI certificate.
- 3.2.7 Incorporating PKI into the network's security documents and having them available for Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) reviews, such as procedures and guidance for handling access to the network when a PKI certificate is not available for a user including priority and emergency access.
- 3.3 MHS/TMA users of PKI are responsible for:
 - 3.3.1 Using their DoD PKI certificate for DoD business only.
 - 3.3.2 Protecting their PKI certificates.
 - a. An individual's certificate or Personal Identification Number (PIN) shall not be shared, regardless of certificate storage method or location.
 - b. Maintaining control of the PKI certificate token at all times. If the PKI certificate is stored on a hardware token, the user must remove the PKI token from the workstation and take the token with them whenever they leave the immediate area of the workstation.

- c. Protecting the PIN used to access the user's PKI certificates as they would any password (e.g., memorize the PIN and not write it down or post on terminals or blackboards; do not tell any other user or person what the PIN is).
- 3.3.3 Reporting to a CAC PIN reset facility as soon as possible after three consecutive unsuccessful attempts at entering the correct PIN locks the CAC.
- a. TMA users of the Health Affairs (HA)/TMA Network should contact the TMA Office of Administration for directions to the proper CAC PIN reset facility.
 - b. HA users of the HA/TMA Network should contact HA Operations for directions to the proper CAC PIN reset facility.
 - c. MHS users not on the HA/TMA network should contact their Service's local command IA or network security official for the location of the CAC PIN reset facility.
- 3.3.4 Reporting to the immediate supervisor and designated office, as soon as possible upon recognizing that the event has occurred, any lost, missing, stolen, or compromised PKI certificates including a certificate PIN, whether stored on soft or hardware tokens.
- a. For TMA users of the HA/TMA Network, the designated office for reporting lost, missing, stolen, or compromised PKI certificates on CACs is the TMA Office of Administration.
 - b. For HA users of the HA/TMA Network, the designated office for reporting lost, missing, stolen, or compromised PKI certificates on CACs is HA Operations.
 - c. For users of the HA/TMA Network, the designated office for reporting lost, missing, or stolen PKI software certificates is the HA/TMA network Local Registration Authority (LRA) who issued their certificate.
 - d. For MHS users not on the HA/TMA network, the designated office is provided by the Service's local command IA guidance or network security guidance. At a minimum, the user should report the event to their supervisor and the local network security officer.
 - e. Users who suspect that the PIN has been compromised must go to the CAC PIN reset facility and have the PIN changed.
- 3.3.5 Obtaining a replacement PKI certificate for any lost, missing, stolen, compromised, or expired certificate/token.
- a. This includes resubmitting any required forms with signatures for approval in accordance with local guidance. A DD1172 form is required for a CAC.
 - b. For PKI certificates stored on DoD CACs, this involves traveling to a CAC issuance facility to obtain a replacement.
- 3.3.6 Following DoD PKI policy and Service/organization-specific guidance for when one should apply the user's PKI certificate for digitally signing and encrypting e-mail or digitally signing a document.

- 3.3.7 Following the application IA and PKI guidance and procedures to apply the user's PKI certificate for a transaction or data in an application.
- 3.4 Contractors accessing DoD networks or systems or doing electronic business with DoD from their own networks are responsible for:
 - 3.4.1 Using only DoD-approved certificates from an authorized DoD External Certificate Authority (ECA) when conducting electronic business that requires PKI with DoD.
 - a. Specific guidance requiring the use of DoD PKI shall be provided in contractual documents and correspondence.
 - b. Information on the DoD ECA program, including how to purchase DoD-approved ECA PKI certificates, can be found at <http://iase.disa.mil/pki/eca/index.html>.
 - c. DoD-approved ECA certificates are different from standard PKI certificates from vendors.
 - 3.4.2 Using DoD PKI ECA certificates only for authorized DoD business unless authorized by DoD for use with other DoD partners (federal, state, local governments, or contractors).
 - 3.4.3 Contractors shall establish IA guidance and procedures for controlling DoD ECA PKI certificates and have them available for DITSCAP reviews. These should at a minimum include:
 - a. Identifying personnel whose job function requires a DoD ECA PKI certificate.
 - b. Authorizing and purchasing a DoD-approved PKI certificate from a DoD ECA.
 - c. Tracking who is issued certificates, when issued, job function requiring PKI certificate, date of revocation, and reason for revocation.
 - d. Providing personnel training on the correct use of the PKI certificate.
 - e. Providing rules for their use (signing e-mail, access to DoD networks or systems, etc.), protection of the PIN, renewal, and handling compromise and revocation including loss or no longer required (job change, departure from company, etc.).
 - f. Assigning responsibilities for PKI management, ensuring technical matters are properly handled including removing certificates when no longer required or are revoked.
 - 3.4.4 Ensuring that DoD ECA certificates are not shared or used by anyone except the specific individual for whom the ECA authorized and provided the certificate.
 - 3.4.5 Ensuring that any compromised or no longer required certificate is reported in accordance with the ECA guidance and procedures where the certificate was purchased.
- 3.5 HA Operations and TMA Office of Administration are responsible for:
 - 3.5.1 Authorizing individuals (depending on their organization) who need a CAC with PKI certificates to access the HA/TMA Network and providing a list of CAC issuance facilities where individuals can go to receive their CACs with DoD PKI certificates.

