Headquarters
United States Army Europe
United States Army Installation Management Command
Europe Region

Army in Europe Regulation 25-1-5*

2 May 2013

Information Management

Public Key Infrastructure (PKI)

***This regulation supersedes AE Regulation 25-1-5, 30 March 2012.**

For the Commander:

JAMES C. BOOZER, SR.
Major General, GS
Chief of Staff

Official:

DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

Summary. This regulation prescribes policy on using public key infrastructure (PKI) to protect classified and unclassified official information in the European theater.

Summary of Change. This revision—

● Establishes AE Form 25-1-5A.

● Establishes the prohibition of using DOD-approved PKI tokens on computers that are accessible to the general public (for example, computers in Internet cafes, kiosks, and public libraries) (para 15a(5)).

● Prescribes requirements for inserting tokens and procedures to follow if tokens are inadvertently inserted into the wrong domains (SIPRNET token inserted into NIPRNET domain and vice versa) (para 15d).

● Establishes the authority for system administrators and data owners to require stronger credentials than the minimum required (para 15g).

● Prescribes the requirement for access authorization to be based on the user's need to know (para 15h).

● Incorporates a template for reporting lost or stolen SIPRNET tokens (app B).

● Incorporates a template for requesting exceptions to the mandatory user-based enforcement (app A).

● Makes administrative changes throughout.

Applicability. This regulation applies to DOD military, civilian, and contractor personnel (both U.S. and non-U.S. citizens) in the European theater who use U.S. Government computers and U.S. Government-issued mobile devices to process classified and unclassified official information over the NIPRNET and SIPRNET.

NOTE: This regulation does not apply to organizational messages sent through the Defense Message System.

Records Management. Records created as a result of processes prescribed by this regulation must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information Management System website at *https://www.arims.army.mil*.

Supplementation. Organizations will not supplement this regulation without the approval of the Information Assurance Program Management (IAPM) Division, Office of the Deputy Chief of Staff, G6, HQ USAREUR.

Forms. This regulation prescribes AE Form 25-1-5A. AE and higher level forms are available through the Army in Europe Library & Publishing System at *https://aepubs.army.mil/*.

Suggested Improvements. The proponent of this regulation is the IAPM Division, Office of the Deputy Chief of Staff, G6, HQ USAREUR (DSN 537-6213). Users may suggest improvements to this regulation by sending DA Form 2028 to the USAREUR G6 (AEIM-I), Unit 29351, APO AE 09014-9351, or by e-mail: usarmy.wiesbaden.usareur.list.dl-g6-iapm@mail.mil.

CONTENTS

Figures
A-1. Memorandum Format for Requesting Temporary Log-on Capability for Non-PKI-Compatible Software
B-1. Memorandum Format for Reporting Lost or Stolen SIPRNET Tokens

Glossary

---

1. PURPOSE

This regulation—

a. Establishes policy on properly using DOD public key infrastructure (PKI) in the European theater.

b. Requires organizations to—

(1) Ensure their personnel use DOD PKI to protect official Government information sent by e-mail over the NIPRNET and the SIPRNET.

(2) Use DOD PKI to protect infrastructure and information on the Army portion of the Global Information Grid.

2. REFERENCES

a. Publications.

(1) DOD Instruction 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling.

(2) AR 25-400-2, The Army Records Information Management System (ARIMS).

(3) USCYBERCOM Execute Order 2012-151, Implementation of SIPRNET Public Key Infrastructure (PKI) Token (*https://portal.eur.army.mil/sites/iassure/Identity%20Management/SIPRToken/Documents/US%20Army%20Cyber%20Command%20EXORD%202012-151%20SIPRNET%20PKI%20Token.pdf*).

(4) USCYBERCOM FRAGO 01 to OPORD 002, Gladiator Shield, Defending the NIPRNet, 2 February 2012, annex C, appendix 3, tab E.

(5) DISA Field Security Operations Multi-Function Device (MFD) and Printer Checklist for Sharing Peripherals Across the Network Security Technical Implementation Guide (*https://portal.eur.army.mil/sites/iassure/Identity%20Management/PKI%20Software/Documents/span_mfd_checklist_v1r1-3_04_15_2009.pdf*).

