Headquarters
Department of the Army
Washington, DC
27 April 2023

***Department of the Army Pamphlet 25–2–13**

Information Management : Army Cybersecurity

Army Identity, Credential, and Access Management and Public Key Infrastructure Implementing Instructions

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant to the Secretary of the Army

History. This publication is a major revision.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated.

Proponent and exception authority. The proponent of this pamphlet is the Deputy Chief of Staff, G–6. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific requirements.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) via email to usarmy.pentagon.hqda-cio-g-6.mbx.policy-inbox@mail.mil.

Distribution. This pamphlet is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

*This regulation supersedes DA Pam 25-2-13, dated 8 April 2019.

Contents (Listed by chapter and page number)

Figure List

Glossary of Terms

Summary of Change

Chapter 1
Introduction

1–1. Purpose
This pamphlet institutes identity, credential, and access management (ICAM) and public key infrastructure (PKI) standards and procedures for all information technology (IT) capabilities used in and by the Army. It supports AR 25–2 in implementing Public Law 104–106; Title 10, United States Code, Section 2223 (10 USC 2223); DoDI 8520.02; DODI 8520.03, and other guidance. These management processes involve strategic planning, routine operations, and IT performance measurements.

1–2. References, forms, and explanation of abbreviations
See appendix A. The abbreviations, brevity codes, and acronyms (ABCAs) used in this electronic publication are defined when you hover over them. All ABCAs are listed in the ABCA database located at https://armypubs.army.mil/abca/.

1–3. Associated publications
See AR 25-2.

1–4. Records management (recordkeeping) requirements
The records management requirement for all record numbers, associated forms, and reports required by this pamphlet are addressed in the Records Retention Schedule-Army (RRS–A). Detailed information for all related record numbers, forms, and reports are located in Army Records Information Management System (ARIMS)/RRS–A at https://www.arims.army.mil. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

1–5. Exclusions
a. This pamphlet does not address identification (ID) and authentication credentials issued on the common access card (CAC). CAC credentials and tokens are issued by the Defense Manpower Data Center (DMDC) through local Defense Enrollment Eligibility Reporting System (DEERS)/Real-time Automated Personnel Identification System (RAPIDS) facilities. CAC eligibility, issue procedures, and provisioning are outside of Army control and outside the scope of this pamphlet. CAC references in this pamphlet are provided for clarity and to present a complete picture of a given topic.

b. Eligibility criteria for Secure Internet Protocol Router Network (SIPRNet) and Nonclassified Internet Protocol Routing Network (NIPRNet) alternate smart card logon (ASCL) accounts are also outside the scope of this pamphlet. All references to the issuance of SIPRNet and NIPRNet ASCL credentials and tokens presuppose the recipient is eligible to receive them.

1–6. Overview
a. This pamphlet implements DoDI 8500.01 and DoDI 8510.01. Army ICAM programs must incorporate all Army, National Institute of Standards and Technology (NIST), Department of Defense (DoD), Joint, Committee on National Security Systems (CNSS), and Office of Management and Budget (OMB) policies and procedures addressing cybersecurity as directed by proper authority.

b. Army organizations must ensure individual accountability and responsibility for assigned personnel.

(1) Commanders, directors, information system (IS) owners, authorizing officials (AO), IS security managers, information system security officers (ISSOs), program managers (PMs), supervisors, individual users, and users filling positions with privileged access are responsible and accountable for the implementation of Army security requirements in accordance with AR 25–2, and as required by their job role and function.

(2) Military and civilian personnel are subject to administrative or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place at risk DoD/Army information by not ensuring correct implementation of Army security requirements in accordance with this pamphlet and other Army and DoD directives and DoDIs.

(3) Defense contractors are responsible for complying with contracted terms and applicable directives, laws, and regulations, and must ensure employee compliance. The contracting officer, or designee, is the

liaison with the defense contractor for directing or controlling contractor performance. Outside the assertion of criminal jurisdiction for misconduct, the contractor is responsible for disciplining contractor personnel. Only the Department of Justice may prosecute misconduct under applicable Federal laws, absent a formal declaration of war by Congress (which would subject civilians accompanying the force to Uniform Code of Military Justice jurisdiction). For additional information on contractor personnel authorized to accompany U.S. Armed Forces, see DoDI 3020.41.

Chapter 2
Background

2–1. Identity, credential, and access management background
ICAM is programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-person entities (NPEs), bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources. Identity authentication is the process of establishing confidence in a user, process, or device through an assertion or claim of an identity that is electronically presented to an IS. In addition, the IS or DoD network ensures that any credential used for identity authentication has been issued by an approved DoD identity credential provider or a DoD approved Federal or industry partner identity credential provider (see app B).

2–2. Public key infrastructure background
a. PKI is a specific set of identity and authentication services, implemented by a combination of technology, people, and processes (see app C).

b. Different source documents (policies and regulations) use different terms to refer to the same thing—

(1) The SIPRNet PKI is also called the National Security Systems (NSS) PKI.

(2) The NIPRNet PKI is also called the DoD PKI.

Chapter 3
Identity, Credential, and Access Management

3–1. Overview
a. This pamphlet provides guidance on electronic identity authentication (e-authentication). DoDI 8520.03 defines identity authentication as "the process of establishing confidence in an entity's (user, process, or device) assertion or claim of an identity that is electronically presented to an information system." The instruction further states, "…identity authentication refers to electronic authentication to information systems conducted by human users or by non-person entities such as information systems or devices."

b. Authentication focuses on confirming a person's identity based on the reliability of their credential. There are two types of individual authentication—

(1) Identity authentication—confirming a person's unique identity.

(2) Attribute authentication—confirming the person belongs to a particular group (such as military veterans or U.S. citizens).

c. Authorization focuses on identifying a properly authenticated person's user privileges. Authorization is the access privileges granted to a user, program, process, or the act of granting those privileges. The allocation of privileges to users is a system-level task. Authorization to any Army IT system will be implemented using the appropriate access control method that best supports their appropriate IT system. Additionally, Army IT will also employ the following principles when granting access to IT systems:

(1) *Least privilege.* An individual should only have the minimum set of privileges/permissions necessary to carry out their job function.

(2) *Separation of duties.* Sensitive operational functions should require the involvement of at least two people.

3–2. Person entity requirements for information technology systems

a. Army IT system owners (SOs) must use DoD persona-based identifiers for person entity (PE) authentication and authorization to Army resources. Specifically, all systems PE identifiers (user accounts) for all applications and services must map to one of the following persona-based identifiers:

(1) DoD ID number + persona type code.

(2) Federal agency smart credential number.

(3) Persona username.

b. The ID and authentication of person entities for access control must be persona-based as the PE and not as an attribute, such as a role.

3–3. Centralized master identity directory service

a. The Army will maintain a centralized master identity directory service that includes data for all users who require access to Army owned or sponsored IT systems and applications. The Army Master Identity Directory (AMID) service consolidates personnel identity data from multiple authoritative sources (for example, DMDC, Human Resources Command, Defense Civilian Personnel Data System, and so on) in order to provide a single Army identity record for all users. The AMID is the authoritative data source for all DoD CAC holders and Army non-CAC eligible mission partners.

b. Army IT systems, applications and cloud-based services that require identity information are only authorized to obtain that data from the AMID service or an authorized interface partner (for example, Enterprise Access Management Service–Army or Network Enterprise Technology Command (NETCOM) Managed Identify Service). Refer to the Army Identity Attribute Specification (see app A) for detailed information about the data available from the AMID. The Army ICAM Roadmap (see app A) provided the requirements to establish AMID as the source for Army authoritative identity data.

c. All enterprise systems, applications and cloud-based services that require multifactor authentication for disadvantaged users or non-CAC eligible mission partners must use EAMS–A.

d. All enterprise systems and applications, regardless of hosting location, must leverage direct PKI, or EAMS–A as the Army's enterprise identity provider/Identity Federation Service (IFS) for authentication.

3–4. Attribute Change Management Process

a. When a change to an identity attribute standard is required, the requesting party must submit a change request, using the Army Identity Attribute Standard Change Request Template (see app I), to the Army Chief Information Officer (CIO). A change request can be submitted in the event of—

(1) A change to Federal, DoD, or Army ICAM-related guidance that directly impacts an already documented standard.

(2) The inclusion of a new DoD enterprise and/or Army unique identity attribute used for logical access control.

b. The change request will be evaluated and voted on by the Army ICAM Integrated Process Team (IPT). If the proposed change is agreed upon by the IPT, the standard is adopted and documented in the Army Identity Attribute Specification.

c. Once the Army Identity Attribute Specification has been coordinated through the proper approval authorities and signed, the specification will be republished with the new changes.

d. If the standard is not approved, the requestor will be notified and allowed the opportunity to address the IPT in support of the requested change.

3–5. Identity, credential, and access management capability requirement process

a. When a new ICAM capability gap or use case is identified, the requesting party must submit written requirements to the Army ICAM IPT for review and approval.

b. The Army ICAM IPT is an advisory body that identifies capability gaps, revise policies, transform business processes and resolves conflicts related to enterprise ICAM capabilities.

c. Once ICAM requirements are received, the Army ICAM IPT will—

(1) Review and assess the requestor's ICAM requirement to determine feasibility, and the impact to policies, processes, and the technologies required to support the capability.

(2) The Army ICAM IPT will vote to approve/disapprove the capability based on its members assessment. An approved capability will be supported and incorporated into the larger ICAM enterprise.

d. AMID and EAMS–A are DoD-approved multi-factor authentication (MFA) and IFS capabilities. Requirements for new and existing IT systems must specify the use of AMID, EAMS–A, or direct PKI. IT

SOs that do not use AMID, EAMS–A, or direct PKI must submit a business case to the Army ICAM IPT for review and approval.

3–6. Artificial Intelligence, Machine Learning, and Robotic Process Automation Technology

a. Artificial Intelligence (AI) and Machine Learning (ML) technology refers to the ability of machines to perform tasks that normally require human intelligence (for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action) whether digitally or as the smart software behind autonomous physical systems. Robotic Process Automation (RPA) is a software technology that allows a person to deploy and manage software robots (bots) that emulate human actions within an overall business or IT process; however, unlike AI and ML technology, RPA perform highly logical tasks that don't require knowledge or human understanding.

b. AI, ML, and RPA technologies must be positively authenticated and authorized to access DoD and Army IT resources (for example, networks, applications, systems, and so forth) by using Army or DoD-approved credentials.

c. To mitigate the potential risks associated with these technologies, this pamphlet establishes guidance for verifying and issuing credentials to AI, ML, and RPA technologies operating on the Army Department of Defense Information Network (DoDIN).

d. Army organizations implementing AI, ML, and RPA technologies that need to authenticate to and access IT resources must—

(1) Use DoD or Army approved credentials in accordance with DoDI 8520.03, register with the Army Master Identity Directory (AMID) and be specifically identified as an NPE.

(2) AI, ML, and RPA technology credentials must have a specific expiration date not to exceed 3 years from the date of issue to align with current DoD policy.

(3) DoD or Army approved credentials must be associated with the name of the organization and a government civilian or military sponsor who is responsible for the operation of the AI, ML, and RPA technology. If/when the sponsor leaves the organization, sponsorship must be transferred to another government civilian or military sponsor within 30 days. If ownership is not transferred, the credentials will be disabled or revoked.

(4) Each AI, ML, and RPA technology must have a unique identifier within its operational domain (for example, Enterprise, Army, local) that is clearly associated with an approved NPE credential, in order to support the following system owner access requirements.

(a) System owners must be able to positively identify AI, ML, and RPA technologies that access their systems from the NPE credential/authenticator presented upon login.

(b) System owners must enforce the concepts of least privileges and separation of duties assigned to AI, ML, and RPA technologies which cannot exceed the entitlements authorized to the identified sponsor, or AI/ML/RPA operator.

(5) AI, ML, and RPA technologies authorized to have an email account or granted access to a group email account to perform its mission, must operate in compliance with the Army digital signature guidance within this pamphlet.

(6) AI, ML, and RPA technologies that access external systems must follow the system owner's account and access request procedures to ensure the external system owner enforces security policy in accordance with subparagraphs 3–6*d*(4)(a) and 3–6*d*(4)(b), above, for the AI, ML, and RPA being utilized for access.

e. All AI, ML, and RPA technologies that do not meet this criterion must submit a waiver for approval to the Army CIO.

f. Exceptions: CRN, standalone networks, and tactical systems.

Chapter 4
Public Key Infrastructure Credential Request and Issue

4–1. Selecting appropriate credentials

a. The SIPRNet certificate authority (CA) will issue any credential used to access or perform any function on the SIPRNet. The NIPRNet PKI (unclassified) CA issues credentials used on the NIPRNet.

(1) A subscriber is the entity whose name appears as the subject in a certificate.

(2) The PE who controls and uses the physical token is hereafter referred to as the user.

b. The SIPRNet and NIPRNet PKIs support issuing certificates to three types of subscribers: name, role, and system or device (also called a NPE). Privileged users are a special category of name subscriber. It is the user's responsibility to identify the appropriate credential for their needs. The selection is as follows for both SIPRNet and NIPRNet use:

(1) Name certificates (sometimes called PE certificates) for general users contain an individual name as the subject. These are tightly coupled with the individual named in the certificate, and are issued to and for Federal government employees, military, contractors, and affiliates (for example, foreign nationals). Name certificates for general users are provided on the CAC. The person responsible for a name certificate, the PKI sponsor, is the individual named in the certificate.

(2) Role certificates contain a role, group, or organization name as the subject; they do not contain the name of an individual. The PKI sponsor for a role certificate is the individual who is appointed in writing by the commander and is explicitly responsible for managing access to the private key associated with the certificate. In addition, the PKI sponsor is responsible for establishing technical or procedural controls and managing access to the private key associated with the certificate. Group credentials are a type of role credential associated with a group, such as a help desk, rather than a single individual. Code signing certificates are special role certificates that are used only to sign software/application code for use on computers.

(3) System or device certificates contain a system or device name as the subject. Systems and devices may be virtual or actual physical entities. Systems and devices, entities with a digital identity that act in cyberspace but are not human actors, are referred to as NPEs. Examples of systems or devices are workstations, cross-domain solutions (CDSs) (also called guards), firewalls, routers, web servers, applications, database servers, and other infrastructure components.

(a) The PKI sponsor for a system or device certificate is an individual who is to be explicitly responsible for managing access to the private key associated with the certificate. The owner of the system in question, or their designated representative, assigns this individual in writing.

(b) System or device certificates are issued in software form on an encrypted compact disc-read only memory (CD–ROM). The key/password to the file will be provided via different means.

(c) An individual may be the PKI sponsor for more than one system or device.

(4) Privileged user certificates are name certificates used by system administrators, domain administrators, auditors, and others who access ISs with more access or action privileges than general users. They require a separate set of credentials for this purpose to ensure separation of activities, and to facilitate activity logging for audit.

c. When requesting credentials, the PKI sponsor must specify the network on which it will be used (SIPRNet or NIPRNet) and the type of subscriber (name, role, NPE, or privileged).

d. Senior officials (general officer (GO) and senior executive service (SES)) may require a variant form of a name or role credential.

e. In rare cases, user or role credentials may be issued in software form. Such software certificates, also known as soft certs, require special justification for their unusual format and require additional security control protections.

4–2. Requesting credentials

a. Use DD Form 2842 (Department of Defense (DoD) Public Key Infrastructure (PKI) Subscriber Certificate of Acceptance and Acknowledgement of Responsibilities) to request individual user, privileged user, role, or group PKI credentials or DD Form 2841 (Department of Defense (DoD) Public Key Infrastructure (PKI) Registration Official Certificate of Acceptance and Acknowledgement of Responsibilities) for registration authorities (RAs), local registration authorities (LRAs), enhanced trusted agents (ETAs), and trusted agents (TAs). RAs and LRAs are staffed and approved through NETCOM to the Deputy Chief of Staff (DCS), G–6 for approval. Registration officers (TAs and ETAs) are staffed and approved by NETCOM. Guidelines are as follows:

(1) A separate DD Form 2842 or DD Form 2841 is required for each credential.

(2) Requests on old versions of DD Form 2842 or DD Form 2841 will not be processed. Be sure to use only the most recent version of DD Form 2842 and or DD Form 2841.

(3) Do not put a social security number on the form. Use the DoD ID number instead. (Electronic Data Interchange Personnel Identifier is the old term for the DoD ID number.)

(4) Do not sign the form until the credentials are received by the user.

b. Additional information (such as the type of credential or user/subscriber address) will be provided in memorandum form and signed by the individual making the request.

c. Name credentials for SIPRNet general users must be accompanied by a memorandum from the individual's commander (or designated representative) verifying that the PKI sponsor has a secret or higher clearance, a need to know, and a valid network logon account on the SIPRNet.

d. Requests for role (or group) credentials must include documentation describing—

(1) The role.

(2) The name of the person filling the role or the members of the group.

(3) The contact information of the single PKI sponsor for transfer of the token and activation data.

(4) The process (if a group credential) the PKI sponsor will use to control access and verify the group member's possession of a valid CAC or SIPRNet token.

(5) A copy of the commander's memo or order appointing the individual to the role.

e. For NPE credential requests, the PKI sponsor must provide—

(1) A copy of the commander's (or designated representative's) privileged user appointment memorandum assigning the PKI sponsor to the system or device.

