

**12 JULY 2004**



**Communications and Information**

**IDENTITY MANAGEMENT**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>

---

OPR: HQ AFCA/WFP (SMSgt Vincent Jones)

Certified by: HQ USAF/XIC  
(Maj Gen Charles E. Croom)

Pages: 18

Distribution: F

---

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*) and directs the use of the Department of Defense (DoD) Public Key Infrastructure (PKI), outlines capabilities, assigns responsibilities for the use and management of PKI functions within the Air Force, and establishes Air Force PKI usage and registration requirements. This instruction applies to all Air Force military, civilians, and contractor personnel under contract by the DoD, who develop, acquire, deliver, use, operate, or manage Air Force information systems. This document takes precedence over all conflicting Air Force documents. Additional instructions and manuals are listed on the Air Force Publishing Web site at Uniform Resource Locator (URL):

<http://www.e-publishing.af.mil> under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct questions or comments on the contents of this instruction through appropriate command channels to Headquarters Air Force Communications Agency (HQ AFCA/WFP), 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications to HQ AFCA/ITXD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/WFP, and Headquarters United States Air Force (HQ USAF/XIC), 1800 Air Force Pentagon, Washington DC 20330-1800. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records*, and disposed of in accordance with Air Force Web-RIMS *Records Disposition Schedule (RDS)* located at

<https://webrims.amc.af.mil/rds/index.cfm>. Public Law 104-13, *The Paperwork Reduction Act of 1995* and AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*, affect this publication. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. See **Attachment 1** for a glossary of references and supporting information.

**This is the initial publication of Air Force Instruction (AFI) 33-213.**

## 1. Introduction.

1.1. Assistant Secretary of Defense (ASD) Command, Control, Communications, and Intelligence (C3I) Memorandum, *Department of Defense (DoD) Public Key Infrastructure (PKI)*, dated August 12, 2000, mandates the implementation and use of a DoD PKI across the services and updates previous DoD PKI policy to align with the DoD Common Access Card (CAC) programs. This instruction implements Air Force Chief Information Officer (AF-CIO) Memorandum, *AF Public Key Infrastructure (AF PKI) Guidance*, 29 March 1999, which provided high-level guidance on Air Force implementation of the DoD PKI. Deputy Secretary of Defense (DEPSECDEF) Memorandum, *Smart Card Adoption and Implementation*, November 10, 1999, mandated the CAC (the new military/civilian identification [ID] card) as the primary token for DoD PKI certificates. ASD(C3I) Memorandum, *Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD)*, dated May 17, 2001 provides guidance for the PKE of applications. ASD(C3I) Memorandum, *Public Key Infrastructure (PKI) Policy Update*, May 21, 2002, updated the August 12, 2000 DoD PKI policy and the May 17, 2001 PKE guidance.

**NOTE:** ASD(C3I) is now the Assistant Secretary of Defense, Networks and Information Integration (NII). ASD(NII) Memorandum, *Public Key Infrastructure (PKI) and Public Key Enabling (PKE) Implementation Update*, October 7, 2003, updates and outlines plans for updating these memorandums.

1.2. The DoD PKI provides public/private key pair generation, key distribution, key recovery, certificate generation and revocation, and certificate management services to subscribers (end users and devices) of PK-enabled systems and applications. The DoD PKI has two basic components: certificate management and user registration. The National Security Agency and the Defense Information Systems Agency (DISA) provide the certificate management. The services and agencies provide user registration capabilities. All Air Force users of PK technology must use the DoD PKI and register with a DoD PKI registration authority (RA). Each user will be issued an identity certificate (used for digital signature and authentication functions), an electronic mail (E-mail) signing certificate (used to sign E-mail), and an encryption certificate (to support data confidentiality), along with the associated private key for each certificate. Related to, but not part of the PKI, are directory services. All individual DoD PKI certificates will be posted to the Global Directory Service operated by DISA. The Air Force Directory Service is under development and will be the primary repository and source for PKI certificates issued to Air Force personnel.

1.3. The goal of the DoD PKI is to implement a single PKI that will encompass all DoD PKI requirements. Because of security implications, there will be parallel implementations of the DoD PKI on networks of differing classification. Except where otherwise stated, this policy applies to both the Non-Secure Internet Protocol Router Network (NIPRNET) and the SECRET Internet Protocol Router Network (SIPRNET) implementations of PKI. This policy does not apply to the use or implementation of PKI services supporting the Multi-Level Information System Security Initiative (MISSI) FORTEZZA card used by the Defense Message System High Grade Service. This policy does not address the process of issuing PKI certificates on or providing password or other security controls for the CAC or FORTEZZA card (refer to AFI 33-113, *Managing Air Force Messaging Centers*).

1.4. PKI certificates and private keys will be stored on devices known as tokens. There are two types of tokens: Hardware such as the CAC and FORTEZZA card, and software which is a floppy disk or other standard computer read-write media which provides no security beyond that provided by the operating system. PKI assurance levels are grouped in classes and defined in the DoD Certification Policy (ASD (C3I), *X.509 Certificate Policy for the United States Department of Defense*). The current

level of assurance of the DoD PKI is Class 3. Ultimately, the MISSI FORTEZZA PKI and DoD PKI will merge into a single PKI referred to as "Target CLASS 4." The primary token for the individual PKI keys and certificates on the NIPRNET will be the CAC, which are issued via the DoD Identification Card System. All PKI certificates and any other certificates not supported on the CAC use the registration infrastructure described in this instruction.