(6) National Security Systems Public Key Infrastructure Department of Defense Registration Practice Statement, Version 2 (*https://portal.eur.army.mil/sites/iassure/Identity%20Management/SIPRToken/User/Documents/NSS_RPS_V2_-_8SEP10.docx*).

(7) Situational Awareness Report (SAR) 2011-XXX Approval of User-Based Enforcement (UBE) Waiver Request from NETCOM/9th SC(A), 1 August 2011.

b. Forms.

(1) DA Form 2028, Recommended Changes to Publications and Blank Forms.

(2) AE Form 25-5-1A, Enhanced Trusted Agent (ETA) Replacement Token Request.

3. EXPLANATION OF ABBREVIATIONS

The glossary defines abbreviations.

4. GENERAL

DOD PKI provides data integrity, authentication, confidentiality, and nonrepudiation (digital signature) services to systems and applications on the DOD NIPRNET and SIPRNET. To benefit from these services, organizations in the European theater must do the following:

a. Take steps to protect Government information from unauthorized disclosure and modification using DOD PKI. This includes protecting information processed using automated messaging systems (for example, e-mail, two-way electronic devices, mobile devices) and posted on classified and unclassified organizational websites and portals.

b. Use DOD PKI to protect all official Government information by—

(1) Digitally signing e-mail messages.

(2) Encrypting information transmitted by e-mail when required (para 7).

(3) PKI-enabling websites, portals, enterprise tools, and web-enabled applications unless an appropriate waiver applies.

c. Implement the DOD PKI functionality through distributed public keys and secured private keys stored on hardware tokens such as common access cards (CACs), SIPRNET tokens, and alternate smart card logon (ASCL) tokens; and through role-based certificates where applicable.

NOTE: Users who are not authorized CACs may still be eligible to receive ASCL tokens for authentication purposes to use NIPRNET assets.

d. Acquire role-based certificates to allow PKI protection for organizational mailboxes. Organizations may request role-based certificates through their trusted agent (TA). TAs will request certificates from the Army PKI Registration Authority at the Army Chief Information Officer/G-6 Identity Management Office by e-mail (netcom-9sc.registration.authority@mail.mil). The Registration Authority will notify the requester when role-based certificates are created and ready for downloading.

5. RESPONSIBILITIES

Cybersecurity is everyone’s responsibility. Organizations and users must ensure the effective use of PKI services in the European theater. Leaders must ensure the following:

a. All NIPRNET users must possess and use a CAC before receiving a NIPRNET account. User accounts must be provisioned, user-based enforced, and require tokens with personal identification numbers (PINs) to log onto the NIPRNET.

b. Users must not write down their PINs for their CACs or their tokens. PINs must be memorized.

c. NIPRNET elevated-privilege users must have an ASCL token and an active PIN before the elevated-privilege account is created. Accounts will not be set to usernames and passwords. User-based enforcement (UBE) is mandatory. Any exceptions must be requested by memorandum, and the memorandum must be prepared as shown in appendix A.

d. All users must use PKI-enabled e-mail and enterprise websites when processing official Government information.

e. All users must use Government-owned computers equipped with CAC readers and PKI middleware when accessing networks.

f. All users must publish their PKI certificates to the global address list.

g. All organizations must purchase only CAC-enabled hardware.

h. Before any SIPRNET user account is created, the user must have a SIPRNET token and an associated PIN to log onto the SIPRNET. Each user account must be UBE to require the token for logging on.

i. PKI trusted agents (TAs) or enhanced trusted agents (ETAs) must control SIPRNET and ASCL tokens. SIPRNET token TAs must be Committee of National Security Systems-trained, qualified, and approved by a PKI local registration authority (LRA). When an individual receives SIPRNET token TA status, the individual also becomes an ASCL TA.

j. An ETA is a TA who is capable of requesting a replacement SIPRNET token within 24 hours to support mission requirements. When a SIPRNET token is urgently required, the ETA will use AE Form 25-1-5A at *https://aepubs.army.mil/* to request a replacement token. More information on replacing SIPRNET tokens is available at *https://portal.eur.army.mil/sites/iassure/Identity%20Management/SIPRToken/TA/*.

k. If an ETA is not available to replace a SIPRNET token, the user will contact the Enterprise Service Desk (ESD) at 119 to generate a service request for temporary access to network resources and enterprise e-mail using a username and password. If granted, this access will last no longer than 24 hours from the next workday, with a maximum of 96 hours if non-workdays are included. After that, immediate UBE will be reinstated. No extensions will be granted.