(2) Documentation identifying or describing the system or device.

(3) Any attributes not part of the standard profile (for example, globally unique identifier in a domain controller certificate).

(4) The device-generated certificate request number to the supporting RA or LRA in a digitally signed email using the PKI sponsor's name signature certificate.

(5) The process the PKI sponsor will use to manage access to the private key associated with the certificate.

f. Privileged user credential requests require the same documentation as a regular name credential, but also require a copy of the commander's privileged user appointment memorandum.

4–3. Request routing

a. Route DD Form 2842 or DD Form 2841 requests through the requestor's supervisor to the PKI sponsor's supporting TA or ETA. If the request is completed electronically, it must be sent by digitally signed, encrypted email to the TA/ETA. If the request is done in hard copy, it must be delivered to the TA/ETA in person by the PKI sponsor.

b. The TA/ETA receiving a request must verify that additional documentation appropriate to the request type is provided. The TA/ETA will also confirm that the date on the DD Form 2842 or DD Form 2841 is within 30 days of the current date. Incomplete documentation or outdated signatures will cause the request to be returned to the requestor.

c. Upon verification that the request is complete and current, TA/ETA will forward the request to the supporting RA or LRA for further processing.

d. Requests that are rejected by a supporting RA or LRA will be returned to the requestor via the TA/ETA with an explanation.

e. DD Form 2841s receive additional processing and verification, contact NETCOM for assistance. See chapter 10 of this pamphlet for TA/ETA and chapter 11 of this pamphlet for RA and LRA for additional information.

4–4. Issuance

a. PKI credentials (other than CACs) will be issued in person by two TAs/ETAs. One will provide the token (or in the case of software certificates, a CD–ROM containing the encrypted credentials), the other will provide the initial token unlocking personal identification number (PIN) (or the password to decrypt the software certificates).

b. The TA/ETA will brief the user on appropriate certificate use, the need to protect the credentials, the prohibition against sharing the token or PIN, and instructions to contact a TA in the event of suspected or actual compromise *(*these TAs/ETAs are hereafter referred to as first and second to distinguish their actions).

c. The first TA/ETA will then perform the in-person verification of the user's identity. This requires the user to present acceptable identity documents to the TA/ETA.

(1) One document should be a Federal government official picture ID credential. A DoD ID card, the CAC, a DoD Civilian or military retiree ID card, a non-expired U.S. passport or a U.S. Government personal identity verification (PIV) card are acceptable.

(2) If the user does not have appropriate Federal ID, two nonfederal government issued official ID credentials must be presented, at least one of which must contain a picture (such as a driver's license).

(3) Per AR 600–8–14, Federal Information Processing Standards (FIPS) 201–2 list documents that are acceptable for identity proofing.

d. The first TA/ETA will examine the presented ID to ensure that they are authentic, original (copies are not acceptable), current (expired documents are not acceptable), and have no apparent signs of alteration or tampering.

e. Upon successful validation of the user's identity, the first TA/ETA will complete the DD Form 2842 and will provide the user with the token or the CD–ROM.

f. The second TA/ETA will receive and process the DD Form 2842 and will observe the user signing the document.

(1) For software certificates, the second TA/ETA will then provide the password to the user.

(2) For token credentials, the second TA/ETA will provide the initial token unlocking PIN; the user must immediately change the token unlocking PIN. The second TA/ETA will assist the user with changing the PIN but must not observe the new PIN being entered.

g. A graphic representation of distributed SIPRNet PKI token issuance that is illustrative of the process for all types of credentials is in appendix G.

4–5. Public Key Infrastructure network access tokens

a. The NIPRNet PKI is capable of issuing different types of certificates, including identity, authentication, signature, encryption, group/role, device, and code signing to satisfy DoD component requirements.

b. DoDM 1000.13, Volume 1, establishes the CAC as the DoD Federal PIV card. The CAC, as the DoD Federal PIV card, conforms to the NIST FIPS 201 PIV standard. FIPS 201 meets the Homeland Security Presidential Directory (HSPD)-12 policy for a government-wide standard for secure and reliable forms of ID for Federal employees and contractors requiring physical and logical access to Federally-controlled facilities and ISs. This makes the CAC the primary hardware token used to identify individuals for logical access to NIPRNet resources and physical access to DoD facilities.

c. Use of a NIPRNet ASCL token with NIPRNet PKI certificates is authorized for specific cases where certificates issued on the CAC cannot be used by various groups of network users.

d. Hardware tokens used for network logon to the SIPRNet will be issued by a credential service provider (CSP) that is either a member of the SIPRNet PKI, is cross-certified with the SIPRNet PKI, or has been specifically approved by the DoD CIO.

e. Other hardware tokens, as approved by the DoD CIO, may be authorized to facilitate DoD missions where accepting trust in the certificates on the token is consistent with DoD cybersecurity requirements. See paragraph 6–2 of this document for the list of approved DoD PKI.

f. The CAC and approved ASCL are the preferred methods of accessing the NIPRNet.

g. Username and password (UN/PW) are authorized when a CAC or alternate token is not authorized for specific user populations and when an approved MFA solution cannot be implemented. See paragraph 5–4 for UN/PW authorized use cases.

h. Privileged users must use a separate token (that is, not the individual user's CAC or SIPRNet token) to perform privileged user functions on the NIPRNet or SIPRNet. Privileged users must have two verified and issued NIPRNet/SIPRNet tokens, one issued for privileged use (for example, system administration) and one issued for nonprivileged use (for example, web applications or email). Tokens issued for privileged use must not be used for nonprivileged actions.

i. All privileged users must be identified and appointed in writing by commanders (or their designated representative) prior to being issued privileged access tokens for either network. An appointment letter and Privileged-level Access Agreement must be in the individual's Army Training and Certification Tracking System profile and validated quarterly.

j. Exceptions and exemptions to SIPRNet and/or NIPRNet access requirements must be sought through the exception process outlined in this publication (see chap 8 and app D).

4–6. Additional Public Key Infrastructure token couriers

a. Individuals who do not hold RA, LRA, TA, or ETA roles may act as couriers for transporting NIPRNet ASCL and SIPRNet PKI tokens on behalf of the RA, LRA, TA, or ETA.

b. Personnel who act as couriers must have a DoD secret clearance, possess a CAC, hold a valid DD Form 2501 (Courier Authorization) (available through normal supply channels), current courier orders that

authorize carrying of PKI tokens, and a general understanding of PKI tokens and token security requirements.

c. Couriers must maintain positive personal control over the PKI tokens in their possession at all times, ensuring that tokens are in the possession of the courier or secured in a safe, footlocker, or file cabinet at all times during transport.

d. Continuously accountable methods must be used by couriers to maintain a chain of accountability for possession of the tokens:

(1) Each person that takes possession of PKI tokens signs DA Form 3964 (Classified Document Accountability Record), which will provide a chain of accountability log and allow for continuous accountability.

(2) If using a package delivery service, ensure that the service is used in a manner that provides continuous accountability (for example, United States Postal Service Registered Mail with return receipt, and so on).

e. Upon receipt of a PKI token, the TA/ETA inspects the package and tokens for evidence of damage or tampering.

4–7. Safeguarding of Public Key Infrastructure tokens

a. The CNSS requires the following minimum security standards for the safeguarding and control of all SIPRNet PKI tokens:

(1) The SIPRNet token is considered a high-value unclassified item.

(a) The SIPRNet token is considered unclassified when removed from the card reader and not in use.

(b) The SIPRNet token PIN is classified secret when spoken or written. If written, the SIPRNet token PIN must be stored in a container or physical area authorized for secret storage. Store in a manner that provides evidence of unauthorized access.

(c) The SIPRNet token is classified secret when unlocked with the PIN and in use.

(2) Maintain the SIPRNet token under positive control of the assigned user, who is represented by the embedded certificates. To maintain positive control, the assigned user must—

(a) Maintain visual control of the token when in use.

(b) Keep the token on their person or lock the token in a container only intended to be unlocked by the assigned user, and which makes unauthorized access evident, when not in use.

(c) Never, under any circumstances, disclose the PIN associated with a SIPRNet token.

b. NIPRNet ASCL and CAC tokens and PINs are sensitive material and must be safeguarded. The assigned user must—

(1) Handle NIPRNet tokens and PINs as unclassified, for official use only (FOUO) at all times.

(2) Maintain visual control of the token when in use.

(3) Protect the token from theft or misplacement when not in use.

(4) Never disclose the PIN associated with a CAC or NIPRNet ASCL token.

c. Report any suspected loss of positive control or unauthorized use of either the SIPRNet or NIPRNet ASCL token immediately to the supporting RA by the most expeditious means available.

d. In the event a SIPRNet or NIPRNet token user, unit, or organization is determined to be missing, the token(s) must be suspended immediately. Report the situation and information regarding individual, unit, or organization affected immediately to the supporting RA by the most expeditious means available.

e. Submit a lost token report using the format provided at appendix F supporting TA or ETA as soon as possible.

4–8. Compromise of a Public Key Infrastructure token

a. If a SIPRNet token is inserted into a NIPRNet ASCL or CAC reader and the PIN is not entered—

(1) This is not a security incident and does not need to be reported to the local facility security officer (FSO).

(2) Remove the token immediately.

b. If a SIPRNet token is inserted into a NIPRNet ASCL or CAC reader and the PIN is entered:

(1) This is a security violation. The user must—

(a) Remove the token immediately.

(b) Report the incident to the supporting TA or ETA for evaluation.

(c) Return the token to the local supporting TA or ETA.

(d) Report the certificates for revocation.

(e) Report the incident to the local FSO.

(2) The appropriate security officer must investigate the incident.

c. If a token other than an NSS token (an unclassified token) is inserted into a token reader connected to a SIPRNet or other classified system (with or without PIN entry)—

(1) The user will remove the token immediately.

(2) The user will determine if the system uses properly configured domain aware middleware.

(a) If the system uses domain aware middleware that is properly configured, insertion of an unclassified token into the classified system is not a security violation unless it is apparent the unclassified token has become activated. (Correctly configured, domain aware middleware would detect the unclassified token as unauthorized and block PIN entry and block any service applets that do not require PIN entry.)

(b) If the system does not use domain aware middleware or it is not properly configured, any introduction of an unclassified token on a classified system is a potential security violation, regardless of whether the PIN is entered. Report such instances to the local information security officer. The incident must be investigated to determine if classified data were written to the token, or if malicious code was introduced into the network. (Non-domain aware middleware is incapable of blocking token activation.)

d. If a user knows or suspects that their PIN has been compromised (become known by anyone else)—

(1) The user must report the event to their TA/ETA.

(2) The TA/ETA must report the loss to the ISSO and RA/LRA and the security violation to the local FSO.

(3) The TA/ETA must report the security violation to the local security officer.

(4) The local security officer and/or ISSO may direct additional actions or require an investigation into the violation.

(5) The user must change the PIN as soon as possible.

(6) The user must comply with any instructions from the RA/LRA, security officer, or ISSO regarding the incident or the token involved.

(7) The RA will revoke the credentials associated with the token as soon as possible.

e. Report any suspected unauthorized use of any PKI token to a supporting TA or ETA and to the local security officer and/or ISSO.

f. If there is evidence of tampering, a SIPRNet token must be returned to the National Security Agency (NSA) for investigation and/or destruction.

4–9. Credential revocation and suspension

a. Revocation of credentials permanently renders the private keys useless for further transactions.

(1) They cannot be used for identity validation, encryption, or digital signature.

(2) They can be used to decrypt files or documents encrypted with the private keys prior to revocation.

(3) They can be used to validate digital signatures made prior to revocation.

b. Revocation is permanent and cannot be reversed. Revoked credentials must be replaced with a new set of credentials.

c. Suspension, like revocation, renders credentials useless but suspension can be reversed (vacated).

(1) Suspension is used when—

(a) An investigation is needed to confirm loss or compromise.

(b) Contact is lost with a user, unit, or organization but token compromise is not suspected.

(c) Technical issues prevent access to a token (no suspicion of compromise).

(2) Suspension is limited to no more than 30 days.

(3) If not vacated before the end of the suspension period, suspension automatically becomes revocation.

d. Credentials suspected of compromise may be used to request revocation/suspension.

e. Suspension vacation may only be requested using valid (unsuspended) credentials.

f. Revocation and suspension requests must—

(1) Include the full name and/or DoD ID number of the subscriber whose credentials are to be revoked/suspended.

(2) Cite the reason for revocation/suspension.

(3) For suspension, give either an ending date or period (30 days or less).

(4) Be signed by one of the following:

(a) The subscriber (compromised or suspect credentials may be used for this purpose only).

(b) The PKI sponsor of an NPE or role/group credentials.

(c) The commander or supervisor of the user (the command/supervisory relationship must be cited).

(d) A TA, ETA, LRA, or RA with knowledge of the circumstances warranting revocation or suspension.

(5) Be submitted to an RA by the most expeditious means (need not be routed through a supporting TA/ETA/LRA).

4–10. Credential renewal, rekey, or replacement

a. Renewal, rekey, or replacement of CACs is done through the DEERS/RAPIDS system.

b. Credential renewal (extending the life of existing keys) for SIPRNet or NIPRNet ASCL credentials is permitted in cases where thick-client systems have installed and configured 90Meter SCM + software. Use of 90Meter SCM + software for token rekey is not permitted on virtual desktop systems. In the event that rekey fails, the token holder must request replacement from the user's supporting ETA/LRA/RA.

c. SIPRNet and NIPRNet ASCL credential rekey is performed in the same manner as initial key issue. Where technically possible, tokens may be reused at the discretion of the supporting RA/LRA.

d. Lost or stolen tokens will be replaced.

(1) The user must report the loss/theft/malfunction to the nearest supporting ETA or LRA.

(2) The user must provide a DD Form 2842 and copies of any additional supporting documentation.

(3) Documentation outlining the requirement to replace the token must be generated by the local TA/ETA; additional documentation may be needed if the initial loss/theft/malfunction was a result of user actions.

(4) The TA/ETA or LRA will coordinate with an RA to revoke the credentials involved and issue new ones. Replacement for damaged or failed tokens will be done within 24 hours.

e. Malfunctioning/failed tokens must be handled and turned in as described in paragraph 9–3.

4–11. Token unlock and personal identification number reset

a. If the user enters their PIN incorrectly (three failed PIN attempts on NIPRNet ASCL token, five failed PIN attempts on SIPRNet token) resulting in a locked token, assistance will be required from a TA or ETA.

b. The user will notify the supporting TA/ETA of the situation and request assistance.

c. Token unlock or PIN reset must be done by the user at the location of the TA/ETA.

(1) A NIPRNet ASCL token requires an "unlock code" that will not be given to a user.

(2) A SIPRNet token PIN reset must be done by the TA/ETA and the new PIN immediately changed.

d. CAC PIN reset is performed by a CAC PIN reset trusted agent (CTA). Location of and access to CTAs is controlled by local policy.

4–12. Turn in and recovery of tokens

a. NIPRNet ASCL/SIPRNet tokens that are excess, unneeded, unserviceable, or suspected of being compromised must be recovered and returned through the supporting TA/ETA to the Army RA/LRA.

b. SIPRNet and NIPRNet ASCL token recovery must be included on organization/installation out-processing checklists. However, whether or not an individual retains their SIPRNet token is outlined in paragraph 4–14. NIPRNet ASCL tokens must be turned in upon permanent change of station (PCS).

c. If the situation warrants, commanders, supervisors, or managers may recover tokens for later transfer to a TA, provided the PIN that grants access to the token is not also obtained.

d. Malfunctioning/failed tokens must be handled and turned in as described in paragraph 9–3.

e. CACs must be recovered/turned in as described in AR 600–8–14.

4–13. Nonclassified Internet Protocol Router Network token retention during duty assignment changes

a. The Army CIO authorizes eligible military and Department of the Army (DA) Civilian personnel to retain NIPRNet tokens during PCS and training, to improve mission readiness, lower sustainment costs, and reduce user downtime.

b. The legacy alternate logon token (ALT) and the NIPRNet Enterprise Alternate Token System (NEATS) token are the "NIPRNet tokens" referred to in this section.

c. Retention of NIPRNet tokens is approved during the following duty assignments:

(1) Eligible personnel may retain a NIPRNet token during deployment and redeployment. Personnel that are changing duty assignments (that is, to PCS or to attend school or training) must turn in their token prior to departure.

(2) To be eligible to retain a PKI token, the cardholder must be a member of the United States Armed Forces or a DoD Civilian employee who has verified access requirements at the gaining organization, as confirmed by the personnel office at the losing organization, and who requires access for training purposes and/or requires NIPRNet access for deployment and redeployment.

d. To be eligible to retain a PKI token, the cardholder must be a member of the United States Armed Forces or a DoD Civilian employee who has verified access requirements at the gaining organization, as confirmed by the personnel office at the losing organization, and who requires access for training purposes and/or requires NIPRNet access for deployment and redeployment.

e. Contractors must turn in a NIPRNet token whenever they no longer require access, their contract ends, or their employment terminates.