## **2. Use of Department of Defense (DoD) Public Key Infrastructure (PKI).**

2.1. All computer applications, systems, servers, and networks used within the Air Force that incorporate or rely on PK technology (data encryption, identification and authentication, and digital signature capabilities) shall use the DoD PKI for certificate (key) support. Exceptions to this direction require AF-CIO approval. MAJCOM validated exception requests will be forwarded through HQ AFCA/WFP.

2.2. Any organization that intends to implement a PK-enabled application which requires accelerated PKI registration support will contact the Air Force lead command. The lead command will then contact the Air Force PKI System Program Office (SPO) to determine the type and magnitude of support required. If the requirement is supportable, the lead command will forward the requirement to HQ USAF/XIC for approval actions. Points of contact for technical support are identified on the Air Force PKI web site at <https://afpki.lackland.af.mil/html/appdevs.html>.

2.3. DoD entities eligible for registration into the DoD PKI include active duty and reserve military, civilian employees, and contractor employees who are working in government spaces or using government-furnished computer equipment.

2.4. Contractor employees not covered in paragraph 2.3. and business partners of the DoD who require PKI certificates to conduct business with the DoD, must obtain them from DoD-established or DoD-recognized External Certification Authorities (ECA). (ECA information is available at <http://www.disa.mil/pao/products/pki.html>).

2.5. In addition to individual certificates, the DoD PKI can issue code signing, device, and group/role certificates. Certificates must be issued to DoD employees, DoD owned devices or group/role entities comprised of DoD employees.

2.6. Attribute authority for code signing is AFCA/CC. Attribute authority for group/role base is any organization commander or any staff section principle in the grade of GS-15/colonel or above.

## **3. Responsibilities.**

3.1. HQ USAF/XI will:

3.1.1. Develop policy and guidance governing Air Force use of PKI.

3.1.2. Provide Air Force representation to the DoD Certificate Policy Management Working Group and other appropriate working groups.

3.1.3. Sponsor Air Force certification practice statements (CPS) through the DoD Certificate Policy compliance process.

3.2. HQ USAF/IL will: Conduct Training Planning Team meetings with AFCA, major command (MAJCOM), field operating agency (FOA), direct reporting unit (DRU), and Air Education and

Training Command (AETC) to identify new training requirements. Develop course training plans and course training standards.

3.3. HQ AFCA will:

- 3.3.1. Serve as the Air Force lead command for the USAF implementation of PKI (see AFI 10-901, *Lead Operating Command--Communications and Information Systems Management*).
- 3.3.2. Develop, in coordination with participating and operating commands, the operational and maintenance concepts for all aspects of PKI.
- 3.3.3. Review, evaluate, and interpret DoD PKI policy and doctrine, and make recommendations on implementation, management, and use of the PKI in the Air Force.
- 3.3.4. Identify, prioritize, and document PKI user requirements in conjunction with the MAJCOMs, FOAs, and DRUs.
- 3.3.5. Lead Air Force PKI working groups and provide USAF representation at DoD/Joint PKI working groups when requested by HQ USAF/XI.
- 3.3.6. Advocate and coordinate Air Force PKI manpower requirements with operating and participating commands.
- 3.3.7. Maintain a list of recommended commercial-off-the-shelf products supporting PK-enabled solutions using the Infostructure Technology Reference Model (i-TRM) process.

3.4. MAJCOMs will:

- 3.4.1. Ensure all eligible Air Force personnel receive their DoD PKI certificates and support agreements are modified or developed for issuance and control of certificates to eligible non-Air Force DoD members.
- 3.4.2. Provide resources for user registration and certificate revocation necessary to support NIPRNET and SIPRNET software certificate requirements including device registration. The sponsoring MAJCOM will negotiate with all other MAJCOMs to obtain lateral registration support, if required.
- 3.4.3. Include additional manpower required for permanent PKI user registration support in the Program Objective Memorandum (POM) submission according to Air Force POM guidance.
- 3.4.4. Establish a network of local registration authorities (LRA) and trusted agents (TA) sufficient to provide coverage for all MAJCOM facilities in support of classified systems, to provide device certificates on classified and unclassified networks, and to provide other than CAC-based certificate support on the NIPRNET. Identify personnel to perform LRA and TA duties as required and coordinate with the Air Force PKI SPO for LRA training and specific guidance.
- 3.4.5. Identify the need and establish LRAs and TAs required to provide PKI user registration and certificate management support to deployed, mobile, contingency, tactical, and Air Force-supported commander-in-chief users. The LRA and TA selection criteria is available from the Air Force PKI SPO.
- 3.4.6. Ensure LRAs and TAs are complying with the Air Force LRA CPS and the X.509 Certificate Policy.

3.5. Air Force Materiel Command (AFMC) has established a PKI program office to implement the Air Force portion of the DoD PKI. The Air Force PKI SPO will:

3.5.1. Deploy the necessary registration capability to support Air Force PKI requirements not covered by Defense Enrollment Eligibility Reporting System (DEERS)/Real-Time Automated Personnel Identification System (RAPIDS) issuance of the CAC.

3.5.2. Ensure Air Force segment of non-DEERS/RAPIDS registration infrastructure is upgraded consistent with release levels of the DoD PKI.

3.5.3. Provide training for LRAs until such time as the training function migrates to AETC.

3.5.4. Provide guidance and engineering assistance to all Air Force organizations implementing PK-enabled applications within allowed resource constraints.

3.6. USAF RA, Headquarters Electronic Systems Center, Network Services Division (HQ ESC/DIW) will:

3.6.1. Approve properly validated certificate requests for all required Air Force network servers and devices submitted to the DoD Certification Authority (CA).