6. DIGITAL SIGNATURE AND ENCRYPTION

Information sent by e-mail is vulnerable to compromise. PKI helps protect that information through the use of digital signatures and encryption.

a. A digital signature on an e-mail message confirms that the—

(1) Message was sent by the individual identified as the sender (nonrepudiation).

(2) Contents of the message were not changed after the message was digitally signed (integrity).

(3) Sender’s certificate is valid.

b. Users must encrypt e-mail messages before sending sensitive information.

7. INFORMATION REQUIRING DIGITAL SIGNATURE AND ENCRYPTION

Depending on the sensitivity of the information being sent, e-mail messages must be digitally signed or encrypted. Users will—

a. Digitally sign e-mail messages generated in support of official Government business, including e-mail messages generated or received on mobile devices.

b. Encrypt e-mail messages when sending the following:

(1) Sensitive operational information. This includes but is not limited to unclassified tactical, administrative, and logistical information that supports Soldiers (for example, casualty reports, exercise deployment manning documents, information regarding installations and infrastructure, movement or transportation information, network data, unit status reports).

(2) For Official Use Only (FOUO) information.

(3) Information about medical care and personnel management.

(4) All personally identifiable information (for example, Social Security numbers associated with names).

(5) Messages with attachments that include any of the information in (1) through (4) above.

8. TWO-FACTOR AUTHENTICATION REQUIREMENTS FOR MULTIFUNCTIONAL DEVICES

Before connecting a PKI multifunctional device to a network, the system owner will—

a. Ensure that the device is accredited.

b. Disable all nonessential protocols and services on the device.

c. Attach an approved CAC reader to the device and configure the device for two-factor authentication.

d. Password-enable the device's remote-access (web-interface) function to prevent unauthorized access.

e. Disable telephone capabilities on the device (if applicable).

f. Ensure no universal serial bus (USB) drives or other removable storage devices are connected to or installed on the device.

9. MAINTAINING ENCRYPTED OFFICIAL E-MAIL MESSAGES

Users must maintain critical e-mail messages in accordance with AR 25-400-2. All users will—

a. Ensure their encrypted data is recoverable when their CACs are replaced, compromised, or become invalid.

b. Contact the ESD for assistance by submitting a ticket online at *http://119.eur.army.mil/* or calling DSN 119 to request help with PKI-related issues. More information on PKI is available at *https://portal.eur.army.mil/sites/iassure/Identity%20Management/CAC/*.

10. CERTIFICATES FOR NON-DOD ENTITIES, MILITARY RETIREES, AND FAMILY MEMBERS

DOD PKI certificates may be issued to military retirees and Family members for official communication purposes. To interact with the DOD PKI infrastructure, these users will acquire DOD PKI certificates from external certification authorities (ECAs). These certificates will enable secure e-mail exchange between DOD and non-DOD entities. More information on obtaining DOD ECA PKI certificates is available at *http://iase.disa.mil/pki/eca*.

11. ARMY IN EUROPE PKI MIDDLEWARE

All classified and unclassified Army in Europe systems must have appropriate PKI middleware installed as described below.

a. Tumbleweed Desktop Validator. This software maintains a copy of certificate revocation lists (CRLs) on the SIPRNET and NIPRNET. CRLs include information about revoked DOD certificates. Users are informed if any certificates are revoked.

NOTE: Users should be suspicious when receiving e-mail messages from senders with revoked certificates.

b. ActivClient. This middleware is installed on NIPRNET clients to retrieve certificates from CACs and ASCL tokens.

c. 90 Meter. This middleware is installed on SIPRNET clients to retrieve certificates from SIPRNET tokens.

12. CAC PIN RESET

The common access card personal identification number reset (CPR) capability allows specific trusted agent security managers (TASMs) to unlock and reset PINs on CACs.

a. The Information Assurance Program Manager (IAPM), Office of the Deputy Chief of Staff, G6, HQ USAREUR, will—

(1) Verify the identity of CPR TASMs supporting CPR in Europe.