4–14. Secure Internet Protocol Router Network token retention during duty assignment changes

a. The DCS, G–6 authorizes eligible DA Civilian and military to retain non-privileged SIPRNet tokens during PCS, duty assignment changes and during training. DA Civilians and military who retain their tokens are responsible for maintaining physical control of their tokens during movement. These personnel are not authorized to obtain a new token at gaining organization without reporting the token as lost, stolen, or failed.

b. Systems and network administrators are not permitted to keep or retain their privileged user tokens when changing duties; transitioning to a new post, camp, or station; or separating from service. Eligible personnel may retain a SIPRNet PKI token used for privileged access during deployment and redeployment only.

c. The holder who is permitted to retain a SIPRNet token must—

(1) Have verified access requirements for SIPRNet at the gaining organization as confirmed by the personnel office at the losing organization.

(2) Require SIPRNet access for training purposes or require SIPRNet access for deployment and redeployment.

d. System and network administrators who are authorized SIPRNet tokens and who will be out-processing due to a PCS must turn in these tokens to the organization's supporting TA/ETA.

e. Second SIPRNet token holders (O–9, O–10, and SES-equivalents) must turn in their second tokens if they will not be required at their new duty station or if they are separating from service.

f. Contractors are not permitted to retain SIPRNet tokens (individual user or privileged user tokens) and must turn them in to their local TA/ETA at termination of employment, end of contract, or whenever they no longer require access.

4–15. Public Key Infrastructure token retention guidance

a. When personnel are leaving an organization, the organization's TAs or ETAs are notified of departing personnel and whether each individual will retain their PKI token or is required to turn it in before departure. If the individual is retaining the token, the TA or ETA records which of these conditions permitting retention apply—

(1) Out-processing due to a PCS.

(2) Scheduled to attend training that requires nonprivileged access to SIPRNet and will return to duty station.

(3) Preparing to deploy or redeploy.

b. Military and DoD Civilian personnel ensure that the gaining organization's supporting information management officer and system administrator are notified during in-processing that they transitioned with their PKI token.

c. Under no circumstances will a Contractor retain a NIPRNet token.

4–16. Instructions for Public Key Infrastructure token turn in

a. NIPRNet ASCL and/or SIPRNet PKI tokens are to be retrieved and recorded in an organization's out-processing procedures to ensure that these tokens are collected from all transitioning personnel who no longer require network access. The procedures include DoD Civilians, military, and contractor personnel.

b. Users will turn in their PKI token to their organization's supporting TA or ETA when access is no longer required.

c. Personnel who no longer require access but for whatever reason failed to turn in their PKI token at the losing organization are required to immediately turn in the token to the local TA or ETA at the gaining organization upon arrival at the new duty station.

d. All contractor personnel will turn in their PKI token to their organization's supporting TA or ETA at contract completion, and/or when they no longer require access (this includes employment termination).

e. Under no circumstances will a contractor retain a NIPRNet token.

f. TAs, ETAs, or the LRA will notify the Army RA when a cardholder's status changes to ensure that SIPRNet and NIPRNet ASCL tokens are revoked.

4–17. U.S. Army Cyber Command Secure Internet Protocol Router Network token use exceptions

a. U.S. Army Cyber Command defines seven categories of temporary exception (also known as a waiver) to the requirement that all SIPRNet users use PKI tokens for SIPRNet access—

(1) *Non-embedded Department of Defense mission partner.* That is, non-DoD personnel who are DoD-cleared contractors; Federal departments/agencies and their cleared contractors; or state, local, tribal entities, and their cleared contractors who are not located in DoD facilities and access the SIPRNet through DoD-sponsored SIPRNet connections or DoD gateways such as the SIPRNet Federal demilitarized zone (FED DMZ).

(2) *Non-embedded foreign users.* Foreign nationals who are not located in DoD facilities and access the SIPRNet through DoD-sponsored SIPRNet connections or DoD gateways such as the Secure Internet Protocol Router (SIPR) releasable demilitarized zone (REL DMZ).

(3) *Department of Defense non-Defense Enrollment Eligibility Reporting System users.* Agency employees, contractor support at contractor sites, interns, or other user types who do not have an active record with an associated DoD ID number in the DEERS.

(4) *Department of Defense deployed users.* Users who are in a deployed environment or situations, either ashore or afloat, that prevent or inhibit the use of a PKI hardware token for operational mission reasons are not required to use PKI or two-factor authentication (2FA)/MFA. In lieu of PKI or 2FA/MFA authentication, maximized use of user ID and password meeting current guidelines must be in place and used. At the point where the environmental challenge is no longer an issue, individual user and privileged users must use PKI or approved 2FA/MFA. These situations may include personnel conducting wartime and/or military operations, personnel requiring access to systems from low-bandwidth or disconnected environments, and personnel assigned to an embassy or coalition partner location that does not have a SIPRNet token issuance capability on the same base, post, camp, station, vessel, and so on.

(5) *Cross-domain users.* Users who access the SIPRNet through a high assurance CDS (also called a guard) from a higher classification network.

(6) *Temporary loss users.* Users who experience a loss or failure of a PKI hardware token in an operational environment, which will create a stop work situation.

(7) *Technical limitation users.* Users experiencing situations with equipment, software, or system configuration which prevents the use of a PKI hardware token.

b. Use of one of these temporary exceptions must be documented in a memorandum that—

(1) States the specific exception cited.

(2) Includes a realistic expiration date for the exception.

(3) Is signed by the system ISSO or other security authority.

(4) Is retained to support Risk Management Framework (RMF) control assessments and security status reporting.

c. Alternate authentication methods must be implemented to comply with RMF security control requirements.

4–18. Nonclassified Internet Protocol Router Network Enterprise Alternate Token System

a. The Nonclassified Internet Protocol Router Network (NIPRNet) NEATS is a DoD managed enterprise system for issuing and managing NIPRNet ASCL tokens. NEATS and the legacy NIPRNet ASCL token system used by the Army and other DoD Components are both approved for use until NEATS fully replaces the legacy NIPRNet ASCL token system.

b. ASCL and NEATS tokens that are issued to the staff of a GO/SES can contain all the certificates of the GO/SES's CAC except for the signature certificate. The signature certificate can only be used by the

original CAC holder, it cannot be used by any individual (for example, senior leader staff) to sign on behalf of another person (for example, GO/SES).

c. The CAC is the primary hardware token for NIPRNet logon by eligible DoD and Army military, civilian and contractor personnel, and properly vetted foreign officials and foreign nationals. However, network users who are otherwise eligible to receive a CAC but are prohibited due to technical network constraints or host-nation agreements, are eligible to receive a NEATS or legacy NIPRNet ASCL token.

d. NEATS tokens will be the primary ASCL token issued unless the legacy NIPRNet ASCL tokens are required for mission.

*e. S*pecific user groups are authorized to receive NEATS and legacy NIPRNet ASCL Token to access DoD and Army network resources. User groups outside those listed in this pamphlet are not authorized to receive ASCL tokens; organizations must submit a request to the DCS, G–6 to add a specific user group or to request consideration to perform an action not aligned with the instructions within this pamphlet.

f. The following user groups are eligible to receive NEATS or legacy NIPRNet ASCL tokens:

(1) System or network administrators and other users who have responsibilities that require elevated privileges.

(2) GO or civilian equivalent, and staff aides.

(3) Paid American Red Cross employees supporting U.S. military installations in the continental United States.

(4) Army Junior Reserve Officer Training Corps instructors.

(5) Vetted and approved foreign nationals, foreign exchange personnel, foreign officers or foreign liaison officers eligible to receive a CAC whose host-nation agreements prohibit their use or possession of a CAC.

(6) Retired physicians or medical staff who require access to the Medical Protection System application.

(7) Army Emergency Relief personnel requiring logical access to Army networks and websites.

(8) Operators required to monitor multiple systems simultaneously and continuously.

(9) International Military Students while attending training at Army or DoD locations.

g. NIPRNet ASCL tokens issued to GO or SES staff for the purpose of authentication to the network and reading encrypted email on behalf of the GO/SES will contain a DoD PKI identity certificate linked to the GO/SES DoD ID number (formerly known as Electronic Data Interface Personal Identifier) and a copy of the GO/SES recovered encryption key.

h. NIPRNet ASCL tokens issued to GO/SES staff will not contain a DoD Email Signature certificate, and staff will not have the capability to sign emails or sign forms as or on behalf of the GO/SES.

i. Exceptions to the NIPRNet ASCL and NEATS certificate requirements must be sought through the exception process outlined in this publication (see chap 8 and app D).

4–19. Senior official second tokens (Secure Internet Protocol Router Network only)

a. The Army CIO authorizes the issuance of a second SIPRNet PKI token for primary token owners in the GO rank of O–9/lieutenant general and O–10/general, and SES three- and four-star equivalents.

b. Request second tokens for senior officials using DD Form 2842 through the PKI sponsor's local TA or ETA to the Army RAs, to the Army CIO for approval.

(1) The GO or civilian equivalent must sign the DD Form 2842.

(2) Provide a memorandum stating the requirement for, and expected duration of, the second token issue. This must be signed by the GO or civilian equivalent.

(3) The staff aides or administrative assistants to GOs or civilian-equivalents processing the request through the local TA/ETA must provide copies of the documents appointing them to their positions in order to process the requests.

c. Second tokens must be turned in upon departure of the senior official from the organization or if the requirement for the second token ends.

(1) The second token will be turned in to the local TA or ETA within 24 hours of a change in requirements to hold a second token.

(2) The TA/ETA will notify the RA to revoke the credentials associated with the token.

d. In situations when the intent of the second token is for the senior official to receive direct support staff (in other words, aides de camp, executive officers, communication officers, and so on) to log on in order to bring up the very important person's (VIP) computer in order to download or read emails, it is not recommended to request a second SIPRNet token. The VIP should request, through the TA/ETA, that a

VIP group be established; identify who should be assigned to the group, and specify what credentials are required for each member of the group. To logon and read unencrypted emails, only the ID certificate is required. To logon and read all emails (encrypted and unencrypted emails) the ID and encryption certificates are required. Only the VIP is authorized to receive the VIP's signing certificate. There is no limit to the number of individuals to receive a token; however, the VIP is encouraged to limit access to only those with a need to know. The VIP is required to notify the local TA/ETA when an individual with VIP group access departs the organization so their access can be removed. Users are not allowed to share their individual user NIPRNet ASCL or SIPRNet tokens.

4–20. Public Key Infrastructure code signing certificates

a. The potential adverse impact of the improper use of code signing certificates requires their issue to be tightly controlled. Controls include—

(1) No more than two sets are issued to a given organization.

(2) Their use is restricted to the specific code signing task.

(3) Their usage period is limited to 13 months (NIPRNet) or 36 months (SIPRNet).

b. NETCOM serves as the code signing attribute authority (CSAA) for the Army.

c. Organizations requiring code signing certificates must first obtain a code signing identifier (CSID) from the Army CSAA. Requests will—

(1) Be submitted on organizational letterhead.

(2) Describe the mission or activity that requires development and distribution of signed software or applications.

(3) Describe the organizational controls implemented to ensure that—

(a) Code signing certificates are used only by authorized persons.

(b) Code signing certificates are only used to sign software code for government use.

(c) Credential use is limited to 13 months (NIPRNet) or 36 months (SIPRNet).

(d) Credential validity is limited to 6 years (NIPRNet) or 8 years (SIPRNet).

(4) Be signed by the organization's commander.

(5) Be routed through the chain of command to the Army CIO for review, approval, and assignment of a CSID.

d. Once an organization has been assigned a CSID, it must submit a request for code signing certificates using DD Form 2842 through a TA or ETA to the supporting RA. The request must include—

(1) The CSID assigned to the organization.

(2) A memorandum approving the individual to receive code signing certificates on behalf of the organization, signed by the organization commander or designated representative.

(3) Verification of the individual security clearance that is to receive the code signing certificates.

e. The RA will issue the credentials to the individual through the supporting TA/ETA.

f. Code signing certificates are subject to the same revocation, suspension, and other processes as all other PKI credentials.

4–21. Public Key Infrastructure digital signature requirements

a. Digital signatures derived from the PKI email signing certificate on the CAC provides the receiver of an electronic email a high level of confidence that the sender is who he or she claims to be. Digitally signing email using the CAC also provides nonrepudiation, which provides a high level of assurance that the data is authentic (data integrity), and the sender cannot be disputed. PKI creates a web of trust between the receiver and sender of electronic email, which enhances Army's cybersecurity.

b. All emails sent from an Army owned, operated, controlled system or account to be digitally signed with a DoD PKI certificate from a CAC or approved DoD PKI hardware token (for example, NIPRNet/SIPRNet ASCL token). These requirements extend to digital machines (for example, faxes, copiers, scanners, and so on). Machines connected to the Army network that are capable of sending email are required to use digital signatures.

c. Exceptions include—

(1) Email sent to addresses other than .mil do not require a digital signature except when email contains sensitive data that requires encryption.

(a) Encrypted emails are required to be digitally signed. While encryption ensures the confidentiality of data, it does not provide data integrity or nonrepudiation of the email.

(b) Senders should only send digitally signed/encrypted emails to addresses other than .mil when a trust relationship has been established through a DoD approved method.

(2) Pure text references to uniform resource locator (URL) web addresses or email addresses do not require digital signature; only emails with an active hyperlink (URL web address or email address) that has clickable content must be digitally signed.

(a) Senders with an automatically appended email signature block should remove all active hyperlinks from the signature to prevent having to sign the email solely because of a hyperlink in the email signature.

(b) If the sender has a v-card (an attachment containing the sender's contact information) selected by default, they must either delete the v-card before sending the message or must sign the message.

(3) Digital signature is not required for automated email notifications such as a helpdesk mailbox that sends standard responses to user inquiries.

d. Email recipients should assess a digital signature's level of assurance.

(1) Emails signed using revoked certificates should be treated as not having originated from the indicated sender except when opening an archived email that was previously opened and its signature validated at the time of receipt but now gets a "revoked certificates" warning. This indicates the sender's signing certificate expired after the message was received, but the signature was valid at the time the email was sent.

(2) Valid PKI digital signatures originating outside DoD PKI domains and generated by a DoD approved PKI certificate source (for example, Federal Bridge Certification Authority (FBCA), External Certificate Authority (ECA)) should be trusted. Emails that are digitally signed by unapproved sources or with revoked certificates may be opened and read but should be acted upon with caution. Entities that are cross-certified with the FBCA are listed at https://playbooks.idmanagement.gov/fpki/tools/fpkigraph/. Information on the ECA program is available at https://cyber.mil/eca/.

(3) Recipients should validate the contents of unexpected and unsigned emails. Do not click on active links (URLs or email addresses) in unsigned emails. Instead, contact the sender and verify the link using Army best practices. All attachments should be scanned for malware and viruses prior to being opened.

4–22. Derived credentials

a. Derived credentials leverage the initial identity proofing process used during PKI credential issue to reduce the in-person proofing burden. A derived credential is issued based on proof of possession and control of a token associated with a previously issued credential. This avoids duplication of the identity proofing process while facilitating more flexible issuance procedures. For example, a derived credential request may be signed (validated) and encrypted (protected) using a CAC or SIPRNet token. Alternate MFA solutions may use credentials derived from CACs, NIPRNet ASCL tokens, or SIPRNet tokens. NIST SP 800–157 contains additional information and guidance.

b. Derived credentials are an emerging technology within DoD and are strongly tied to mobility efforts. Policy and procedures will be developed and provided as the authorization and use of these credentials evolve.

Chapter 5
Public Key Enabling

5–1. Overview

a. DoD policy and DoD CIO instruction require that MFA be employed for all IS access. This applies to individual user and privileged user accounts. DoD policy further establishes that the SIPRNet or NIPRNet PKIs established for DoD use are the standard MFA technologies to be used. The Service proponents are responsible for ensuring compliance (For the Army, this is the CIO).

b. SOs are responsible for ensuring their systems implement PKI or some other Service-approved MFA solution. If this is not possible, they are responsible for seeking an exception to DoD policy prior to system deployment or use.

c. Public Key Enabling (PKE) refers to those capabilities and system components necessary to allow systems, applications, and services to effectively use PKI certificates and credentials. This includes hardware and software components such as cryptographic libraries, card readers, device drivers, and certificate validation software. A system, device, application, or service often has multiple different parts that can or must be public key (PK) enabled. As such, it is important to indicate what part of the system is PK enabled.

d. Standards and specifications may be found at the Defense of Defense CYBER EXCHANGE PKI–PKE webpage https://cyber.mil/pki-pke/.

5–2. Credential validation

a. Each and every time a PKI certificate is used, it is up to the relying party (RP) (that is, the person or NPE using the certificate) to determine if the certificate is actually valid before proceeding with the operation. This validation check is the basis for the decision on whether to trust the certificate before it is used.

b. Validating a certificate includes five separate checks—

(1) Building a path.

(2) Checking the validity period.

(3) Verifying the signatures.

(4) Verifying the extensions.