3.6.2. Specify training requirements for Air Force LRAs and TAs.

3.6.3. Authenticate qualified LRAs to the CA and issue the LRA credentials to the LRA.

3.6.4. Authorize Air Force LRAs to collect and verify subscriber's identity and submit information directly to the CA.

3.6.5. Develop Air Force certificate practice statements (except those required for FORTEZZA).

3.6.6. Oversee Air Force registration infrastructure compliance with the DoD Certificate Policy and all approved practice statements.

3.6.7. Sponsor and maintain oversight of the Air Force PKI Helpdesk.

3.6.8. Ensure registration support is provided for validated requirements.

3.6.9. Authenticate code-signing certificates for Air Force code signers.

**NOTE:** Specific RA, LRA, and TA responsibilities are outlined in the Air Force LRA CPS available on the Air Force PKI web site (a valid DoD PKI certificate is required to access this information). For informational purposes, a TA outline is provided at [Attachment 2](#).

**NOTE:** Refer to [Figure 1](#) for a diagram of the Air Force PKI management structure.

3.7. End Users will:

3.7.1. Provide security (according to paragraph [6.3](#)) for all tokens containing PKI certificates and associated private key issued to them.

3.7.2. Digitally sign E-mail, once the capability is available, in accordance with Air Force guidance (<https://afpki.jackland.af.mil>). ASD (C3I) memorandum, *Public Key Infrastructure (PKI) Policy Update*, May 21, 2002, mandates digitally signing of all .mil E-mail. ASD (NII) Memorandum, *Public Key Infrastructure (PKI) and Public Key Enabling (PKE) Implementation Update*, October 7, 2003, allows Components to modify or adjust their implementation dates. Office of the Secretary of Defense (OSD) direction is available at

<http://www.defenselink.mil/nii/org/sio/ia/pki/>. See AFI 33-119, *Electronic Mail (E-mail) Management and Use*, for additional guidance. Encryption is encouraged but not required.

3.7.3. Maintain currency of certificates by ensuring certificate renewal before expiration.

3.8. Information Technology Executive Agents and designated IT managers will:

**NOTE:** The term "information technology," with respect to an executive agency means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, interchange, transmission, or reception of data or information by the executive agency. (Source: DoD IT Registry Implementing Instructions)

3.8.1. Register for, obtain, and use DoD PKI certificates for all private web servers. ASD(C3I) Memorandum, *Public Key Enabling (PKE) of Applications, Web Servers, and Networks for DoD*, May 17, 2001, directs the enabling of all private web servers to use DoD PKI certificates for servers and client/user authentication.

3.8.2. The AF-CIO has authority to issue waivers to PKE policy for individual applications on a case-by-case basis, consistent with the waiver guidelines and provisions published by Defense-wide Information Assurance Program (DIAP). Waivers shall be granted only for the minimum length of time required to achieve compliance. Approved waivers shall be reported to the DoD CIO within 15 days of approval.

3.8.3. All requests for waivers to this instruction will be submitted through Information Assurance (IA) organizational channels, including the MAJCOM IA to the MAJCOM SC, then to HQ AFCA/WF. Requests must include supporting documentation with specifics on what aspect of the policy is being waived, specific reason for needing the waiver, the duration of the waiver - when will compliance with policy be possible, and the Mission Category (Mission Category I, II, or III) of the system affected by the waiver. Documentation will include, if the request is for a permanent waiver, what is the reason for it to be permanent (most likely cost), and impact of denying the waiver. Waiver request will be signed by MAJCOM SC or equivalent. After review for completeness, etc., HQ AFCA/WF will forward the package, with HQ AFCA's recommendation, to HQ USAF/XI for processing at the appropriate level.

3.8.4. Ensure PK-enabled Air Force Information Technology is tested for DoD PKI interoperability. The Joint Interoperability Test Command (JITC), Ft. Huachuca AZ, offers this testing on a fee-for-service basis.

3.8.5. All Air Force systems and computer applications must be registered in the Air Force Systems Compliance Database (SCD). If the systems and computer applications use or will use PK technology, it will be so stated in the SCD. This does not include previously PK-enabled commercial-off-the-shelf (COTS) products such as Web browsers and E-mail. The SCD is located at URL: <https://scd.scott.af.mil>. Entry in the SCD will allow capture and reporting compliance data to ASD(NII) (formerly ASD[C3I]) on an annual basis.

3.8.6. Implement client authentication process supported by DoD PKI certificates on all private Web servers on unclassified networks according to timelines established by OSD. OSD direction is available at <http://www.defenselink.mil/nii/org/sio/ia/pki/>.

3.8.7. Enable all unclassified networks for hardware token, certificate-based access control according to timelines established by OSD. OSD direction is available at <http://www.defenselink.mil/nii/org/sio/ia/pki/>.

3.8.8. Migrate unclassified networks hosting mission critical systems to Release 4 certificate-based access control according to OSD established timelines. OSD direction is available at <http://www.defenselink.mil/nii/org/sio/ia/pki/>.