(2) Validate CPR site identification registration requests.

(3) Validate applications for TASMs.

(4) Liaise between the DA Identity Management Office and Army in Europe TASMs.

b. Organizations requesting CPR will—

(1) Coordinate with the IAPM to validate the CPR requirement.

NOTE: Information about CPR requirements is available at *https://portal.eur.army.mil/sites/iassure/Identity%20Management/cpr/*.

(2) Assign two organizational CPR TASMs (a primary and an alternate).

(3) Send a digitally signed e-mail message to cpr.apoc@us.army.mil to validate their identity.

(4) Contact the Army CPR POC to register a CPR site or workstation.

(5) Acquire CPR equipment in accordance with the DA CPR Required Hardware List.

13. UPDATED ENCRYPTION ALGORITHMS

a. System owners—

(1) Will ensure current, new, and upgraded system components, software applications, products, and operating systems are compatible with secure hash algorithm (SHA) 256 and elliptic curve cryptography (ECC) for applications that use encryption, digital signature, and authentication. New certificates for these items are available from current DOD certificate authorities through nonentity (that is, equipment) PKI registration authorities (RAs) (for example, Army equipment RAs at Fort Huachuca, Arizona).

(2) Will ensure authentication with software certificates and ASCL tokens.

(3) With issues concerning technical software certificates associated with AKO will contact the AKO Products Directorate and Security System Office Team by e-mail at usarmy.belvoir.peo-eis.list.peoeis-ako-all@mail.mil or by commercial telephone at 703-704-0244.

b. Information assurance managers (IAMs) with users who have difficulty using software certificates to access DOD websites must contact the Army CIO/G6 Identity Management Office by e-mail at army.ra@us.army.mil or by commercial telephone at 703-545-1749.

c. System administrators must be designated as PKI-equipment authorized agents to obtain equipment or server certificates. Procedures, instructions, and further guidance can be found at *https://portal.eur.army.mil/sites/iassure/Identity%20Management/PKI/*.

14. SIPRNET TOKEN ACCOUNTABILITY WHEN USER RELOCATES

a. SIPRNET tokens have special restrictions when users relocate from a theater of operations, undergo a permanent change of station (PCS), retire, or change agencies.

(1) When undergoing a PCS, users may take their SIPRNET tokens to the new theater of operations, provided the assignment remains within the Army.

(2) Users who retire from the military or from U.S. Federal civilian service, leave a company as a contractor, change branches of military service, or change the agency to which they are assigned must give their SIPRNET tokens to their local PKI SIPRNET TA.

b. Any SIPRNET PKI TA or any PKI LRA may collect SIPRNET tokens from any user and submit the token for revocation.

c. Users who lose a SIPRNET token must notify a SIPRNET token TA and provide a signed memorandum to that TA using the template in appendix B. The TA will forward the memorandum with signatures from the user, the user's commander, and the user's IAM to the LRA to revoke the lost token and issue a new one.

15. CAC AND SIPRNET TOKEN PROHIBITED ACTIONS

a. Users will not—

(1) Insert NIPRNET CACs into SIPRNET token readers.

(2) Insert SIPRNET tokens into NIPRNET CAC readers.

(3) Leave CACs, ASCLs (NIPRNET tokens), or SIPRNET tokens unattended.

(4) Insert DOD-approved PKI tokens in systems that do not have up-to-date antivirus, spyware, and malware protection. Out-of-date antivirus, spyware, or malware protection must be reported to the system owner for remediation.

(5) Use DOD-approved PKI tokens on computers accessible to the general public (for example, in Internet cafes, kiosks, and public libraries).

b. Inserting a SIPRNET token into an unclassified workstation and entering the PIN (regardless of middleware) is a potential security violation. If a SIPRNET token is inserted into an unclassified system—

(1) The user will return the token to the TA and report the incident to the IAM.

(2) The TA will report the certificate for revocation to the LRA and notify the security manager of the incident.