(5) Checking the revocation status of the certificate.

c. If any one of these five checks do not pass, the certificate should not be trusted. Steps one through four are performed locally on the system. Step five (revocation status check) requires that a current status be obtained for the certificate; this status can be provided via a certificate revocation list (CRL) or via the Online Certificate Status Protocol (OCSP). CRLs are published by the CAs that issue the certificates and OCSP requires connection to a server that provides OCSP responses in accordance with IETF RFC 6960.

d. Credential validation requires access to an authoritative CRL or OCSP response.

e. The Secure Administration Authentication Gateway (SAAG) is the Army gateway solution that provides MFA capability for systems, devices, and applications that do not natively support MFA. It enables multi-factor system administrator and privileged user authentication, not general user MFA. System administrators and privileged users connect to their devices by authenticating to the SAAG portal via DoD CAC/PKI. This solution is being deployed within the Army. Further guidance and instructions will be forthcoming and will be incorporated into future editions of this pamphlet.

5–3. Off-line operation

a. All systems using PKI certificates must check the status of the certificate to determine if it can be trusted. It is required that systems validating certificates locally cache OCSP and CRL information to speed up operations, reduce the load on the network, and to ensure status availability when the system is unable to reach an authoritative source of CRLs or OCSP.

b. To ensure an optimal certificate validation, check the status in the following order:

(1) Locally cached status information—

(a) Locally cached OCSP response.

(b) Locally cached CRL.

(2) OCSP to primary OCSP responder (primary responder should be a locally available asset).

(3) OCSP to secondary OCSP responder (secondary should be an alternate local asset or it can be a globally load balanced asset provided by Defense Information Systems Agency (DISA) at ocsp.disa.mil).

(4) If all other checks pass but updated certificate revocation status cannot be obtained, the system may elect to trust the certificate without said status (that is, “fail open”). This is important for mission critical operations in disconnected, interrupted, and low-bandwidth environments where connectivity for updated status may not be available.

c. If network connectivity is not available by architecture/design, the system cannot be considered PKE.

d. The RP (entity using a PKI credential to identify or authenticate a user) may make a risk-based decision to accept an invalidated credential or one that has only been checked against a cached CRL that may be outdated. CRL issuance frequency is specified in the NSS and DoD certificate policies and varies depending on circumstance (the most common frequency is daily).

5–4. Public key infrastructure for non-person entities

a. Army components are authorized to issue Only Locally Trusted (OLT) NPE Public Key Infrastructure (PKI) certificates on NIPRNet and SIPRNet NPE devices. These OLT NPEs must be subordinate to those operated by the NETCOM, the Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance Center (C5ISR), Program Executive Office Command, Control and Communications-Tactical (PEO C3T) or Program Executive Office Soldier (PEO Soldier).

b. This guidance does not affect Army use of Medium Assurance PKI certificates issued by the DoD or NSS PKIs or PKI certificates issued by the Intelligence Community (IC) PKI.

5–5. Tactical PKI for non-person entities

a. Army components capable of issuing tactical OLT NPEs PKI certificates on NIPRNet and SIPRNet NPE devices must be subordinate to, and interoperable with those operated by the approved PKIs listed in paragraph 5–4. Army components that operate a tactical OLT NPE PKI that is not subordinate to an approved PKI listed in 5–4 must submit requirements and justification to the Army ICAM IPT.

b. Army components are authorized to issue OLT NPE Public Key Infrastructure (PKI) certificates on all tactical networks.

5–6. Requirements for Personally Owned Devices to Access Unclassified Information Systems

a. DoD and Army policy authorizes personally owned devices (non-Government Furnished Equipment (non-GFE) to access DoD information systems (IS) based on the credential strength used for authentication (for example username and password (UN/PW), Multifactor authentication (MFA), (Common Access Card (CAC)) and the type of Controlled Unclassified Information (CUI) being accessed.

b. Army Data and system owners are responsible for determining the sensitivity level of their data and the credential strength required to access that data based on the impact (Low, Moderate and High) to the DoD mission if the data were compromised.

c. Army systems owners are also responsible for ensuring the appropriate security controls are in place to safeguard CUI data based on Federal, DoD and Army policy requirements.

d. DoD 8520.03 and Army Regulation 25-2 authorizes personally owned devices to access sensitivity level 1, 2 and 3 data using the appropriate credential strength. Accessing sensitivity level 4 CUI from personally owned devices requires approval from the authorizing official (AO).

(1) Sensitivity Level 1 data is categorized as data that is personal in nature and pertains to a single individual such as Personally Identifiable Information (PII) and Protected Health Information (PHI). This type of CUI data would have a low impact to the DoD mission if the information were compromised. Policy allows access to your own Sensitivity Level 1 PII, and PHI using a DoD Self-service Logon (DS Logon) UN/PW credential from a Self-Service web portal or to access non-Self Service web-based training with a non-DS Logon UN/PW credential.

(2) Sensitivity Level 2 data is considered business sensitive and provided by a source or sources, such as a commercial or foreign government partner, under the condition that it not be released to other parties presents a low or moderate impact to DoD mission if compromised. To access systems hosting sensitivity level 2 data from a personally owned device requires the use of a hardware token technology, such as a multifactor one-time password or PKI certificate technology solution.

(3) Sensitivity Level 3 data is operational sensitive information such as that in DoD payroll, finance, logistics, and personnel management systems and would have a moderate or high impact to the DoD mission if compromised. To access systems hosting sensitivity level 3 data from a personally owned device requires the same hardware token technology used for accessing systems hosting sensitivity level 2 data.

(4) Sensitivity Level 4 data is Combat mission sensitive information that is critical to DoD missions, such that unauthorized access to or compromise of this information could result in severe mission capability degradation, major damage to DoD information based resources, or a risk of serious injury or death to personnel. Personally owned devices are not authorized to access this data without AO approval. Access to systems hosting sensitivity level 4 data requires a hardware PKI token such as a CAC or NIPRNet Enterprise Alternate Token System (NEATS) token.

5–7. Exemptions

a. The following use cases describe situations and environments where Army organizations may issue DoD approved UN/PW credentials to users (that is, Identity Assurance Level (IAL) 2/Authenticator Assurance Level (AAL) 1, see NIST SP 800–63A, NIST SP 800–63B, and NIST SP 800–63C). Army organizations must implement risk mitigations for these use cases to prevent users from accessing high-sensitivity information that requires a higher credential strength such as a PKI token (for example, CAC). DoDI 8520.03 defines information sensitivity levels and credential strengths. Army organization's chief information security officers must validate, in Defense Cyber scope, all claims a network, Information System (IS), or user(s) fall under one of these use cases. Army organizations must utilize the DoD RMF described in DoDI 8510.01 to regularly verify whether UN/PW for the network, IS, or user is still required. If an IS

has both UN/PW users and non-UN/PW users, the IS must still require the non-UN/PW users to authenticate with DoD approved PKI, MFA, or IFS. Systems authorized to use UN/PW authentication must transition to an Army approved MFA solution when available and technically feasible. DoDI 8520.03 and AR 25–2 authorizes UN/PW from privately owned IT to access data at sensitivity level 1 (your own personal data). Sensitivity level 1 data is categorized as personally identifiable information (PII). To access PII in aggregate (sensitivity level 3) requires a hardware token (for example, CAC).

b. Certain systems are exempted from the requirement to be PKE for user authentication as a matter of DoD and DA policy due to specific circumstances that prevents the use of PKI or MFA. These systems must use compensating controls to help mitigate the use of single-factor username/password logon, which strengthens network security.

c. Compensating controls such as the use of physical access control for standalone systems and ISs that are part of closed restricted networks (CRNs) that are not externally connected to live operational networks; do not have the ability to access the network infrastructure; cannot transmit, receive, route, or exchange information outside of the system or network boundary; and that reside in physical spaces that restrict access to only authorized users may use username/password or approved MFA for authentication.

d. DoDI 8520.03 names the following exceptions:

(1) Unclassified internet based systems specifically intended to engage DoD mission partners, known and unknown, in nontraditional missions such as humanitarian assistance, disaster response, stability operations, or building partner capacity.

(2) Sensitive compartmented information and ISs operated within the DoD that fall under the authority provided in ICD 503. DoDI 8520.03 also does not apply to top secret collateral systems or special access programs.

e. Additional networks and systems exempt from PKE requirements include the following:

(1) *Stand-alone networks and systems.* A stand-alone network is not connected to any other network, and does not transmit, receive, route, or exchange information outside of the network's authorization boundary. DoDI 8500.01 defines stand-alone systems. Army AOs should require the strongest feasible authentication methods for these networks and systems, but may allow DoD approved, non-DoD Self-Service Logon (DS Logon) UN/PW.

(2) *Closed restricted network.* A CRN is a closed Type IV system enclave not logically connected to any other global system or network, such as the internet, NIPRNet, or SIPRNet, but that cryptographically tunnels over one or more of these networks for transport purposes. CRN traffic must be encrypted end-to-end over the transport network using DoD approved cryptography. Army AOs should require the strongest feasible authentication methods for these networks but may allow DoD approved non-DS Logon UN/PW.

(3) *Platform information technology.* Army organizations will consult with DoDI 8500.01 and DoDI 8510.01 regarding authentication and other cybersecurity requirements for platform IT.

(4) *Lab and testing environments.* Army organizations may permit DoD approved non-DS Logon UN/PWs to be used in lab and testing environments that wholly or partially are isolated from the Department of Defense Information Network (DoDIN). Many of the systems in these environments are either immature, still in development, or perform testing for the purposes of system validation where PKI, MFA, and IFS are infeasible. At a minimum, these systems must operate in an out-of-band environment with no email or web access capabilities. Once a system is ready to be put on the DoDIN, it must be brought into compliance with strong authentication and other cybersecurity requirements as part of the authorization to operate process.

(5) *Emergency, backup, and local logon accounts.* Army organizations may permit DoD approved non-DS Logon UN/PWs to be used for authentication to these types of privileged accounts, when required to do so by applicable DISA Security Technical Implementation Guides or Security Requirements Guides.

(a) Emergency accounts are established in response to crisis situations. The accounts must be automatically deactivated after a preset amount of time.

(b) Backup accounts are able to read and write to any file in a system. Due to these privileges, these accounts must be closely tracked.

(c) Local logon accounts are used when network or normal logon/access is unavailable. They must not be used at any other time.

(6) *Tactical, deployed, or low bandwidth environments.* There are certain deployed or tactical environments or situations where either the system or the network infrastructure cannot support DoD approved PKI, MFA, or IFS, or the user cannot obtain DoD approved PKI, MFA, or IFS. The base commander or on-site commanding officer may authorize the issuance of DoD approved non-DS Logon UN/PWs to users operating in these environments. Base commanders or on-site commanding officers must:

(a) Determine feasibility of supporting PKI, MFA, or IFS based on operational risk, warfighter safety, and available IT infrastructure.

(b) Direct and enforce limits on which networks, systems, and information the tactical, deployed, or low bandwidth users can access with UN/PW.

(c) Ensure the SO or AO of relying parties are briefed on the situation and user requirements for access to their systems.

(d) Revoke user's UN/PW after the user is redeployed from the tactical, deployed, or low bandwidth environment.

(7) *Medical devices.* Users may authenticate to certain medical devices with a DoD approved non-DS Logon UN/PW.

f. Nonprivileged user populations residing on an unclassified DoD IS are exempt from using a PKI token for authentication. This includes—

(1) *Servicemembers for life, dependents, and students.* DoD retirees, dependents, students, and employees may authenticate from their own non-DoD personal devices (that is, privately owned IT) to their own Sensitivity Level 1 PII and protected health information (PHI) with a DS Logon UN/PW. These users are also authorized to use a non-DS Logon UN/PW for domain logon via Soldiers for Life–Transition Assistance Program Center Workstations.

(2) *Students in schoolhouse environments.* Students in schoolhouse environments may authenticate to the schoolhouse domain with a non-DS Logon UN/PW to "Recruit, Train, and Equip" content that is low-risk and nonsensitive.

(3) *Servicemembers, employees, and students accessing web based training.* These users may authenticate from their privately owned IT to access non-FOUO web based training.

(4) *Nontraditional mission systems.* Users may authenticate with a DoD approved non-DS Logon UN/PW to unclassified internet based systems specifically intended to engage DoD mission partners, known and unknown, in nontraditional missions such as humanitarian assistance, disaster response, stability operations, or building partner capacity (for example, Coalition Accounts, All Partners Access Network).

(5) *Non-Five Eyes foreign nationals.* Non-Five Eyes (FVEY) foreign nationals authenticating from foreign countries who are not eligible for or cannot obtain CACs, ECAs, ALTs, or DoD approved MFA, may authenticate with a DoD approved non-DS Logon UN/PW to Sensitivity Level 1 and 2 information. DoD components must closely monitor the activity of these users and revoke, reissue, or reproof for passwords as necessary.

(6) *Pre-accession recruits, reservists, and National Guard members.* Reservists, National Guard members, and new recruits to the U.S. Armed Services who have not yet been issued a DoD ID number, may authenticate with a DoD approved non-DS Logon UN/PW to Sensitivity Level 1 information. Once these users are issued DoD ID numbers, their UN/PW must be revoked, and they must be issued a CAC.

g. Nonprivileged user populations that reside on a classified IS and are exempt from using a PKI token for authentication include—

(1) DoD non-DEERS users, who must follow the direction in the DoD CIO Memorandum, "SIPRNet PKI Tokens for Contractor SIPRNet Enclaves." Since the memorandum was signed, the capability for non-Microsoft active directory (AD) environments to support PKI network crypto-logon to the SIPRNet has been developed. DoD sponsors of non-AD connections must now configure the connections to require user network crypto-logon with DoD NSS SIPR PKI tokens.

(2) FVEY users accessing the SIPRNet via UN/PW are authorized uninterrupted access via the SIPRNet REL DMZ account management process until the deadlines for their respective nations in the DoD CIO Memorandum, "Requirements for the FVEY Nations to Establish PKI Interoperability with DoD Classified Networks." This access is granted as an interim solution while FVEY partners complete development, testing, and validation for PKI based authentication to the SIPR REL DMZ proxy.

h. Privileged users must use an Alternate Smartcard Logon (ASCL) PKI token, NIPRNet NEATS PKI token or a DoD/Army approved MFA solution to authenticate to NIPRNet or SIPRNet systems and applications. Privilege users require a waiver to use UN/PW authentication. Waivers grant organizations a temporary exemption to policy (1 year) until the organization can comply with policy requirements.

i. Exemptions based on DoD policy do not require formal approval from Army CIO or from DoD. However, for RMF security control assessment purposes, the non-use of PKI based ID and authentication must be documented. Documentation must—

(1) Cite the policy basis for tailoring out PKI controls.

(2) Provide an explanation of how the system meets the criteria of the exemption.

j. For systems that are exempt from the requirement to be PKE for user authentication or have been granted a waiver by the Army CIO, the following standards must be implemented:

(1) Remove, change, or disable all default, system, factory installed, guest, function-key embedded, or maintenance accounts and passwords.

(2) All system or system-level passwords and privileged-level accounts (for example, root, enable, admin, administration accounts, and so on) will have a minimum of a 15-character case sensitive password changed every 60 days.

(3) All user level, user generated passwords (for example email, web, desktop computer, and so on) will have a minimum of a 14-character case sensitive password changed every 60 days.

(4) Password history will be set to a minimum of 10.

(5) Accounts must be configured to be locked after three unsuccessful login attempts within a configurable time period in accordance with the appropriate Security Technical Implementation Guides. Accounts must be configured to be locked until unlocked by a system administrator. Accounts must not be configured to automatically unlock after a set time period.

(6) Passwords will be a mix of uppercase letters, lowercase letters, numbers, and special characters, with the minimum number of characters as specified in the applicable DISA Security Technical Implementation Guides.

k. For operating system service accounts, the following standards must be implemented:

(1) All system, system-level, and service account passwords manually generated and entered by an administrator must be changed yearly or upon loss of system administrator that had knowledge of password, whichever is earlier.

(2) System, system-level, and service account passwords randomly generated and automatically entered into systems do not have to be changed as frequently.

(3) Many Windows Services do not require accounts to operate effectively. SOs must reevaluate the need for Windows service accounts when modernizing legacy applications and minimize their use unless required.

5–8. Reporting

DoD has implemented a cybersecurity scorecard reporting system to track status of, and improvement to, cybersecurity across the department. Status of PKE of systems and PKI use by privileged users are specifically reported, and ID/authentication impacts other reporting areas. To ensure correct reporting, all organizations must—

a. Report PKE status of Army ISs in both the Army Portfolio Management Solution (APMS) and the Enterprise Mission Assurance Support System (eMASS) authoritative databases. The data in APMS and eMASS referencing PKI compliance and reporting should match.

b. Ensure architecture artifacts, PKI control data, and other information related to PKI are entered as required into eMASS. Additional information related to meeting PKI compliance such as the plan of action and milestones (POA&M) and funding data that will facilitate achievement of PKI compliance are also entered. Additionally, clearly identify the planned end state and any intermediate capabilities or alternate MFA authentication employed.

c. Additional reporting to ensure compliance with special or short term requirements may be required. Details regarding format, content, and level of detail will be provided by the NETCOM and/or the Army CIO as required.

d. Once PKI compliance is achieved, both the APMS and eMASS repositories must be updated in concert to reflect the change in PKI status.

e. Guidance regarding PKI waivers, in the interim of compliance, must be staffed via the Army CIO and/or the Defense Security/Cybersecurity Authorization Working Group as the process is codified by the DoD CIO to the Services.