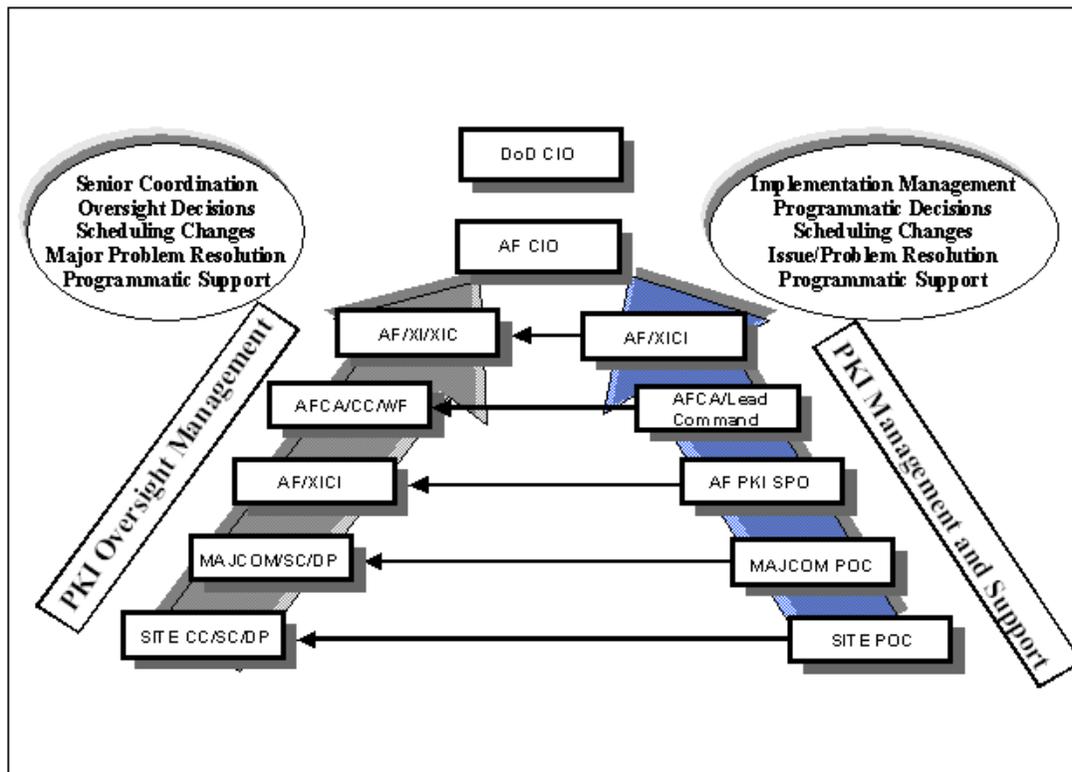
3.8.9. Ensure all PK-enabled capabilities use National Institute of Standards and Technology (NIST) (Federal Information Processing Standards [FIPS]-140) validated cryptographic modules.

3.8.10. Program management offices and SPOs deploying PK-enabled systems/applications shall coordinate with their target audiences/locations and the Air Force PKI RA to ensure user registration and certificate support functionality is available.

3.8.11. Evaluate all legacy, new, and planned systems and applications to determine if they would benefit from the use of PK technology and conduct economic analysis to determine if PKE is warranted.

3.8.12. Ensure resources are provided and end user training is conducted for all PK-enabled systems and applications.

**Figure 1. Air Force PKI Management Structure.**



#### 4. Registration.

4.1. The primary unclassified PKI token is the CAC. Verifying official (VO) assigned to the military personnel flight will issue DoD PKI certificates contained on the CAC. Until individual registration functions are available at Air Force military personnel flights, registration support for DoD and HQ USAF/XIC-validated requirements must be negotiated with the Air Force PKI SPO. The primary token to support these requirements will be the CAC when possible. When software tokens (certificates on floppy disks) are required, the requiring MAJCOM/user will develop a CAC migration plan

or provide justification to maintain use of software tokens. All PKI registration on the SIPRNET uses the LRA/TA model described in paragraph 4.2.

4.2. LRA personnel will facilitate issuing individual certificates, Group/Role based certificates, and device certificates on both NIPRNET and SIPRNET. The need for LRAs to support the individual certificates on the NIPRNET infrastructure will be reevaluated as the CAC reaches full deployment. To assist in the face-to-face verification of identity at geographically remote USAF sites or locations where LRAs are not currently assigned, LRAs or RAs may use TAs (see [Attachment 2](#)). The MAJCOM must determine the need to use LRAs, TAs, or a combination based on the number of certificates that must be issued and maintained at a location. When LRAs are required, MAJCOMs will obtain HQ USAF/XIC approval through HQ AFCA/WFP and coordinate with the USAF PKI SPO to obtain LRA workstations and training. TA candidates will be appointed by their organization in coordination with the RA or LRA they will support. TAs will be trained by the RA or LRA they support. Training guidance is available at the Air Force PKI web site (<https://afpki.lackland.af.mil/html/training.html>).

4.3. When an LRA is required, LRA user registration duties should be assigned as an additional duty to personnel within the supporting communications flight/squadron at the host base. Services provided by and/or required of LRAs should come from the same set of assets that provide other information technology services for a base. However, giving consideration to availability of personnel, the wing commander may place these registration responsibilities where resources allow. Depending on the number of software certificates to be issued, LRA duties may require full-time attention for a short period of time. As certificate registration is accomplished in conjunction with issuance of the CAC, it is expected that LRAs will have a significantly reduced workload. After the initial registration of PKI users, LRA services should be implemented via the normal support request mechanisms used for other information technology services.

4.4. All LRA candidates shall complete formal training. They must complete DD Form 2841, **Department of Defense (DoD) Public Key Infrastructure (PKI) Registration Official Certificate of Acceptance and Acknowledgement of Responsibilities**, which is approved by the Air Force Class 3 PKI RA. The candidates must obtain coordination from the Air Force PKI SPO prior to performing LRA registration duties. MAJCOMs must contact the Air Force PKI SPO to obtain LRA equipment, training quotas, and to schedule personnel for LRA training. Procedures are available at <https://afpki.lackland.af.mil/html/training.html>.