(3) The security manager will investigate the incident.

c. Inserting a SIPRNET token into an unclassified workstation without entering the PIN does not create a security violation.

d. Properly configured middleware on SIPRNET computers will accept only SIPRNET tokens. Inserting a CAC or an ASCL (NIPRNET tokens) into the SIPRNET is not a security violation unless the NIPRNET token has become activated. Correctly configured, domain-aware middleware would detect the NIPRNET token as unauthorized and block the PIN from being entered; the middleware would also block any service applets that do not require a PIN. Violations must be reported to the IAM.

e. When using any system that requires PKI credentials to log on, users will remove any token inserted in the system before walking away from the computer to which they have logged on.

f. IAMs, system administrators (SAs), data owners, and users must be trained on identity authentication and data-access control measures.

g. The level of sensitivity of a given system is the basis for determining the system's minimum credential strength required for authentication. SAs and data owners are authorized to require stronger credentials for a system than the minimum required. In addition to the minimum credential strength, all information systems containing controlled unclassified information (CUI), including FOUO, must also accept authentication with approved PKI hardware tokens. Whenever logging onto a network, UBE with CACs and tokens remains in effect.

h. Authorization to log onto a system will be based on the user's need to know.

i. All SAs will keep a record of data owners and validate the list once a year.

j. Data owners will enforce an access-control system that provides a means of restricting access to users or groups based on need to know. For example, using role-based access control, an SA can limit access to CUI. The data owner will ensure that each SA adequately implements access-control mechanisms before placing CUI on systems with direct or indirect NIPRNET connectivity.

16. EXEMPTION FOR ELEVATED-PRIVILEGE, TWO-FACTOR AUTHENTICATION

Any user requesting to log on to a DOD-authorized ASCL-exempt application with a username and password must submit a memorandum to request that access (app A). Exemptions to ASCL two-factor authentication will apply only to the DOD-approved software applications listed on the iAssure website at *https://portal.eur.army.mil/sites/iassure/Identity%20Management/CAC/*.

17. EXCEPTIONS TO POLICY

Requests for exceptions to the policy in this regulation must be sent to the Information Assurance Program Management Division, Office of the Deputy Chief of Staff, G6, HQ USAREUR, Unit 29351, APO AE 09014-9351, or by e-mail: usarmy.wiesbaden.usareur.list.dl-g6-iapm@mail.mil.

APPENDIX A
REQUESTING TEMPORARY LOG-ON CAPABILITY FOR NON-PKI-COMPATIBLE SOFTWARE

Figure A-1 shows the memorandum format for requesting temporary log-on capability for software applications that the Army Chief Information Officer (CIO)/G-6 has approved as non-PKI-compatible applications. Users will send the completed memorandum as an attachment to an e-mail message addressed to usarmy.badenwur.usareur.mbx.usareur-registration-authority@mail.mil.

UNIT LETTERHEAD

Office Symbol Date

MEMORANDUM FOR PKI Governance Team, Office of the Deputy Chief of Staff, G6, HQ USAREUR

SUBJECT: Nomination for Temporary Log-on Capability (Username and Password) for PKI-Exempt Software Application [*Enter Name of Product*]

1. Request *Enter name of elevated system administrator (SA) account* be allowed temporary use of a username and password for *Enter name of software application* enterprise software acknowledged or approved by the Army CIO/G-6 as being non-PKI-compatible.

2. This elevated-privilege network account user requires this software application to perform assigned duties. The exempted application may require the SA to present a valid training certificate for that application, which must be uploaded in the Army Training and Tracking System. When an individual who is using a username and password departs the Army in Europe for any reason, the *enter the name of the user's organization* will notify the Information Assurance Program Manager, Office of the Deputy Chief of Staff, G6, HQ USAREUR, by sending an e-mail message to usarmy.badenwur.usareur.mbx.usareur-registration-authority@mail.mil.

3. All elevated-privilege network account users must have and use alternate smartcard logon (ASCL) tokens and personal identification numbers (PINs). Usernames and passwords are exclusively for software specified in paragraph 1. ASCL tokens with associated PINs are required for all other actions.

DISCLAIMER: If approved, this temporary exemption will remain in effect until the product becomes PKI-compatible, is discontinued, has its software or certificate-of-networthiness license expire, or whenever the user who was granted the exemption departs the Army in Europe.