Chapter 6
Alternate Multi-Factor Authentication

6–1. Description and requirement

a. MFA is the use of two or more of these authentication factors—

(1) Something you know (for example, password or PIN).

(2) Something you have (for example, ID badge or hardware token).

(3) Something you are (for example, fingerprint or other biometric data).

b. Environmental data, such as location or device identity, is not an authentication factor.

c. Repeating one type of authentication factor is not MFA.

d. PKI is an example of an MFA technology.

e. DoD requires authorized users to authenticate to DoD ISs and applications with a CAC or DoD approved alternate MFA.

f. DoDI 8520.03 states that the DoD alternate MFA standard for DoD IS users is a SIPRNet or NIPRNet ASCL hardware token.

g. DoD requires authorized users to authenticate to DoD ISs and applications with DoD approved PKI credentials but permits other DoD approved MFA solutions when PKI is infeasible.

h. DoD approved MFA and IFS solutions can be found here: https://cyber.mil/idam/idam-program-documentation/. See the DoD Documentation Section.

i. In circumstances where MFA cannot be implemented using NIPRNet or SIPRNet PKI, but is still required per NIST SP 800–53A, Revision 4 and Committee on National Security Systems Instruction (CNSSI) 1253 security controls, an alternate MFA technology may be used.

j. DoD approved MFA or IFS solutions will be considered before any other MFA or IFS solutions are considered.

(1) EAMS–A is the Army's DoD-approved IFS that provides alternative MFA solutions (for example, MobileConnect and cryptographic hardware token).

(2) SOs must submit their requirements to the Army ICAM IPT if they identify gaps in existing approved capabilities.

k. SOs that require the use of a non-Army approved MFA must follow the process outlined in paragraph 6–5 to request approval.

l. UN/PW logon is a single-factor authentication solution that is less secure than MFA solutions. UN/PW logon is authorized for specific use cases only as described in paragraph 5–4.

m. Army approved UN/PW login includes the following:

(1) *DoD Self-Service Logon.* DS Logon is a secure, self-service logon ID account for unclassified DoD ISs provided by DMDC. DS Logon can only be used for self-service, web based IS.

(2) *Non-DoD Self-Service Logon username/password.* These UN/PWs must meet the requirements for IAL 2/AAL 1 in NIST SP 800–63–3 and can be used for web based and domain logon as described in paragraph 5–4 of this pamphlet.

6–2. Use of biometrics for authentication

a. This guidance pertains to the use of biometrics data for logical access to Army IT resources. It does not cover the use of biometrics for physical access control, threat actor identification and tracking, law enforcement, or intelligence activities. It also does not cover the common storage, matching, analysis, and sharing activities of the DoD biometrics enterprise for biometric data collected as a part of military operations.

b. Specifically, Army guidance on using biometrics for logical access is as follows:

(1) Biometrics may be used as an additional authentication factor (such as one factor of an approved MFA solution). Biometrics cannot be used as the ONLY authentication factor to access Army IT resources except in a tactical environment when operational mission imperatives dictate its use.

(2) When DoD-approved hardware PKI is required, biometrics may be used as an authentication factor in combination with those hardware PKIs. When DoD-approved alternate MFAs (for example, Rivest-Shamir-Adleman (RSA) secure ID or YubiKeys) are permitted, biometrics may be used as an authentication

factor in combination with those approved MFAs (for example, RSA secure ID with a biometric instead of RSA secure ID with a PIN). When UN/PW is permitted, biometrics may be used in combination with (not in lieu of) the UN/PW.

(3) Biometrics data used for logical access will not be collected or stored in any centralized IT system or repository, Army enterprise-wide or within a local network IT resource, so as to reduce the attack surface of the network.

(4) Biometrics data used for logical access to the Army's network must remain securely within the user's control (for example, on a device that remains in the user's possession) and not be transferred or accessed across the network—biometric data cannot be stored in a central repository/server and transferred across the network to authenticate users for logical access.

(5) Biometrics data may be used for authentication on personally owned endpoint devices (laptops, tablets, smartphone, and so forth.) when in compliance with NIST SP 800–63B.

(6) Biometrics capabilities that are commercially available on existing, or already purchased government furnished equipment must be the material approach to capture and store biometrics data on that given device, when in compliance with DoD and Federal cryptographic standards. This approach must be exhausted before any consideration or justification is given to expending dollars for one-off or add-on solutions.

(7) Any use of biometrics capabilities must comply with applicable host-nation agreements, and or international policy requirements when used for Foreign National employees supporting the DoD and meet the data-at-rest security requirements outlined in DoDI 8420.01.

6–3. Department of Defense approved Public Key Infrastructure

a. Approved authentication capabilities. The following provides DoD approved authentication capabilities for DoD unclassified and secret networks:

(1) *Common access card.* The CAC is the primary DoD PKI credential for logical authentication to unclassified DoD networks, systems, servers, and applications. The CAC meets the criteria for AAL 3 in NIST SP 800–63–3.

(2) *Nonclassified Internet Protocol Routing Network alternate logon token.* The DoD ALT is the mandated DoD PKI credential for authentication to privileged user accounts on the NIPRNet. The ALT is also used for group and role accounts and may be used for NIPRNet logon in accordance with DoD policy.

(3) *External certification authority Public Key Infrastructure credentials.* ECA medium token assurance and medium hardware assurance PKI credentials may be used to authenticate to unclassified DoD ISs but may not be used for network logon and authentication to privileged user accounts. These ECA PKI credentials meet the requirements for AAL 3 in NIST SP 800–63–3. For more ECA information, see https://cyber.mil/eca/.

(4) *Personal identity verification Public Key Infrastructure credentials.* DoD approved Federal PIV PKI credentials qualify as AAL 3. DoD approved PIV PKI credentials may be used for both network logon and authentication to unclassified DoD ISs on unclassified DoD networks. DoD approved PIVs are listed at https://cyber.mil/pki-pke/interoperability/.

(5) *Personal identity verification–interoperable and industry partner Public Key Infrastructure credentials.* DoD approved personal identity verification–interoperable (PIV–I) PKI credentials and industry partner medium hardware PKI credentials qualify as AAL 3 in NIST SP 800–63–3. DoD approved PIV–I PKI credentials and industry partner medium hardware PKI credentials may be used to authenticate to unclassified DoD IS but may not be used for network logon and authentication to privileged user accounts. DoD approved PIV–I PKI credentials and industry partner medium hardware PKI credentials are listed at: https://cyber.mil/pki-pke/interoperability/.

(6) *Five Eyes mission partner Public Key Infrastructure credentials.* FVEY users must use either ECA Medium Token Assurance (or above) PKI credentials or their own unclassified PKI credentials to authenticate to unclassified DoD systems. Unclassified FVEY PKI credentials must be issued under a FVEY unclassified PKI root CA cross-certified with a DoD PKI, in line with Allied Communication Publication 185.

(7) *Secret classified networks.* For example, SIPRNet.

(a) National Security Systems Secure Internet Protocol Router Network Public Key Infrastructure token. The NSS SIPRNet PKI Token is the primary credential for logical authentication to Secret classified DoD networks, systems, and applications.

(b) Department of Defense National Security Systems Secure Internet Protocol Router Network Public Key Infrastructure Admin-I token. The DoD NSS SIPR PKI Admin-I token is the mandated DoD PKI credential for authentication to DoD administrative accounts on the SIPRNet.

(c) Federal partners. NSS PKI tokens from other Federal departments and agencies are approved for authentication to SIPRNet DoD resources, provided the Federal entity has connected their NSS secret classified network to the SIPRNet via the FED DMZ in accordance with the DoD CIO Memorandum, "Improving Security of Federal Department and Agency Connections to the DoD SIPRNet FED DMZ."

(d) Contractors at contractor facilities. DoD contractors who access the SIPRNet via contractor-facility enclaves must obtain NSS SIPRNet PKI tokens from their Army sponsors.

(e) Five Eyes mission partner Public Key Infrastructure credentials on the Secure Internet Protocol Router Network.

b. Mobile Public Key Infrastructure credentials. At this time, DISA's Purebred is the only authorized DoD derived PKI credential issuance system. DoD approved MFA and IFS may be used to authenticate to unclassified DoD resources via a mobile device.

6–4. Assurance standards

a. NIST SP 800–63–3A defines a set of IALs and corresponding validation requirements for establishing confidence in entity/user identities electronically presented to an IS. DoDI 8520.03 defines sensitivity levels for the determination of appropriate authentication methods and mechanisms. NIST IAL and validation requirements assert the degree of confidence that others may reasonably place in the binding of a user to the identity and privileges asserted in a presented digital certificate.

b. NIST SP 800–63–3B provides recommendations on types of authentication processes, including choices of authenticators, that may be used at various AALs. Any MFA used in place of the CAC, NIPRNet ASCL, or SIPRNet token must conform to the same AAL standards as the PKI technologies they would replace in order to be used to access data of the same sensitivity level (unless DoD approved/authorized by the Army AO); see the Entity Environment Chart in DoDI 8520.03 to align credential strengths with data sensitivity levels.

c. The CAC, NIPRNet ASCL, and SIPRNet token meet AAL 3. Per NIST SP 800–63–3B, AAL 3 authentication will use a hardware-based authenticator.

d. MFA credentials appropriate for DoD and Army use are determined by the sensitivity level of the data that is being accessed and the environment from which that data is accessed. NIST SP 800–63–3B lists approved authenticators (that is, credentials) for AAL 1 through AAL 3. DoDI 8520.03 lists the appropriate credentials required to access data of specific sensitivity levels.

e. MFA credentials authorized within the DoD and Army must—

(1) Provide identity authentication using at least two authentication factors.

(2) Comply with specified identity proofing, registration, issuance, and CSP.

6–5. Technical requirements

a. Requests for alternate MFA solutions must include a system risk assessment that—

(1) Addresses the threats to the ID and authentication processes.

(2) Describes how the proposed solution counters, compensates for, or mitigates those risks.

(3) Considers the following threats (as a minimum):

(a) Eavesdropping attacks.

(b) Replay attacks.

(c) Man in the middle attacks.

(d) Token device theft/reuse.

(e) Token device substitution.

(f) Credential cloning (replication).

(g) Enrollment attacks.

(h) Seed key attacks.

(i) Brute force PIN attacks.

(j) Audit log attacks.

(k) Biometrics templates attacks (biometric solutions).

(l) Attacks against stored biometrics data (biometric solutions).

b. A proposed MFA must also—

(1) Have documented reliability in all potential operating environments (for example, dust, high/low temperature, low light).
(2) Provide operational efficiency (for example, cost to implement, operate, and maintain; administrative overhead requirements).
(3) Allow effective implementation (for example, ease of integration with existing system, impact to system processing times, user impact).
(4) Comply with standards and guidelines (for example, FIPS 140–2, Unified Capabilities Approved Products List, DISA Security Technical Implementation Guides).
(5) Use validated components/products (for example, NIST-validated FIPS 140–2, National Information Assurance Partnership-compliance, and so on).
(6) Demonstrate assurance that any reference biometric was derived from a living sample (biometrics solutions).
(7) Provide performance reliability regarding false positives/false negatives (biometric solutions).
(8) Include detailed identity proofing, registration, issuance, and CSP process and procedure documentation.
c. Any MFA proposed should reflect the results of respected private industry evaluations (for example, Gartner's Magic Quadrant for User Authentication, 1 December 2014) and/or reference existing evaluations and approval to operate (ATO) elsewhere in DoD and/or Federal departments and agencies.
d. Alternate MFA solutions may use credentials derived from CACs, NIPRNet ASCL tokens, or SIPRNet tokens. See NIST SP 800–157 for additional information and guidance.

6–6. Requesting approval to use alternate (non-Public Key Infrastructure) multi-factor authentication

a. In accordance with policy, PKI is the standard MFA solution within DoD. MFA solutions proposed in place of direct PKI authentication on SIPRNet or NIPRNet, or EAMS–A must receive Service-level approval prior to implementation and use if not already approved by DoD and Army policy. The Army CIO is the service approver for the Army.
b. MFA may only be used when a system or application does not support authentication using DoD approved PKI credentials or a portion of the system's or application's subscribers are unable to obtain DoD approved PKI credentials.
c. SOs seeking approval for MFA and IFS solutions that are not DoD approved must coordinate directly with the Army CIO PKI Office.
d. SOs will fully document implementation of alternative MFA as part of their RMF compliance documentation. This must include—
(1) Technical aspects of the implementation (that is, how the solution is installed, who does it, who maintains it, and so on).
(2) How users are added to the system, including identity proofing requirements, procedures, and documentation?
(3) How the solution will be funded (if not part of system development)?
(4) What process is followed if the MFA functionality fails (and users must revert to Username/Password access)?
e. Requests must include documentation to support—
(1) Inability to use a SIPRNet or NIPRNet ASCL token (justification for non-use).
(2) Mitigation of system risks introduced by the non-PKI MFA solution.
(3) Compliance with DoD, Federal, and industry standards and guidelines.
(4) Use of validated components and products or why such use is not appropriate.
(5) Compliance with specific RMF controls relating to ID, authentication, and access control.
(6) Implementation of the identity proofing, registration, issuance, and CSP requirements supporting the MFA solution.
(7) Compliance with technical requirements described in paragraph 6–3.
f. Requests for approval of non-PKI MFA must—
(1) Be signed by the system AO, or by the PM for systems in development.
(2) Be routed through the requesting organization's servicing Network Enterprise Center.
(3) Be sent for staff review and approval to the Army CIO/G–6 PKI mailbox, "usarmy.pentagon.hqda-cio-g-6.mesg.idam-and-pki-requests@mail.mil."

g. The Army CIO will approve the request in writing or disapprove with justification. Disapproved requests may be resubmitted when the reasons for such disapproval have been addressed.

h. SOs that have obtained Army CIO approval of the proposed MFA/IFS solution will be required to brief the DoD Privileged User Working Group and seek approval from the DCIO–CS.

i. Final approval of non-PKI MFA solutions will be included in the system PKI/MFA Plan. It is an artifact of the system Security Plan Approval Package as described in the NETCOM document "Stand-Alone Information System and Closed Restricted Network Assessment and Authorization Operational Tactics, Techniques, and Procedures," Version 1.0, April 2016.

j. The system Security Plan Approval Package must be included as an artifact of the system RMF compliance documentation.

Chapter 7
Trust of External Public Key Infrastructure

7–1. Federal Bridge

a. Some Army SOs, end users, and applications trust Army and external networks through the Federal Bridge (including PIV and PIV–I) or through external certification authorities (ECAs). Such use is authorized per DoD CIO Memorandum. See appendix E for Army best business practice for trust of external PKI.

b. This does not apply to DoD gateways such as the SIPR REL DMZ. They are governed by their own standard operating procedures.

7–2. Non-Department of Defense Public Key Infrastructure credentials

Use of interoperable, non-DoD PKI credentials enables secure information sharing with DoD partners, supports appropriate access control (partners can't access information intended for CAC holders only), helps partner organizations eliminate the cost and management overhead of issuing partners CACs, and facilitates Federal policy compliance.

Chapter 8
Requests for Exception to Army or Department of Defense Policy

8–1. Need for exception

a. Certain users may require an exception to the CNSS requirement that all SIPRNet users use PKI tokens for SIPRNet access. These users are described in paragraph 4–13 of this pamphlet.

b. Some systems are unable to be PK enabled due to technical issues or mission constraints. Such systems cannot implement PKI based authentication and therefore need an exception to the requirement.

c. Exceptions must be requested and received prior to system deployment and use.

8–2. General

a. Exceptions to Army or DoD policy for users or systems unable to comply with SIPRNet or NIPRNet token use or PKE requirements are limited to 12 months (1 year) but may be renewed.

(1) Exceptions to Army policy are granted by the Army CIO.

(2) Exceptions to DoD policy must be requested through the Army CIO to the cognizant DoD exception authority.

b. Exceptions to policy are granted in one of three types, each with somewhat different documentation requirements—

(1) Systems (Type 1).

(2) Tools (Type 2).

(3) Users (Type 3).

c. Exception guidance and criteria checklists for all three types is provided at appendix D.

8–3. Exception memorandum format and content

a. Submit memoranda requesting exceptions on organizational letterhead and include—

(1) Organization.

(2) Point of contact for the exception request.

(3) System name and acronym.
(4) System description.
(5) Exception requested (use of PKI, use of alternate MFA, use of user ID/password, and so on).
(6) Reason for exception (including citation of specific relevant policy).
(7) Impact if denied.
(8) Expiration date (no longer than 12 months from the date of the request).
(9) Risk assessment to DoDIN-Army (formerly Land Warrior Network (US Army enterprise network)).
(10) Risk mitigation.
(11) Contact information (both AO and action officer).
(12) Request date.

b. Exception requests anticipated to recur must also include a final remediation date.

c. All exception requests must include a copy of the applicable POA&M or an explanation as to why one is not necessary. Requests will be returned without action if a required POA&M or suitable explanation is not provided.

d. All exception requests must be routed through command channels to the Army CIO.

8–4. Document routing and processing

a. Exception requests for systems, applications, and/or devices must be initiated by the SO.

b. Exception requests for individuals or groups must be signed by the commander (O–6/GS-15).

c. Exception requests must be routed through the chain of command to the Army CIO.

d. Exception requests will be reviewed by the Policy and Risk Governance Division of the Army CIO Cybersecurity Directorate prior to staffing to the CIO.