## 5. Certificate Issuance and Control.

5.1. LRAs will register users to receive certificates on a floppy disk. This is distinctly separate from the CAC issued by a DEERS/RAPIDS VO that will be described in a separate AFI. The files placed on the floppy disk containing the certificate and private key are protected/encrypted with a password of the end user's choosing. This password shall include upper case, lower case letters and numbers and shall be a maximum of 14 characters in length. Because they are not compatible with some applications, special characters (e.g., !@#\$%^&\*) must NOT be included in passwords. This is an approved deviation to AFMAN 33-223, *Identification and Authentication*.

5.2. The LRA shall use the registration practices defined in the Air Force LRA CPS that can be found on the Air Force PKI web page ([https://afpki.lackland.af.mil/html/lra\\_ta.html](https://afpki.lackland.af.mil/html/lra_ta.html)). The certificate registration process requires the LRA to enter the user's identity information into the LRA software, upload the information to the CA, and print a certificate registration instructions (CRI) sheet. The CRI

contains the end user's 10-digit user ID number, one-time password, and instructions for downloading their certificates. The process creates a one-time login account for the user at the CA. The user must then download their certificate using Netscape Browser Communicator 4.73 + (4.79 recommended) along with the Personal Security Manager (PSM) 1.2 or higher or Netscape 7.x (7.1 recommended). The certificate file(s) is/are placed on a floppy disk in password-protected files (PKCS#12). Neither Netscape 6.x nor Microsoft Internet Explorer can be used for this function. The Netscape PSM module functions with the CA to provide automatic escrow of the E-mail key management key (private key associated with the encryption certificate) in accordance with DoD Certificate Policy. Recovery of these escrowed key management keys will be done according to the DoD Key Recovery Policy and associated practice statements.

5.3. The LRA may choose to issue certificates to users singularly or in groups depending on how many users must be served and in what timeframe this needs to be accomplished. New systems requiring issuance of software-based PKI tokens must receive approval from HQ USAF/XIC. Support requirements for mass issuance should be addressed to the Air Force PKI SPO via instructions on the web page identified in paragraph 4.4. Various registration approaches are covered in detail during LRA training.

5.3.1. Standard Issue of Software PKI Certificates. The LRA issues the end-user their CRI either directly or through a TA. The downloading instructions of the CRI should be used at a workstation provided by the LRA to download end-user certificates. The download process requires software as specified in paragraph 5.2. This software is not commonly found on Air Force desktops.

5.3.2. Kiosk Approach. When a large number of certificates must be issued, a kiosk may be the best option. A kiosk used for issuing PKI certificates is an arrangement of workstations and personnel to efficiently assist users with downloading their DoD PKI certificates and private keys to a token (e.g., floppy disk or other device). In the kiosk approach, an LRA creates and provides the CRI to the user as before. Users then proceed to the kiosk area where they are provided assistance with downloading their certificates and private key to a token.

5.4. Validation of Authority to Obtain DoD PKI Certificates. There is no requirement for validation of authority for individual members of the armed services or any DoD employee. DoD PKI certificates shall be issued to all active duty military personnel, members of the Selected Reserve, DoD civilian employees and eligible contractor personnel. The government contract manager, contracting officer technical representative, or contracting officer must validate to the LRA/TA the requirement for a contractor employee to obtain DoD PKI certificates. They will submit an official memo to the LRA/TA stating that the contractor employee works in government spaces or uses government-furnished computer equipment. This documentation will be filed with the DD Form 2842, **Department of Defense (DoD) Public Key Infrastructure (PKI) Subscriber Certificate of Acceptance and Acknowledgement of Responsibilities**. The appropriate attribute authority as identified in paragraph 2.6. must validate Code Signing, Group and Role based certificates. File requirement validation documentation with the DD Form 2842.

5.5. Before the user is given the CRI or provided any DoD certificates, the user is required to read and sign DD Form 2842. The LRA or TA witnesses this signature and verifies the identity of the person with a Federal Government-issued picture ID. In the case of contractor employees who do not have a Federal Government picture ID, two non-Federal forms of ID may be used; one of which must be a picture ID. The DD Form 2842 is then filed by the issuing LRA (TAs must return this form to the issuing RA or LRA). Should this document be required at any time, a copy must be available from the

issuing RA/LRA. The original DoD acknowledgement of responsibilities document used prior to the DD Form 2842 does not need to be replaced in the RA/LRA files; however, all new certificates require the DD Form 2842.

5.6. Issuance and control of PKI certificates is under the policy direction of the DoD. Air Force LRAs and TAs must comply with the detailed policy and procedures in the currently approved "USAF Local Registration Authority (LRA) Certification Practice Statement" which is available at the Air Force PKI SPO web site: (<https://afpki.lackland.af.mil>). Additional procedural and training material is also available from this site.

## 6. Token Handling and Protection.

6.1. DoD PKI certificates and associated private keys are stored on tokens. As the DoD CAC is fielded, it will be the primary token for individual certificates and private keys for use with unclassified applications and on unclassified networks. Tokens other than the CAC will be used to support users of classified applications and on classified networks as well as unclassified applications/network users prior to the full implementation of the CAC. There will be an overlap period where individual certificates and private keys for the unclassified network may be issued on more than one token. To preclude unauthorized access to and compromise of the individual's private key, physical protection and access controls (outlined in paragraphs 6.2. and 6.3.) will apply to these tokens.