- 3.5.2 Notifying the CAC issuance facility as soon as possible after being informed that a CAC is lost, stolen, or compromised to ensure that the certificates are revoked and that a new CAC and certificates are issued.
- 3.5.3 Notifying the CAC issuance facility when the CACs are collected from personnel who are no longer eligible so that the PKI certificates shall be properly disposed of and shall no longer be valid.

4 REFERENCES

- a. DoD Instruction 8520.2 “Public Key Infrastructure (PKI) and Public Key (PK) Enabling,” April 1, 2004
- b. Assistant Secretary of Defense (HA) Memorandum, “Military Health System Information Assurance Policy Guidance,” March 5, 2004
- c. DoD Chief Information Officer (CIO) Memorandum “Public Key Infrastructure (PKI) and Public Key Enabling (PKE),” October 7, 2003
- d. DoD Under Secretary of Defense for Personnel and Readiness Memorandum, “Common Access Card Issuance Mandate,” September 25, 2003
- e. DoD Directive 8190.3, “Smart Card Technology,” August 31, 2002
- f. Assistant Secretary of Defense Memorandum, “Guidance and Provisions for Developing Department of Defense (DoD) Component’s Public Key Enabling (PKE) Policy Compliance Waiver Process,” August 5, 2002
- g. Assistant Secretary of Defense Memorandum, “Public Key Infrastructure (PKI) Policy Update,” May 21, 2002
- h. DoD CIO Memorandum, “Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD),” May 17, 2001
- i. DoD CIO Memorandum, “Common Access Card,” January 16, 2001
- j. DoD CIO Memorandum, “Department of Defense (DoD) Public Key Infrastructure (PKI),” August 12, 2000
- k. DEPSECDEF Memorandum, “Smart Card Adoption and Implementation,” November 10, 1999
- l. DoDI 5230.29, “Security and Policy Review of DoD information for Public Release,” August 6, 1999
- m. DoDD 5230.9, “Clearance of DoD Information for Public Release,” April 9, 1996
- n. Federal Information Security Management Act of 2002

5 ACRONYMS

- BCABusiness Case Analysis
- CACCommon Access Card

CIO.....	Chief Information Officer
COTS	Commercial Off-the-Shelf
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DoD.....	Department of Defense
ECA.....	External Certificate Authority
HA.....	Health Affairs
IA	Information Assurance
IS.....	Information System
JMISO.....	Joint Medical Information Systems Office
LRA.....	Local Registration Authority
MHS.....	Military Health System
PEO.....	Program Executive Office
PIN	Personal Identification Number
PKE.....	Public Key Enabling
PKI.....	Public Key Infrastructure
PM.....	Program Manager
TMA.....	TRICARE Management Activity
TRO.....	TRICARE Regional Offices

6 DEFINITIONS

Common Access Card – A Department-wide smart card used as the standard 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 DoD Directive 8190.3, “Smart Card Technology,” dated August 31, 2002.

DoD Private Web Server (From DoDI 8520.2, “Public Key Infrastructure (PKI) and Public Key (PK) Enabling,” dated April 1, 2004) – For unclassified networks, a DoD private Web server is any DoD-owned, operated, or controlled Web server providing access to official information that has not been reviewed and approved for release in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29. 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.

Token (From DoDI 8520.2) – A portable, user-controlled, physical device used to generate, store, and protect cryptographic information, and perform cryptographic functions.