(1) Exceptions to Army policy granted by the Army CIO will be documented to the requesting organization by memorandum.

(2) Exceptions to DoD policy will be endorsed by the CIO to the cognizant authority at DoD for review and approval.

e. Rejected exception requests will be returned to the requesting organization with a reason for rejection. Such requests may be resubmitted when required data is obtained.

Chapter 9
Lost, Stolen, or Malfunctioning Tokens

9–1. Lost or stolen tokens

a. Any token whose location/possession is not known to the user is considered lost if the cause is not deliberate or hostile. For SIPRNet tokens, the standard of positive control described in paragraph 4–7 applies.

b. Any token thought to have been deliberately or intentionally taken without the expressed permission of the user will be considered stolen.

c. Any PKI token that is lost or stolen must be reported to a supporting TA or ETA using the lost/stolen token reporting format provided at appendix F.

d. The supporting TA or ETA will request revocation of any credentials on tokens considered stolen.

e. To ensure the integrity of token usage, the supporting TA or ETA is recommended to query NSS and NIPRNet ASCL token users annually to verify possession of their token.

9–2. Recovered tokens

a. Any token returned to the control of its owner/user after being considered lost or stolen is a recovered token.

b. If a NIPRNet ASCL or NSS token is recovered—

(1) Do not insert the token into a card reader.
(2) Turn in the token to the supporting TA or ETA immediately.
(3) The TA/ETA will contact the RA/LRA for disposition.

c. If a recovered NSS token shows any evidence of tampering, it must be returned to NSA for investigation and/or destruction.

d. Users, TAs, and/or ETAs will not destroy recovered tokens without specific, written authorization from the Army RA.

9–3. Malfunctioning/failed tokens

a. Any token that cannot be unlocked with the correct PIN, cannot be read by the appropriate card reader middleware, or otherwise does not function correctly is considered malfunctioning.

b. Turn in malfunctioning tokens to the supporting TA or ETA.

(1) Tokens will be protected from damage to permit analysis of the cause of the malfunction.

(2) The following information must be provided with all malfunctioning tokens:

(a) Token serial number.

(b) Reader type (make and model).

(c) Number of days after issue that failure occurred.

(d) Approximate number of times used per day.

(e) Error messages (if any).

(f) Token environment (field, office, and so on).

c. Users, TAs, and/or ETAs will not destroy malfunctioning tokens without specific, written authorization from the Army RA.

d. Malfunctioning/failed SIPRNet tokens will be treated as secret and handled/stored accordingly. (Unless the state of the device is positively known, extraction of private keys and other data may be possible.)

Chapter 10
Trusted Agent and Enhanced Trusted Agent Nomination and Approval

10–1. Background

a. TAs and ETAs serve as representatives of the RA at the local level.

b. A TA can—

(1) Conduct user identity proofing.

(2) Assist in the generation of credential requests (see DD Form 2842).

(3) Process and route credential requests to an LRA or RA as appropriate.

(4) Perform credential issue (new and replacement SIPRNet and NIPRNet ASCL tokens).

(5) Assist with token PIN reset or unlock.

c. An ETA can perform the same functions as a TA and can also create replacement SIPRNet tokens.

Note. An ETA cannot normally create new SIPRNet tokens for issue.

d. Neither a TA nor an ETA can create or revoke credentials. This must be done by an RA.

e. Organizations can request the appointment of TAs and ETAs according to their own operational needs.

Note. Token issue requires two TAs/ETAs-one to provide the token to the user, the other to provide the initial token unlocking PIN.

f. TAs and ETAs are part time, additional duties. The organization must fund the TA/ETA position and all required facilities, equipment, supplies, and services, including costs of shipping tokens via registered or certified mail to the Army RA (located at Fort Belvoir, VA).

g. Although TAs and ETAs normally support the organizations to which they are assigned, they may also be required to provide backup to other organizations for credential issue (requires two persons) or emergency situations.

10–2. Qualifications/Requirements

a. TAs/ETAs hold positions of trust within the PKI and therefore must—

(1) Be a U.S. citizen.

(2) Be a DoD employee (may be military, government, or contractor).

(3) Be within the administrative control of a DoD employee or contractor.

(4) Have never been previously relieved of RA, LRA, or communications security. custodian duties (or equivalent positions) in any Federal PKI.

(5) Have never been denied or had a security clearance revoked.

(6) Have never been convicted of a felony.

(7) Be trustworthy.

(8) Be appointed in writing by the organization commander or director.

b. All ETAs and TAs supporting NSS and/or SIPRNet requirements must also have—

(1) A final secret clearance.

(2) Active SIPRNet network and email accounts.

(3) Access to SIPRNet workstations configured with—

(a) 90 Meter Card Issuance Workstation.

(b) A minimum of two SCR3310 v2, Omnikey 3121, or other NSA-approved readers.

(c) Microsoft Internet Explorer browser configured to work with the Token Management System.

(d) Personal computer configuration does not include ActivClient.

c. Nominees must complete the online TA/ETA training located on the U.S. Army milSuite University website located at https://www.milsuite.mil/university/pki-ta-eta-training-certification/.

d. ETA nominees must complete both the TA and ETA training.

e. TA and ETAs must complete annual training for renewal of certification.

f. There is no rank or pay grade restriction on who may serve as a TA or ETA.

g. ETAs will be required to store blank SIPRNet tokens for use in reissuing replacement SIPRNet tokens. Unissued SIPRNet tokens must be secured—

(1) In a safe (General Services Administration (GSA)-approved security container authorized for classified (secret) document storage).

(2) In a physically secured area approved for open storage of sensitive or classified material.

(3) In a manner consistent with local security policy.

f. SIPRNet tokens must be protected from unauthorized access or removal at all times.

10–3. Nomination submission

a. The commander of the proposed TA/ETA must complete a TA or ETA nomination memorandum. The most current version of the TA nomination memorandum can be found at:

https://portal.army.mil, under the TA heading.

b. The nomination memorandum must be signed (physically or digitally) by—

(1) The TA/ETA nominee(s) and alternate nominee(s).

(2) The nominee's supervisor.

(3) The verifying official, who must be—

(a) At minimum, lieutenant colonel/O–5 or GS–14.

(b) The local commander's designated representative (commander's memorandum designating the representative must accompany the request).

c. The completed and signed nomination memorandum, together with copies of the certificates of training for the requisite courses must be emailed to the Army RA at usarmy.pentagon.hqda-cio-g-6.mbx.army-registration-authority@mail.mil. Emails must be sent from an "@mail.mil" email address.

10–4. Nomination approval

a. Individuals must be approved as a TA or an ETA by an Army RA.

b. The RA must respond to a TA or ETA nomination within 30 days.

c. Upon approval, the RA will—

(1) Notify the requesting organization and the TAs/ETAs involved.

(2) Update the TA/ETA roster, located on the NETCOM PKI Portal, located at:

https://portal.army.mil.

(3) Add the new TAs/ETAs to the appropriate email distribution lists.

d. If a nomination is disapproved, the Army RA will notify the verifying official and give the reason for the rejection.

10–5. Maintenance

a. All TAs and ETAs must retake the online TA/ETA training at least once a year to retain their qualification.

b. A TA or ETA must be terminated if the commander or supervisor determines that the TA/ETA—

(1) No longer meets the criteria in paragraph 10–2*a* or 10–2*b* of this pamphlet.

(2) Has been convicted of a felony.

(3) Demonstrates a lack of integrity.

(4) Departs the organization for any reason, including PCS, termination of service or contract (including discharge), or end of employment.

c. The commander or supervisor must report termination of a TA/ETA to the Army RA via signed email to usarmy.pentagon.hqda-cio-g-6.mbx.army-registration-authority@mail.mil as soon as possible.

d. If an individual is no longer qualified to remain a TA or ETA, the RA will—

(1) Remove them from the TA/ETA roster and any email distribution lists.

(2) Will notify the organizational commander that the individual may no longer serve as a TA or ETA.

(3) If removal is for cause, make appropriate note in the Army PKI records to preclude the individual from serving as a TA or ETA in the future.

Chapter 11
Registration Authority and Local Registration Authority Nomination and Approval

11–1. Background

a. The Registration Authority (RA)/LRA is the combatant command/service/agency (CC/S/A) registration component within the DoD PKI. The Certification Practice Statement (CPS) defines the practices, policies, and procedures under which the RAs and LRAs operate.

b. RA and LRA personnel provide 24/7 support to the Army for NIPRNet ASCL and SIPRNet token issue, management, and revocation, as well as token management.

(1) An RA can interact with the PKI credential management infrastructure to create, revoke, and manage credentials, as well as other functions relating to credential management. The RAs are centralized in the Washington, DC area (mainly at Fort Belvoir, with a branch at the Pentagon).

(2) An LRA is authorized by an RA to support users, primarily for a particular group, office, or geographic location. LRAs are located worldwide at major commands and headquarters, based on workload and mission requirements.

c. The RAs supporting Army and LRAs in the Washington, DC area are under NETCOM. NETCOM provides day-to-day operational oversight and balances work based on mission needs and known requirements. LRAs outside the DC area are the responsibility of their parent commands.

d. RA operations are subject to an annual DISA audit. LRAs are inspected/audited by Army CIO personnel annually. NETCOM is responsible for RA compliance with the policies cited in paragraph C–4. LRA compliance with the same policies is the responsibility of their respective commands.

e. Each RA or LRA site must have an ISSO and system administrator assigned to the workstations.

11–2. Scope of duties

a. An RA is an official who interacts with the PKI credential management infrastructure to create, revoke, and manage credentials. RA privileges include—

(1) Revocation or suspension of any certificate, including certificates approved for issue by RA/LRAs from other services or agencies.

(2) Restoration of suspended certificates.

(3) Approval of all credential issue to users pre-registered by an LRA.

(4) Registration of new LRAs and termination of old ones.

(5) Able to add, modify, and delete directory entries.

(6) Can approve issuance of certificates to network NPEs.

(7) Registration of individuals to receive, and approval of issuance of, organizational code signing certificates.

b. LRAs are authorized by an RA to authenticate users, primarily for a particular group, office, or geographic location, to verify the identity and user information for each user under its purview. LRAs register users in their organizations with the PKI and perform face-to-face identity authentication of the users (either directly or via a TA). LRAs can load credentials to tokens and issue them to users. LRAs are authorized to maintain a stock of blank tokens on hand to support this activity. LRAs can request that certificates be revoked, suspended, or restored based on circumstances covered in the CPS or Registration Practice Statement (RPS).

c. RAs and LRAs must comply with all provisions of—

(1) CNSSI 1300.

(2) NSS PKI RPS dated 19 December 2014, Version 8.

(3) United States Department of Defense X.509 Certificate Policy.

(4) DoD Public Key Infrastructure RA/Local Registration Authority CPS, Version 2, 20 May 2015.

d. RAs and LRAs perform their duties under the direction of the lead RA, located at Fort Belvoir, VA.

e. All RA activities are subject to audit by DISA, normally done annually. All LRA activities are subject to audit by DCS, G–6.

11–3. Qualifications and requirements

a. All RAs/LRAs must—

(1) Be U.S. citizens.

(2) Have DoD 8570.01–M Information Assurance Technical Level II baseline or higher (Level III) certification.

(3) Possess a U.S. secret clearance (Tier 3 or equivalent investigation as defined in the Director of National Intelligence (DNI) Federal Investigative Standards (FIS)).

(4) Have favorably completed a single scope background investigation covering at least the past 10 years or to age 18, whichever is less (Tier 5 or equivalent investigation as defined in DNI FIS).

(5) Be a DoD employee (military, government, or contractor) with a CAC.

(6) Be within the administrative control of a DoD employee or contractor.

(7) Have never been previously relieved of trusted role duties for reasons of negligence or nonperformance of duties.

(8) Have never been denied or had a security clearance revoked.

(9) Be appointed in writing by the organization commander or director.

(10) Have never been convicted of a felony offense.

(11) Have active SIPRNet network access and email accounts.

b. Nominees must attend RA/LRA training provided by DISA. Training must be requested through NETCOM G–3/5/7, at email usarmy.pentagon.hqda-cio-g-6.mbx.army-registration-authority@mail.mil. Training must be completed prior to receiving RA or LRA credentials.

c. There is no rank or pay grade restriction on who may serve as an RA or LRA.

d. RAs and LRAs are required to store blank NIPRNet ASCL and SIPRNet tokens for issue. Secure unissued SIPRNet tokens—

(1) In a safe (GSA-approved security container authorized for classified (secret) document storage.

(2) In a physically secured area approved for open storage of sensitive or classified material.

(3) In a manner consistent with local security policy.

e. SIPRNet and NIPRNet ASCL tokens must be protected from unauthorized access or removal at all times.

f. Physically label RA and LRA equipment as being for “DoD/NSS PKI Authorized Use Only.”

(1) RAs and LRAs each require two workstations, one for SIPRNet tokens and one for NIPRNet operations.

(2) RA workstations may only be used for PKI registration activities.

(3) LRA workstations may be used for other than PKI registration activities but may only be used by the designated LRA. It cannot be used by anyone else for any purpose.

11–4. Nominations

a. Individuals identified as an RA/LRA must be nominated in writing by the DCS, G–6 (as the Service proponent), and approved by DISA prior to receiving training and assignment as an RA/LRA. Prospective LRAs must be nominated either by the PKI lead, the Army CIO, or their sponsoring installation/command through the DCS, G–6 to DISA. Appendix H contains samples of the two nomination memoranda.

b. Nominations from installations/commands wishing to sponsor their own LRAs must include a separate letter of justification from the commander to the Army CIO. The justification must state that the requesting command understands that it must fund the position and all required facilities, equipment, and supplies (other than token stocks).

Appendix A

References

Unless otherwise indicated, all Army publications are available on the Army Publishing Directorate website at https://armypubs.army.mil. DoD publications are available on the ESD website at https://www.esd.whs.mil. USCs are available on the USC website at https://uscode.house.gov.

Section I

Required Publications

AR 25–2
Army Cybersecurity (Cited in para 1–1.)

AR 600–8–14
Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel (Cited in para 4–4*c*(3).)

Army Identity Attribute Specification
(Cited in para 3–3*b*.) (Available at https://www.milsuite.mil/.)

CNSSI 1253
Security Categorization and Control Selection for National Security Systems (Cited in para 6–1*i*.) (Available at https://www.cnss.gov/cnss/issuances/instructions.cfm.)

DoD CIO Memorandum, "Approval of External Public Key Infrastructures"
(Cited in para E–1*a*.) (Available at https://www.milsuite.mil/.)

DoD CIO Memorandum, "Department of Defense Acceptance and Use of PIV–I"
(Cited in para E–2*a*.) (Available at https://www.milsuite.mil/.)

DoD CIO Memorandum, "SIPRNet PKI Tokens for Contractor SIPRNet Enclaves"
(Cited in para 5–6*g*(1).) (Available at https://www.milsuite.mil/.)

DoDI 3020.41
Operational Contract Support (OCS) (Cited in para 1–6*b*(3).)

DoDI 8500.01
Cybersecurity (Cited in para 1–6*a*.)

DoDI 8510.01
Risk Management Framework (RMF) for DoD Information Technology (IT) (Cited in para 1–6*a*.)

DoDI 8520.02
Public Key Infrastructure (PKI) and Public Key (PK) Enabling (Cited in para 1–1.)

DoDI 8520.03
Identity Authentication for Information Systems (Cited in para 1–1.)

IETF RFC 6960
X.509 Internet Public Key Infrastructure Online Certificate Status Protocol–OCSP (Cited in para 5–2*c*.) (Available at https://datatracker.ietf.org/.))

Joint Task Force–Global Network Operations (JTF–GNO) Communications Tasking Order (CTO) 07–015 (Cited in para C–4*c*.) (Available at https://www.milsuite.mil/.)

NETCOM Stand-Alone Information System and Closed Restricted Network Assessment and Authorization Operational Tactics, Techniques, and Procedures
(Cited in para 6–6*i*.) (Available at https://www.milsuite.mil/.)

NIST SP 800–53A, Revision 4
Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans (Cited in para 6–1*i*.) (Available at https://csrc.nist.gov/publications/.)

NIST SP 800–157
Guidelines for Derived Personal Identity Verification (PIV) Credentials (Cited in para 4–22*a*.) (Available at https://csrc.nist.gov/publications/.)

Public Law 104–106
National Defense Authorization Act for Fiscal Year 1996, also known as The Clinger-Cohen Act, formerly Division E, Technology Management Reform Act (Cited in para 1–1.) (Available at https://www.govinfo.gov/.)

United States Department of Defense X.509 Certificate Policy
(Cited in para 11–2*c*(3).) (Available at https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/pdf/unclass-dod_cp_v10-6_20180520.pdf.)

10 USC 2223
Information Technology: additional responsibilities of Chief Information Officers (Cited in para 1–1.)

Section II

Prescribed Forms
This section contains no entries.