6.2. The DoD Certificate Policy and the implementing CPS form the basis for security practices to be applied to private key issued via the DoD PKI. These documents are available on the Air Force PKI web site (<https://afpki.lackland.af.mil/html/pubs.html>). The DoD Certificate Policy requires that: **"No one shall have access to a private signing key but the Subscriber"** and **"subscribers are obligated to protect their private keys at all times, as stipulated in their certificate acceptance agreement, and local procedures."** To comply with this policy, all tokens containing a private key must be password protected. See paragraph 5.1. for password composition.

6.3. Users must not share their password and must protect the token containing their private keys from unauthorized access at all times. Until certificates and associated private keys are distributed on hardware tokens, the private key, PK, certificate and signing chain for each certificate will be placed on a password-protected software token. The user or other responsible individuals to whom a PKI certificate is issued will provide appropriate protection for the token upon which it resides. Software tokens for unclassified use will be treated as sensitive, unclassified material, and provided protection using the procedures as stated in AFI 33-277, *FORTEZZA Operational Security*. Specific guidance follows:

**The password-protected unclassified software tokens will be safeguarded in a manner similar to a credit card or high value item in order to limit the possibility of loss, unauthorized use, substitution, tampering, or breakage. Individuals may carry these tokens in their possession, provided they are given the level of protection discussed in this paragraph. Tokens for classified use will be marked at the same classification as the system on which it is used and protected as classified material.**

6.4. Certificates issued to Role or Group accounts are special cases where more than one person may hold the private key. The Information System Security Officer (ISSO) or account sponsor must maintain documentation of who is in possession of such certificates at all times. Certificates, which do not

contain a person's name, may be held by more than one person and may not be relied on for non-repudiation or electronic commerce use.

**7. Key Compromise.** A DoD PKI certificate holder who suspects their private key has been compromised must notify their supporting TA, LRA, or the Air Force RA immediately using the most expeditious means available. The Air Force RA shall revoke certificates suspected of key compromise within 24 hours of notification.

**8. Certificate Revocation.** Revocation is necessary to terminate certificate use before its normal expiration date. Examples of reasons for revocations include private key compromise (e.g., a lost token), loss of trust in a user, changes in a user's legal name, or departure from DoD. If a user's ID certificate is revoked, all other certificates issued based on that ID certificate must also be revoked.

**9. Server Certificates.** The Air Force RA will approve issuance of Class 3 DoD PKI server certificates when an appropriate validation authority validates requirements. Specific instructions to obtain and load DoD server certificates are available on the Air Force PKI web site. The DoD Certificate Policy states that server certificates are used for workstations, guards and firewalls, routers, in-line network encryptors, trusted servers (e.g., database, file transfer protocol, and world wide web servers), and other infrastructure components that may require certificates. Each of these servers must be under the cognizance of a specific individual who accepts the certificate and is responsible for the protection and use of the associated private key. Appropriate validation authorities include LRAs or TAs.

**10. PK Enabling (PKE) of Applications.** The following information is provided to assist Air Force organizations implementing DoD policy regarding PKE and in determining whether supported applications should be considered for PKE. The following highlighted security services illustrate ways supported applications can employ PKI products and services. These examples provide criteria to assist in evaluating supported applications for PKE. The listed items are board service areas and not an exhaustive list of items PKI supported Air Force and DoD applications.

- 10.1. Perform user identity and authentication.
- 10.2. Provide data confidentiality.
- 10.3. Protect data integrity.
- 10.4. Provide nonrepudiation of origin and/or receipt.
- 10.5. Perform access control.

**11. PK Enabling (PKE) Required Applications:** Users of DoD electronic messaging (E-mail) are directed to follow current Air Force guidance for the use of PKI to sign and encrypt E-mail, (<https://afpki.lackland.af.mil>).

**NOTE:** For users with multiple E-mail accounts, the CAC PKI signing and encryption certificates are generally assigned to the user's primary E-mail account and the other accounts will use a software set of certificates.

**NOTE:** As technology evolves and the capability becomes available, users employing remote access or portable and handheld devices to send or receive E-mail will be expected to digitally sign or when necessary, encrypt E-mail.

**12. PK Enabling (PKE) Recommended Applications:** This listing identifies types of applications that information system owners should consider PKE:

- 12.1. Privacy Act materials.
- 12.2. Resource and Procurement Management.
- 12.3. Sensitive Medical Information.
- 12.4. Force Readiness.
- 12.5. Secure, classified or need-to-know information.
- 12.6. Weapons Targeting information.
- 12.7. Command, Control, Communications, Computers, and Intelligence (C4I) Information.
- 12.8. Network topographical information.
- 12.9. Access or identity controlled systems or applications.
- 12.10. Orders and other forms of command and control information.
- 12.11. DoD contract solicitations and responses.

**13. Encryption and Decryption.** Encryption using PKI encryption certificates currently applies only to E-mail. Users should refer to AFI 33-119 for guidance on when to encrypt E-mail traffic. If encrypt is used or if encrypted E-mails are received, users need to be aware of the periodic expiration of the certificates, currently every 3 years. Recommend users store E-mail in the unencrypted form or plan to de-encrypt encrypted E-mail prior to expiration of encryption certificate. Otherwise when the encryption certificate is needed the user will have to go through the key recovery process to gain the necessary keys to access encrypted E-mail.

#### **14. Certificate Reissue.**

14.1. Certificate expiration and reissue refer to the process for limiting the validity period of a certificate and its associated public/private key pair and providing for renewal or replacement prior to a certificate's expiration. Certificate owners needing continued PKI services must ensure their certificates are re-issued prior to the certificate expiration date in order to prevent disruption in service.