4. SA account information for the user account subject to this exemption:

Name: *Enter the name of the nominated user exactly as the name appears on the user's ID card.*
Elevated Account Name for Exemption: *Enter the SA account name.*
Grade/Rank: *Enter the grade or rank of the nominated user.*
Organization/Office Name: *Enter the name of the organization or office to which the user is assigned.*
Class 3 PKI ID Certificate Serial Number: *Enter the serial number that appears on the user's ASCL/PIV card certificate.*
Scope of Authority: *Enter the organizational unit (OU) admin name where the account resides.*
E-mail: *Enter the nominated user's "mail.mil" e-mail address.*
Telephone: *Enter the nominated user's DSN and civilian telephone numbers.*

5. I understand this exemption must be rescinded when the exempt user is relieved of duties or departs the organization.

Figure A-1. Memorandum Format for Requesting Temporary Log-on Capability for Non-PKI-Compatible Software

6. The POC is *Enter name, position, e-mail address, and telephone number (DSN and civilian).*

_____
(Signature block of user's supervisor)

_____
(Commander or director (lieutenant colonel/GS-14 or higher) of the requesting organization)

_____
(date)

SA name:_____

I, *Enter SA name*, acknowledge my responsibilities as stated in this memorandum.

_____
(SA signature) *(date)*

NOTE: If the request for exemption is approved, the PKI Governance Office will generate the 119 ticket necessary to modify the user's elevated-privilege network account, including the associated exemption code.

Figure A-1. Memorandum Format for Requesting Temporary Log-on Capability for Non-PKI-Compatible Software—Continued

APPENDIX B
REPORTING LOST OR STOLEN SIPRNET TOKENS

Figure B-1 shows the memorandum format for reporting lost or stolen SIPRNET tokens.

UNIT LETTERHEAD

Office Symbol Date

MEMORANDUM FOR European Local Registration Authority

SUBJECT: Report of Lost or Stolen SIPRNET Token

1. I acknowledge and will report the loss or theft of my SIPRNET token. As a SIPRNET user, I understand that SIPRNET tokens—

a. Are expensive and replacing them results in a significant cost to the U.S. Government.

b. Must not be left unattended in the SIPRNET reader and must not be given to or taken by unauthorized users.

c. Compromise logical access security of Army classified networks if lost or stolen.

d. Must be immediately reported to the local registration authority (LRA), trusted agent, or the Army Registration Authority if lost or stolen to initiate revocation of the certificate and to issue a new token (para 3).

2. If I find any SIPRNET tokens, I will give them to a supervisor, LRA, or information assurance manager.

3. The following information relates to a lost or stolen SIPRNET token:

Date Lost or Stolen:
Location Where the Token is Believed to Have Been Lost or Stolen:

4. The undersigned requests replacement of a lost or stolen SIPRNET token.

I confirm that I have been counseled and advised of the information in paragraphs 1 and 2 of this memorandum.

_____	_____	_____
SIPRNET Token Holder	**(Signature)**	**(Date)**
_____	_____	_ _____
Commander (Lieutenant colonel/GS-14 or higher)	**(Signature)**	**(Date)**
_____	_____	_____
Information Assurance Manager	**(Signature)**	**(Date)**

Figure B-1. Memorandum Format for Reporting Lost or Stolen SIPRNET Tokens

GLOSSARY

AE	Army in Europe
AEPUBS	Army in Europe Library & Publishing System
ASCL	alternate smart card logon
CAC	common access card
CIO/G-6	Army Chief Information Officer/G-6
CPR	common access card personal identification number reset
CRL	certificate revocation list
CUI	controlled unclassified information
DA	Department of the Army
DISA	Defense Information Systems Agency
DOD	Department of Defense
DSN	Defense Switched Network
ECA	external certification authority
ESD	Enterprise Service Desk
ETA	enhanced trusted agent
FOUO	For Official Use Only
IAM	information assurance manager
IAPM	Information Assurance Program Manager
ID	identification
LRA	local registration authority
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
PIN	personal identification number
PIV	personal identity verification
PKI	public key infrastructure
POC	point of contact
SA	system administrator
SIPRNET	Secret Internet Protocol Router Network
TA	trusted agent
TASM	trusted agent security manager
USAREUR	United States Army Europe
UBE	user-based enforcement
USB	universal serial bus
USCYBERCOM	United States Army Cyber Command