Appendix B

Identity, Credential, and Access Management Background

B–1. Introduction

a. HSPD–12, signed August 27, 2004, established the requirements for a common ID standard for identity credentials issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally-controlled facilities, and logical access to Federally-controlled ISs.

b. The PIV card has been designated for use by Federal employees and other direct support members as the primary credential ID and verification source. The PIV–I card has been designated for use by non-federal employee and other support members to perform the same function. Also, the CAC has been designated for use by DoD employees, military, and eligible DoD contractors as primary credential ID and verification, as well as to be used during IT systems and network authentication and access.

c. Furthermore, PKI is the system used to grant access to DoD and Army networks and systems once user identity has been confirmed. Access is then granted based on verified authentication to approved networks and systems. In addition, the IS or DoD network must ensure that any credential used for identity authentication has been issued by an approved DoD identity credential provider or a DoD approved Federal or industry partner identity credential provider.

B–2. Identity, credential, and access management overview

a. ICAM is the set of policies, processes, standards, and technologies that ensure authorized person entities and NPEs have secure access to Army IT resources anytime and from anywhere.

b. The DoD Information Enterprise Architecture ICAM Reference Design states that DoD ICAM consists of all DoD capabilities that manage and use PE and NPE digital identities and associated data to:

(1) Provide access to and protection for DoD IT-based resources and DoD electronic physical access control system-protected resources.

(2) Provide access accountability by recording ICAM activity.

(3) Enable person entities to look up contact data for person and non-person entities.

c. The Army ICAM Enterprise Reference Architecture Version 4.0 adds to the collection of strategic level architectures by building upon the existing set of Army identity management architecture rules and views with the purpose of refining the guidance and constraints of Army enterprise and component solution architectures.

d. The ICAM Reference Architecture provides additional guidance on specific ICAM subject areas identified by the Army and the broader DoD and Federal ICAM community. In addition to ICAM coordination with mission partners, this Reference Architecture supports the Federal Identity, Credential and Access Management (FICAM) guidance and standards and all applicable executive and Federal guidance and mandates.

B–3. Key functions

a. Before identity authentication is accomplished identity proofing must be conducted. During identity proofing, the applicant is required to provide two forms of identity source documents in original form. The identity source documents must be bound to that applicant and must neither be expired nor cancelled. If the two identity source documents bear different names, evidence of a formal name change must be provided. See FIPS 201–2 for acceptable identity proofing documents.

b. This guidance describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to their identity. In this context, assurance is defined as—

(1) The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued.

(2) The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. The four assurance levels are—

(a) Level 1. Little or no confidence in the asserted identity's validity.

(b) Level 2. Some confidence in the asserted identity's validity.

(c) Level 3. High confidence in the asserted identity's validity.

(d) Level 4. Very high confidence in the asserted identity's validity.

c. DoDI 8520.03 provides greater discussions about the four assurance levels.

B–4. Determining assurance level

a. Compare the impact profile from the risk assessment to the impact profiles associated with each assurance level, as shown in table B–1 below. To determine the required assurance level, find the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment.

b. See OMB Memorandum 04–04 for detailed discussions on risk determination for authentication assurance levels based on impact to organizations.

c. Information about "Minimum Credential Strengths for Authentication to Information Systems" can be found in DoDI 8520.03.

Table B–1
Maximum potential impacts for each assurance level·

Assurance Level Impact Profiles				
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	Not applicable	Low	Mod	High
Unauthorized release of sensitive information	Not applicable	Low	Mod	High
Personal safety	Not applicable	Not applicable	Low	Mod High
Civil or criminal violations	Not applicable	Low	Mod	High

B–5. Authentication factors

a. The classic paradigm for authentication systems identifies three factors as the cornerstone of authentication—

(1) Something you know (for example, a password).

(2) Something you have (for example, an ID badge or a cryptographic key).

(3) Something you are (for example, a fingerprint or other biometric data).

b. Single-factor authentication refers to the use of one of the three factors (something you know, have, or are) for authentication when authenticating users to the system or environment.

c. MFA refers to the use of more than one of the factors listed in paragraph B–5*a*. The strength of authentication systems is largely determined by the number of factors incorporated by the system.

d. Implementations that use multi-factor are considered to be stronger than those that use only one factor; systems that incorporate all three factors are stronger than systems that only incorporate two of the factors.

B–6. Authentication walkthrough

a. E-authentication presents a technical challenge when this process involves the remote authentication of PEs or NPEs over a network. The authentication process may involve one or more ICAM entities such as: RAs, verifiers, relying parties (RPs) and CSPs.

b. Current government systems do not separate the functions of authentication and attribute providers. In some applications, these functions are provided by different parties. While a combined authentication and attribute provider model is used in this document, it does not preclude agencies from separating these functions.

c. This pamphlet provides guidelines to Army organizations to allow an individual person to remotely authenticate their identity to a Federal IT system. This pamphlet also provides guidelines for RAs, verifiers, RPs, and CSPs.

d. E-authentication begins with registration. The usual sequence for registration proceeds as follows:

(1) An applicant applies to an RA to become a user of a CSP.

(2) If approved, the user is issued a credential by the CSP which binds a token to an identifier (and possibly one or more attributes that the RA has verified). The token may be issued by the CSP, generated directly by the user, or provided by a third party.

(3) The CSP registers the token by creating a credential that binds the token to an identifier and possibly other attributes that the RA has verified. The token and credential may be used in subsequent authentication events.

e. The name specified in a credential may be a verified name or an unverified name. If the RA has determined that the name is officially associated with a real person and the user is the person who is entitled to use that identity, the name is considered a verified name. If the RA has not verified the user's name, or the name is known to differ from the official name, the name is considered a pseudonym.

f. The process used to verify a user's association with a name is called identity proofing and is performed by an RA that registers users with the CSP. Also, the party to be authenticated is called a claimant and the party verifying that identity is called a verifier. When a claimant successfully demonstrates possession and control of a token to a verifier through an authentication protocol, the verifier can verify that the claimant is the user named in the corresponding credential.

g. The verifier passes on an assertion about the identity of the user to the RP. That assertion includes identity information about a user, such as the user name, an identifier assigned at registration, or other user attributes that were verified in the registration process (subject to the policies of the CSP and the needs of the application).

h. Where the verifier is also the RP, the assertion may be implicit. The RP can use the authenticated information provided by the verifier to make access control or authorization decisions.

B–7. General identity validation for token attainment

a. The usual sequence of interactions is as follows:

(1) An applicant applies to an RA through a registration process.

(2) The RA identity proofs the applicant.

(3) On successful identity proofing, the RA sends the CSP a registration confirmation message.

(4) A secret token and a corresponding credential are established between the CSP and the new user.

(5) The CSP maintains the credential, its status, and the registration data collected for the lifetime of the credential (at a minimum). The user maintains their token.

b. When the user needs to authenticate to perform a transaction, they become a claimant to a verifier. The interactions are as follows:

(1) The claimant proves to the verifier that they possess and control the token through an authentication protocol.

(2) The verifier interacts with the CSP to validate the credential that binds the user's identity to their token.

(3) If the verifier is separate from the RP (application), the verifier provides an assertion about the user to the RP, who uses the information in the assertion to make an access control or authorization decision.

(4) An authenticated session is established between the user and the RP.

c. Users have a responsibility to maintain control of their token/CAC and comply with the responsibilities identified by the CSP.

B–8. Additional resources

Additional material relating to ICAM may be found on the DoD CYBER EXCHANGE PKI AND PKE website https://cyber.mil/pki-pke/.

Appendix C

Public Key Infrastructure Background

C–1. Introduction

Per DoDI 8520.03, all Army systems will use PKI credentials as the primary means of user ID and authentication. PKI credentials are used to support ID and authentication of individuals seeking to use NIPRNet and/or SIPRNet information resources. The CAC is issued to support NIPRNet access, while a separate SIPR token is used on the SIPRNet. In certain circumstances, a NIPRNet ASCL is provided instead of, or in addition to, the CAC for NIPRNet use.

C–2. What is Public Key Infrastructure?

a. PKI is defined as a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke PK certificates. In practical terms, it is a set of trust services that support digital ID/authentication, encryption, and signature operations. A PK certificate (hereafter "certificate") binds a PK held by an entity (such as person, organization, account, device, or site) to a set of information that identifies the entity associated with use of the corresponding private key. In most cases involving identity certificates, this entity is known as the "subject" or "subscriber" (user) of the certificate. Exceptions include devices (in which the user is usually the individual controlling the device) and certificates binding PKs to attributes other than identity, such as a role, a title, or specific privileged information. Different PKs are used for different functions: identity, encryption, and signature. The combination of a PK and its certificates form a digital credential. The infrastructure that attaches certificates to keys and tracks issuance and revocation of credentials is a CA.

b. An RP is someone who needs to use and rely upon the accuracy of the binding between the subject PK distributed via that certificate and the identity and/or other attributes of the subject contained in that certificate. An RP is the entity that grants access or other privilege based on identity, decrypts messages, or verifies digital signatures.

c. The degree to which an RP can trust the binding of credentials to their entity is the PKI assurance level. This depends on the practices followed by the CA in authenticating the subject; the CA's operating policy, procedures, and security controls; the scope of the user's responsibilities (for example, in protecting the private key); and the stated responsibilities and liability terms and conditions of the CA. These policies, practices, procedures, and controls are detailed in the certificate policy (CP) and the CPS or RPS that govern the CA and its supporting RA. Both SIPRNet (NSS) and NIPRNet ASCL credentials operate at the medium assurance level.

d. Figure C–1 illustrates a simplified credential issuance, use, and validation process. A user applies for a certificate with their PK at an RA. The latter confirms the user's identity to the CA which in turn issues the certificate. The user can then digitally sign a contract using their new certificate. Their identity is then checked by the contracting (relying) party with a validation authority which again receives information about issued certificates by the certification authority.

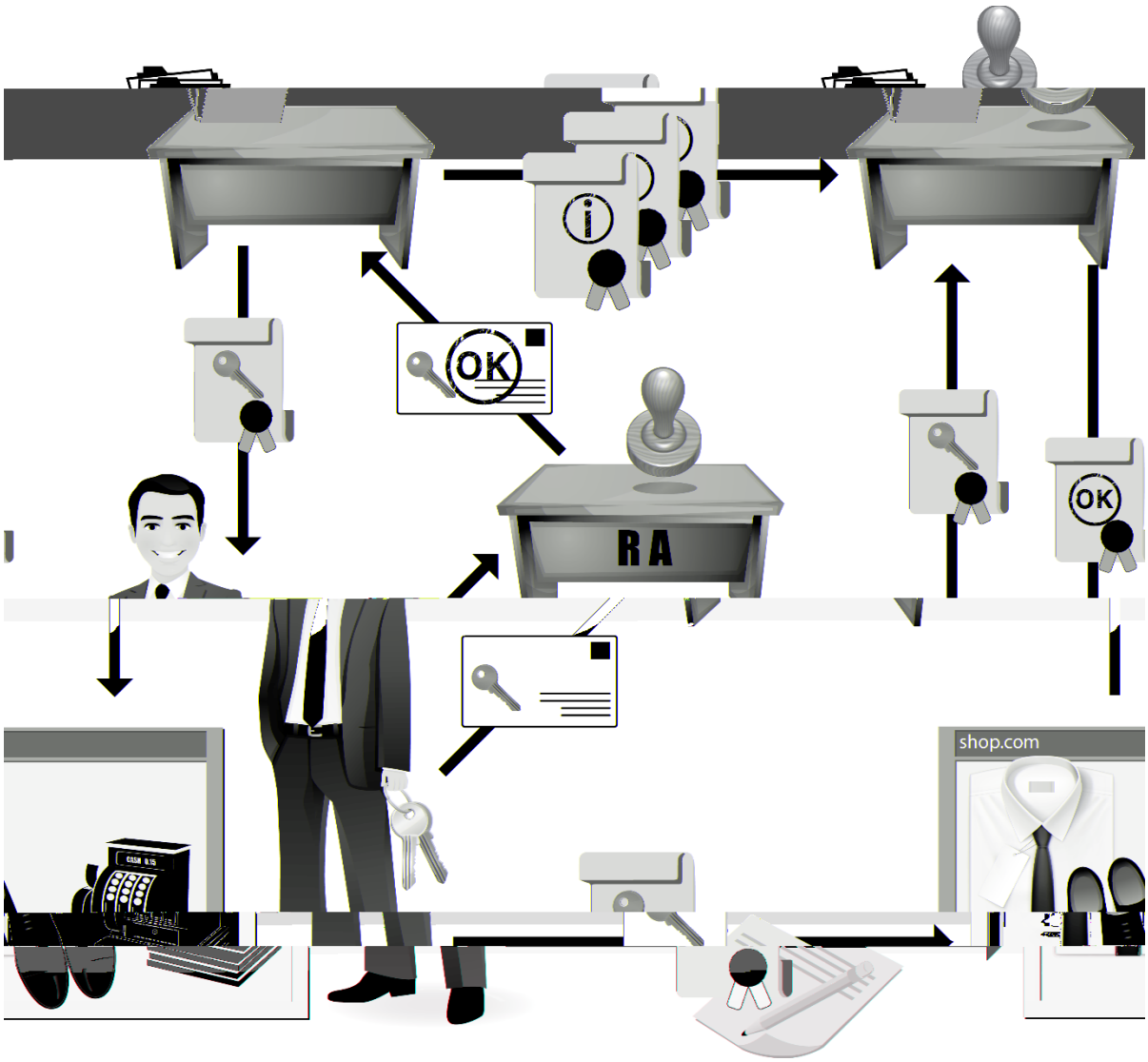

Figure C–1. Credential issuance, use, and validation process

C–3. Tokens and Public Key Enabling

a. Most DoD and SIPRNet credentials are issued on hardware devices called smart card tokens. (Some credentials are issued as software (files).)

b. For PKI to be effective as a security or operational tool, systems, applications, and devices must be capable of using the digital credentials. To do so, a system must have a means to read PKI tokens and effectively use the contained credentials. The tokens themselves require a reader, a means to enter a numeric PIN (to unlock the token), specialized software to communicate between token and system, and programs that can make use of the credentials themselves. Finally, the system must use AD for network logon and provide connectivity through the DoDIN to the PKI credential validation network (to ensure the credentials presented have not been revoked). The provision of all these components is called PKE.

C–4. Policy basis

a. CNSSP 25 establishes the requirement for all Federal departments and agencies to have a PKI to manage and support their secret and unclassified NSS. The CA for the NSS PKI that supports the SIPRNet is governed by CNSSI 1300. The associated RPS is the “National Security Systems Public Key Infrastructure DoD Registration Practice Statement,” Version 8, dated 19 December 2014.

b. DoDI 8520.02 requires the implementation of a DoD-wide PKI. The CA for the NIPRNet PKI supporting NIPRNet activities is based on the United States Department of Defense X.509 Certificate Policy and "DoD Medium Assurance Public Key Infrastructure RA/Local Registration Authority Certification Practice Statement," version 2 dated 20 May 2015.

c. Joint Task Force-Global Network Operations (JTF–GNO) Communications Tasking Order (CTO) 07–015, Revision 1 Public Key Infrastructure (PKI) Implementation, Phase 2 requires DoD components to implement Digital Signature policy.

C–5. Organization

a. For the issue of SIPRNet credentials and NIPRNet ASCL tokens, the Army operates its own PKI RA. The Army PKI RA provides 24/7 support and includes RA and LRA personnel.

(1) An RA is an official who interacts with the PKI credential management infrastructure to create, revoke, and manage credentials. An RA can also register new LRAs and terminate old ones; add, modify, and delete CA directory entries; and approve issuance of organizational code signing certificates. RAs are centralized in the Washington, DC area (mainly at Fort Belvoir, VA with a branch at the Pentagon). RAs require dedicated workstations that may only be used by their assigned RA and only for RA duties.

(2) An LRA is authorized by an RA to authenticate users, primarily for a particular group, office, or geographic location, to verify the identity and user information for each user under its purview. LRAs register users in their organizations with the PKI, perform face-to-face user identity authentication, load credentials to tokens, and issue them to users. LRAs are located worldwide at major commands and headquarters, based on workload and mission requirements. LRAs require dedicated workstations that may only be used by their assigned LRA.

b. RAs and LRAs are authorized to maintain a stock of blank tokens on hand to support their activities. LRAs can request that certificates be revoked, suspended, or restored based on circumstances covered in the CPS or RPS.

c. TAs and ETAs are located at installations and units to perform activities that require direct, in-person interaction with PKI users. TA/ETA is an "additional duty" role.

d. The RAs supporting Army and LRAs in the Washington, DC area are under NETCOM. NETCOM provides day-to-day operational oversight and balances work based on mission needs and known requirements. LRAs outside the DC area are the responsibility of their parent commands.

e. RA operations are subject to an annual DISA audit. LRAs are inspected/audited by DCS, G–6 personnel annually. All RAs and LRAs must comply with all provisions and requirements of the policies in paragraph C–4.

f. Each RA or LRA site must have an ISSO and system administrator assigned to support the PKI workstations.

C–6. Credentials

a. PKI credentials are available for both NSS and unclassified DoD use and come in either file form (password-protected software certificates or "soft certs") or stored on a hardware token locked by a PIN. PKI credentials may also differ in the types of credentials contained. Normally, all three (identity, encryption, and signature) keys with their associated certificates are provided. However, some credentials do not require all three. For example, code signing certificates do not include encryption keys.

b. The value of PKI lies in the strict binding between the credentials and the subscriber (the person or entity whose name is associated with the credential). The RP, who acts on the assurance the PKI provides, depends on this binding. Therefore, it is critical that only the subscriber (or its PKI sponsor) is the only one who has access to both the credential and the PIN/password needed to access it. Thus, during issue these components are delivered by different persons who give their portions to the user separately. Any compromise of this exclusive access is a security violation and must be reported.