14.2. The process for obtaining a new identity certificate is the same as that used to obtain the original certificate. In addition to normal expiration, certificate owners require a new ID certificate when a distinguished name changes (e.g., a legal name change). Certificate owners must furnish their supporting registration official with the legal documentation substantiating a distinguished name change in order to revoke the existing ID certificate.

14.3. When the ID certificate is reissued or when the user's E-mail address changes, the E-mail signing and encryption certificates must be re-issued. The Users must retain their original E-mail encryption private key in order to read any encrypted E-mail they have received based on that certificate. This function is available even after a certificate is revoked. When maintaining confidentiality at the client is not required, it is recommended that users decrypt and save any E-mail that was encrypted with the old certificate prior to revocation. Recovery of E-mail encryption certificates will be possible using the procedures of the DoD Key Recovery Policy (KRP). Specifics will be posted to the Air Force PKI web site.

14.4. A server certificate must be reissued when the network distinguished name (domain name system entry) for the server changes or after 3 years.

**15. Information Collections, Records, and Forms or Information Management Tools (IMT).**

15.1. Information Collections: No information collections are created by this publication.

15.2. Records: Records pertaining to registration, issuance, and control of PKI certificates are created by this publication. Retain and dispose of these records according to Air Force Web-RIMS RDS, Table 33-28, Rules 1-11, located at <https://webrims.amc.af.mil/rds/index.cfm>.

15.3. Forms or IMTs: (Adopted and Prescribed).

15.3.1. Adopted Forms or IMTs: AF Form 847, **Recommendation for Change of Publication**; DD Form 2841, **Department of Defense (DoD) Public Key Infrastructure (PKI) Registration Official Certificate of Acceptance and Acknowledgement of Responsibilities**, and DD Form 2842, **Department of Defense (DoD) Public Key Infrastructure (PKI) Subscriber Certificate Of Acceptance and Acknowledgement of Responsibilities**.

15.3.2. Prescribed Forms or IMTs: No forms are prescribed by this publication.

WILLIAM T. HOBBS, Lt Gen, USAF  
DCS, Warfighting Integration

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

Public Law 104-13, *The Paperwork Reduction Act of 1995*

DEPSECDEF Memorandum, *Smart Card Adoption and Implementation*, November 10, 1999

*X.509 Certificate Policy for the United States Department of Defense* (current version),

<http://www.defenselink.mil/nii/org/sio/ia/pki>

ASD(C3I) Memorandum, *Public Key Infrastructure (PKI) Policy Update*, May 21, 2002

ASD(C3I) Memorandum, *Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the DoD*, May 17, 2001

ASD(C3I) Memorandum, *Department of Defense (DoD) Public Key Infrastructure {PKI}*, August 12, 2000

ASD(NII) Memorandum, *Public Key Infrastructure (PKI) and Public Key Enabling (PKE) Implementation Update*, October 7, 2003

AF-CIO Memorandum, *Air Force Public Key Infrastructure (AF PKI)) Guidance*, 29 March 1999

AFPD 33-2, *Information Protection* (will become *Information Assurance*)

AFI 10-901, *Lead Operating Command--Communications and Information Systems Management*

AFI 33-113, *Managing Air Force Messaging Centers*

AFI 33-119, *Electronic Mail (E-Mail) Management and Use*

AFI 33-277, *FORTEZZA Operational Security*

AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*

AFDIR 33-303, *Compendium of Communications and Information Terminology*

AFMAN 33-223, *Identification and Authentication*

AFMAN 37-123, *Management of Records*

Web-RIMS, *Records Disposition Schedule (RDS)*

**NOTE:** An additional source for referenced publications is the Air Force PKI Home Page at

<https://afpki.lackland.af.mil>

***Abbreviations and Acronyms***

**AETC**—Air Education and Training Command

**AFCA**—Air Force Communications Agency

**AF-CIO**—Air Force Chief Information Officer

**AFDIR**—Air Force Directive

**AFI**—Air Force Instruction

**AFMAN**—Air Force Manual

**AFPD**—Air Force Policy Directive

**ASD(C3I)**—Assistant Secretary of Defense, Command, Control, Communications, and Intelligence

**ASD(NII)**—Assistant Secretary of Defense, Networks and Information Integration

**CA**—Certification Authority

**CAC**—Common Access Card

**COTS**—Commercial Off The Shelf

**CPS**—Certification Practice Statement

**CRI**—Certificate Registration Instructions

**DEERS**—Defense Enrollment Eligibility Reporting System

**DEPSECDEF**—Deputy Secretary of Defense

**DISA**—Defense Information Systems Agency

**DoD**—Department of Defense

**DRU**—Direct Reporting Unit

**E-mail**—Electronic Mail

**ECA**—External Certification Authorities

**ESC**—Electronic Systems Center

**FIPS**—Federal Information Processing Standards

**FOA**—Field Operating Agency

**IA**—Information Assurance

**ID**—Identification

**i-TRM**—Infostructure Technology Reference Model

**JITC**—Joint Interoperability Test Command

**KRP**—Key Recovery Policy

**LRA**—Local Registration Authority

**MAJCOM**—Major Command

**MISSI**—Multi-Level Information System Security Initiative

**NIPRNET**—Non-Secure Internet Protocol Router Network

**NIST**—National Institute of Standards and Technology

**OSD**—Office of the Secretary of Defense

**PK**—Public Key

**PKE**—Public Key Enabling

**PKI**—Public Key Infrastructure

**POM**—Program Objective Memorandum

**PSM**—Personal Security Manager

**RA**—Registration Authority

**RAPIDS**—Real-Time Automated Personnel Identification System

**RDS**—Records Disposition Schedule

**SCD**—Systems Compliance Database

**SIPRNET**—SECRET Internet Protocol Router Network

**SPO**—System Program Office

**TA**—Trusted Agent

**URL**—Uniform Resource Locator

**USAF**—United States Air Force

**VO**—Verifying Official

*Terms*

**A listing of PKI terms is included in the DoD PKI Roadmap available on line at <http://iase.disa.mil/pki/roadmap.html>**

## Attachment 2

### LOCAL REGISTRATION AUTHORITY (RA) TRUSTED AGENTS

**NOTE:** In some instances, the Air Force RA may serve as a LRA and actually register users or devices. Thus the use of LRA in this attachment may, in some cases, also apply to the Air Force RA.

**A2.1. Purpose.** To outline policies and procedures for Air Force TAs supporting DoD Class 3 (Medium Assurance) PKI registrations.

A2.1.1. Air Force users require immediate support from the DoD PKI. There will not be LRAs at every location that require PKI registration support. The use of a TA to verify the identity of and provide information on users to LRAs allows an LRA to provide registration support over a broader area of responsibility. TAs are also empowered to validate an organization's need for DoD PKI server certificates. This is accomplished by signing the validation blocks of the DoD PKI server certificate requirement document before forwarding them to the RA (available at <https://afpki.lackland.af.mil> (under Quick Links)).

A2.1.2. To supplement the LRAs available within the Air Force, a procedure has been established whereby individuals act on behalf of the LRA to ensure the identity of individuals in a specific group or at a certain location is verified. The person performing in this role is called a TA. Please note that TAs will be retained after LRA capabilities are established to support registration of groups of individuals or users geographically separated from the responsible LRA.

**A2.2. Trusted Agent Background.** The following explanation of a PKI LRA is necessary to understand the role of an LRA TA. An LRA provides visual identification verification and electronic input of user information necessary for users to be registered with the DoD CA.

A2.2.1. The LRA verifies the identity of an individual and validates their need for PKI registration. Using an LRA registration workstation, the LRA inputs necessary user information to request a PKI user certificate. When the LRA completes the user information input, the workstation prints a single sheet of paper for each user with a user ID, one-time access code, the URL to contact the CA, and instructions on how to generate their key pairs, download, and save their certificate. This printout, the *DoD PKI Certificate Registration Instructions (CRI)*, is provided to each user.

A2.2.2. LRAs may not be able to personally validate, verify, or gather user information because of geographic separation or user community size. To assist and supplement wing-level LRAs, the Air Force is implementing an LRA TA policy. TAs are to be personally identified by, registered with, and responsible to the LRA they support. As a minimum, TAs will: (1) validate the need for a user to be registered, (2) verify the identity of each user, and (3) gather and forward to the LRA the information required for each individual to be registered with the CA. The LRA will formally register the users identified to them by the TA with the DoD CA and provide the registration printouts to the TA via protected means (e.g., certified mail, encrypted E-mail, etc.). At a minimum, print-outs shall be folded and stapled so as to cover sensitive user data (e.g., one-time access code, etc.) but leave the individual's name exposed at the top to facilitate distribution by the TA (lower third of the form folded over the middle third and stapled). The TA will then verify the identity of recipients, have them sign the acknowledgement of responsibilities forms, and distribute the CRI forms to users within their purview. The TA will then forward the completed acknowledgement of responsibilities forms to the LRA. LRAs and TAs are also authorized to provide a network connected workstation (personal computer

loaded with Netscape Communicator 4.73 or higher (4.76 recommended) along with the PSM 1.2 or higher. This allows the users to download their certificates and associated private key to a token when properly configured Netscape software is not available at the user's desktop computer. Using this workstation, the TA may assist the user in downloading certificates from the CA to a token.

A2.2.3. The other areas in which TAs have responsibility are loss recovery, unblocking one-time passwords, and revocation of certificates. In all three cases, the TA's role is minor but requires attention.

A2.2.4. When a user loses his/her private key, the TA requests the supporting LRA to replace the users lost certificate. The LRA will notify the RA to revoke the old certificate. The LRA will then send the new *DoD PKI Certificate Registration Instruction* to the TA.

A2.2.5. For unblocking the one-time access code (after the user was unsuccessful in their attempt to download a PKI certificate), the TA will contact the supporting LRA to reset the user's access code. The LRA or RA must check at the CA to ensure a certificate was not created. The LRA must first verify that the user certificate was not created, then the LRA will unlock the user account and notify the TA that the user may try to download their certificate again.

A2.2.6. For revocation of a user certificate (e.g., if the user leaves the DoD), the TA will send notice to the supporting LRA by E-mail or fax (digitally signed E-mail should be used when available). The LRA will forward the request for revocation to the Air Force RA at <mailto:afpki.ra@lackland.af.mil> (DSN 945-2562). End Users or TAs may directly forward revocation requests for their own certificates.

A2.2.7. For questions, contact the Air Force RA at Lackland AFB (see [Table A2.1.](#)).

**Table A2.1. Air Force Registration Authority Point of Contact.**

Function	Name	Phone Number	E-mail
Air Force PKI Help Desk	Help Desk	CONUS 1-800-897-2836 OCONUS DSN 553-2423	Web: <a href="https://afpki.lackland.af.mil/html/help_desk.html">https://afpki.lackland.af.mil/html/help_desk.html</a>
Air Force PKI SPO	Registration Authority	DSN 945-2562	<a href="mailto:afpki.ra@lackland.af.mil">mailto:afpki.ra@lackland.af.mil</a>