C–7. Additional resources

Additional material relating to PKI may be found on the DoD CYBER EXCHANGE PKI and PKE website https://cyber.mil/pki-pke/.

Appendix D

Exception Guidance and Checklists

D–1. Department of Defense policy-based exceptions

a. Exemptions based on DoD policy expressed in DoDI 8520.02 and/or 8520.03 do not require formal review from Army CIO, DCS, G–6, or from DoD.

b. For RMF security control assessment purposes, the non-use of PKI based ID and authentication must be documented. Documentation must—

(1) Cite the policy basis for tailoring out PKI controls.

(2) Provide an explanation of how the system meets the criteria of the exemption.

D–2. General exception guidance

a. If DoD policy does not exempt a system from implementing PKI, the organization must either PKE the system and implement PKI or obtain an exception for the system. This includes systems that are technically incapable of implementing PKI based on configuration, topology, or data flow, or have operational conditions that render PKI operations disruptive to the mission. Additionally, some systems may incur additional, unacceptable risk by implementing PKI due to the requirement to connect to the DoDIN for credential validation. Final exception approval comes from DoD once the Army CIO endorses the exception request.

b. When requesting a recurring exception, the organization is stating that—

(1) The organization cannot comply with a mandated policy.

(2) The organization needs the system to accomplish its mission.

(3) At the end of the time period specified in the request, the organization will reevaluate the system to validate the ongoing requirement for the system and its continued inability to comply with policy.

c. When requesting a one-time exception, the organization is stating that—

(1) The organization cannot comply with a mandated policy.

(2) The organization needs time to become compliant with the policy.

(3) At the end of the time period specified in the request, the organization will be compliant with policy.

d. Requesting an exception to any regulation should not be regarded as a permanent substitution for the implementation of the policies and procedures called for by regulation. Army CIO exceptions are granted for up to one year. Renewals may be granted upon resubmission of request and approval by the cognizant authority exception review process. Renewal implies that the organization has conducted a review to ensure that changes to the system, its environment, or the state of technology that would allow the implementation of PKI.

e. Exception requests need not be submitted for systems with a policy-based exemption. Systems that fall in an exempt category per DoD or Army policy (for example, stand-alone networks) will have a formal system architecture and data flows that validate their exempt status sufficient to document their status for ATO or other purposes. The ISSO, with the support of the SO must tailor the security controls for the system, document these controls in the System Security Plan, and have them approved by the AO.

f. The point of contact for exception guidance is the Policy and Risk Governance Division, CIO, 5850 23rd Street, Building 220, Fort Belvoir, VA 22060.

g. Do not wait until the last minute to submit a request as it can take more than 60 days to process, and it may be disapproved or returned as insufficient.

D–3. Public Key Infrastructure exception request checklists

a. All requests for exceptions must complete the system checklist.

b. Requests for exceptions for network tools and other software must also complete the tools checklist.

c. Requests for exceptions for users must complete both the system and user checklists.

d. Exceptions are categorized into one of three types, linked to Joint Task Force-Global Network Operations (JTF–GNO) Communications Tasking Order (CTO) 07–015, Revision 1 Public Key Infrastructure (PKI) Implementation, Phase 2—

(1) Type 1 is part of Task 10.

(2) Type 2 is part of Task 2.

(3) Type 3 is also part of Task 10.

e. Stand-alone ISs, top secret collateral systems, and special access programs are exempt from policy (per DoDI 8520.03) and do not require an exception for PKE. However, completion of systems checklist is recommended to help ensure all aspects of system security are adequately addressed.

D–4. System (Type 1) exception request checklist

a. This checklist is required for all system (Type 1) exception requests. This requests an exception to User Based Enforcement of system requirements due to—

(1) System constraints (for example, low bandwidth).

(2) Technology not available (for example, use of a legacy system).

(3) User populations without PKI credentials.

(4) Mission requirement (for example, access to multiple systems).

b. A system (Type 1) exception is required if any of the following questions in paragraphs D–4*c*, D–4*d*, or D–4*e* are answered in the affirmative for the site.

c. Exception questions are as follows:

(1) Does the exception request explain how complying with policy will adversely affect the organization's mission?

(2) Does the exception request describe how the risk of using usernames and passwords exclusively will be mitigated?

(3) Is the exception request memorandum signed by the AO?

(4) Does the exception request include a POA&M that provides sufficient detail and full justification backed up with detailed data on how the system will be modified to comply with PKI requirements (a PKI transition plan)?

(5) Does the exception request include a POA&M that provides sufficient detail and full justification backed up with detailed factual data on how the system will transition from Army Knowledge Online (AKO) Single Sign-On (SSO) (an AKO SSO Transition Plan)?

(6) Is system incapable of implementing PKI?

(7) Are there any technical limitations that prevent the implementation of PKI?

d. System information questions are as follows:

(1) Does the system use Enterprise Access Management Service-Army?

(2) Does the system use AKO Lightweight Directory Access Protocol (LDAP)?

(3) Is the system accessed by a user population that cannot obtain DoD approved PKI?

Note. System must still be PK enabled if it has users that do possess PKI credentials, and these users are required to authenticate with PKI.

(4) Has full logical layout for diagram/topology (Network/Data Flow Diagrams) been included with exception request?

(5) Is this a legacy system?

(6) Is this a stand-alone system?

(7) Is this a self-service portal?

(8) Does system have a self-service component (for example, training records)?

(9) What is the sensitivity level of data being assessed?

Note. See 5 USC 552 or DoDI 8520.03 for guidance.

(10) Does the system contain FOUO/sensitive data?

Note. If the system does not contain any FOUO/sensitive data a signed memorandum from the AO declaring the system is free of FOUO/sensitive data must be submitted with the exception request?

(11) Has FOUO/sensitive data been separated from non-FOUO data within the system?

Note. If yes, a signed memorandum from the AO stating that FOUO/sensitive data has been separated from non-FOUO data must be submitted with the exception request.

(12) Does the system contain PII and/or PHI that is accessed only by the individual identified in the data?

Note. If yes, a signed memorandum the AO stating PII, and PHI data is only accessed by the individual identified in the data must be submitted with the exception requests.

(13) Does the system contain PII and/or PHI that is being accessed by multiple users?

Note. PHI systems are not authorized for UN/PW authentication.

(14) Does the system require access from employee-owned equipment?

e. User information questions are as follows:

(1) Are non-CAC eligible users eligible for a DS Logon account?

(2) Are non-CAC eligible users eligible for an ECA certificate?

D–5. Tools (Type 2) exception request checklist

a. This checklist is required for all tools (Type 2) exception requests. This requests an exception to PKE requirements because network software, tools, or functions are unable to implement PKI authentication.

b. Tools that may qualify for a Type 2 exception include—

(1) REM® Security Management Console.

(2) Retina Network Security Scanner.

(3) Network Manager (NetMan).

c. A tools (Type 2) exception is required if any of the following criteria is true:

(1) Is there a newer version tool available that incorporates PKI?

(2) Are there plans to upgrade to the latest version tool?

(3) Has a detailed timeline been developed to upgrade the tool?

D–6. Users (Type 3) exception request checklist

a. This checklist is required for all users (Type 2) exception requests. This requests an exception to user PKI-only authentication requirement because the user population does not have a PKI credential (for example, retirees, military dependents, Individual Ready Reserve, and so on).

b. Requests for this type of exception must include ID and description of what credentials non-CAC eligible individuals will use because there are external PKIs approved for use in the DoD.

c. A users (Type 3) exception is required if any of the following criteria is true:

(1) Are non-CAC eligible users eligible for a DS Logon account?

(2) Are non-CAC eligible users eligible for an ECA certificate?

(3) Are users required to monitor multiple systems simultaneously?

Note. If required, explain how function is currently performed.

(4) Does user population include system administrators?

(5) Are system administrators using PKI credentials to access system?

Note. If not, provide full details on access method used by system administrators.

Appendix E

Trust of External Public Key Infrastructures

E–1. Department of Defense policy–external Public Key Infrastructures

a. On 22 July 2008, the DoD CIO issued memorandum "Approval of External Public Key Infrastructures." This memorandum implements policy issued in DoDI 8520.02 requiring the DoD to approve DoD RP use of external PKIs. The memorandum approves four external PKIs for use with DoD ISs—

(1) DoD ECA PKI approved certificates for industry partners and other external entities and organizations.

(2) U.S. Federal agency PKIs cross-certified with the FBCA, commonly referred to as the "Federal Bridge."

(3) Nonfederal agency PKIs cross-certified with the FBCA or PKIs from other PKI bridges that are cross-certified with the FBCA.

(4) Foreign, allied, coalition partners, or other PKIs that are not covered in the three classes above.

b. DoD gateways such as the SIPR REL DMZ are governed by their own standard operating procedures.

E–2. Personal identity verification–interoperable credentials

a. On 5 October 2010, the DoD CIO issued the memorandum "Department of Defense Acceptance and Use of PIV–I Credentials." This memorandum provides guidance and recommends that, in those cases where DoD relying parties, senior commanders, and facility coordinators determine that granting access is appropriate and that appropriate vetting requirements are met, they begin accepting and using DoD approved PIV–I credentials for authentication and access.

b. There are two actions for which PIV–I must be used—

(1) Authentication directly to DoD networks (for example, NIPRNet, SIPRNet).

(2) Physical access control systems where electronic ID systems are not in place.

E–3. Implementation choices

Deployments of disparate Federal/DoD partner PKIs and the introduction of the FBCA have led to two implementation choices for enabling trust for external PKI credentials—

a. Direct trust. To achieve a direct trust relationship between two PKIs, one party establishes a trust relationship with an external root CA. This means the organization can directly verify certificates issued by that CA. As an example, the ECA is a separate PKI from the NIPRNet PKI. Adding ECA root and subordinate root CA certificates to one's NIPRNet PK application or to a computer's PKI trust store creates a direct trust to ECA PKI.

Note. Including the trust anchor and the subordinate CA certificates in one's NIPRNet PK application or one's computer's PKI trust store still requires the RP to validate (that is, ensure that the certificate(s) is(are) still valid), by verifying CRLs and/or OCSP responses.

b. Cross certification trust. To achieve interoperability between two PKIs, a trust path must be established by issuing a "cross" certification to previously unrelated peer root CAs as a mechanism to interconnect them for secure communications. NIPRNet applications accessed using a certificate from a PKI cross-certified with the Federal Bridge follows an attribute in the external user's certificate to establish a trust path to the DoD Interoperability Root installed on the application. The trust path is built through the Authority Information Access attribute and validates the certificate chain in real time.

Note. Having the trust anchor and the subordinate CA certificates in one's NIPRNet PK application or one's computer PKI trust store still requires the RP to validate (that is, ensure that the certificate(s) is(are) still valid), by verifying CRLs and/or OCSP responses.

E–4. Cross certification

Cross certification architectures or models-interoperability between two separate PKIs can follow one of the following approaches:

a. Bilateral cross certification. Mutual exchange of certificates between two peer PKIs, typically at the level of a root CA. Using this model there is a single policy mapping: source PKI remote PKI.

b. Bridge cross certification. A potentially unlimited number of parties perform a bilateral cross certification between their root CA and a bridge CA. The two PKIs trust one another because each one trusts the bridge (that is, transitive trust). Using this model there are two serial policy mappings: source PKI bridge remote PKI.

c. Extended bilateral cross certification. Cross certification relationship (unilateral) is with the interoperability root, which in turn is cross-certified with a trust anchor in the remote PKI (this could be a bilateral cross certification with a bridge, as done between the DoD and the Federal Bridge). The transitive trust paradigm (as with bridged cross certification) applies, but with a single policy mapping (as with bilateral cross certification): source PKI remote PKI. The interoperability root allows splitting between all users and the sub-set who need to be involved in interoperability.

E–5. Federal Bridge trust model

a. The Federal Bridge architecture follows a non-hierarchical structure with the FBCA as its hub. The Federal Bridge interoperability landscape provides a representative view of the trust relationships established between various Federal and trusted nonfederal PKIs.

b. Figure E–1 provides a conceptual overview of the PKI trust model used in the DoD environment using the FBCA. It shows the various chains of trust (current and proposed) that have their roots in the FBCA.

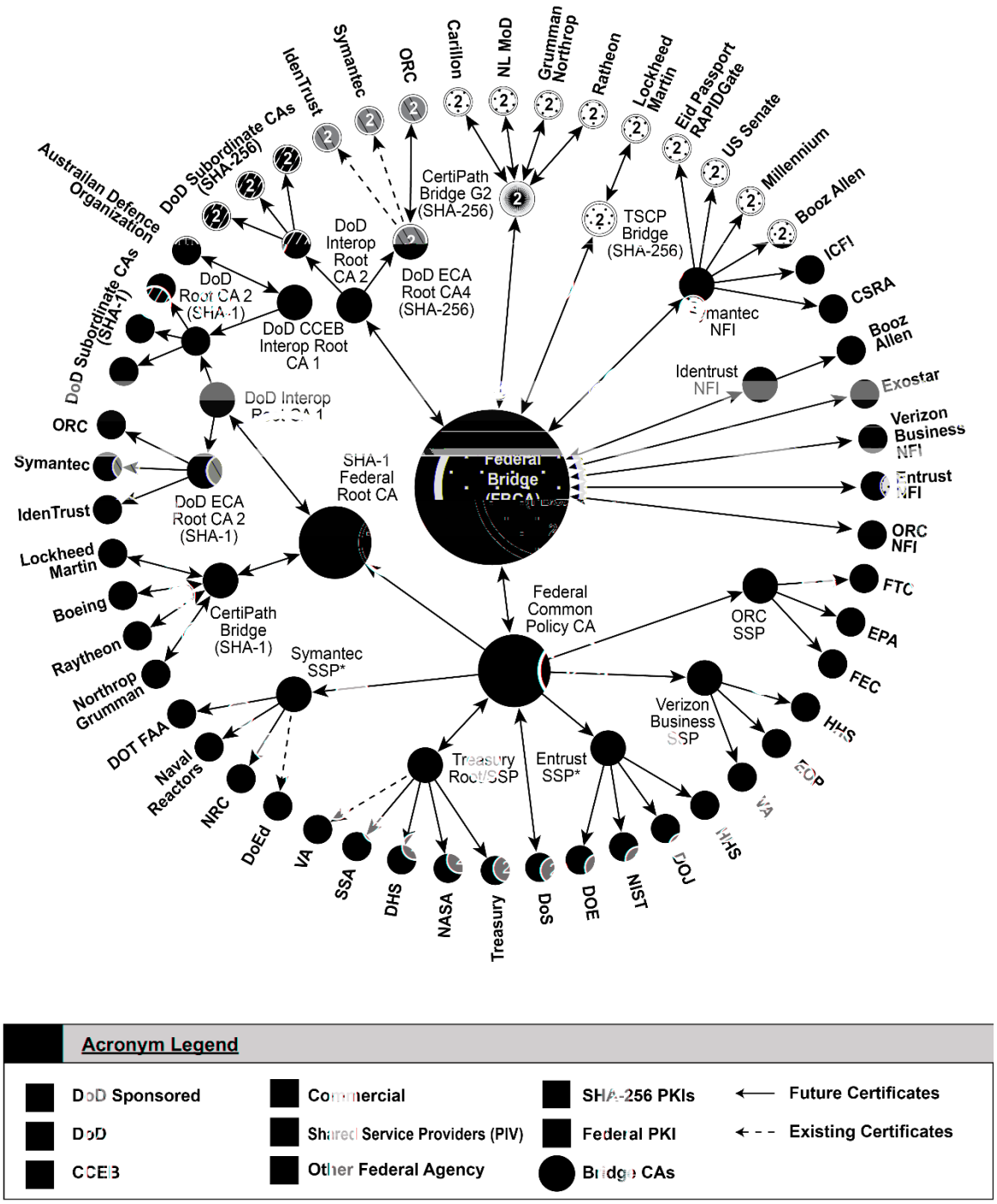

Figure E–1. Conceptual overview of Federal Public Key Infrastructure trust relationships as of March 2013

E–6. Determining partner approval status

Approval status of partners fall into one of the following categories/groups (adapted from DoD CIO Memorandum):

a. Department of Defense external certification authority Public Key Infrastructure. Authorized certificates issued by the approved DoD ECA vendors include DoD ECA Medium Assurance, DoD ECA Medium Token Assurance, and DoD Medium Hardware Assurance. Specifics of the DoD ECA program may be found at the website: https://cyber.mil/pki-pke/eca. The ECA implementation establishes a "direct trust" relationship between DoD and partner entities—

(1) Currently there are three vendors approved as authorized ECA vendors—

(a) Operational Research Consultants, Inc. (https://www.eca.orc.com).

(b) BROADCOM. (https://www.broadcom.com/site-search?q=eca).

(c) IdenTrust Inc. (https://www.identrust.com/certificates/dod-eca-programs).

(2) Industry partners and other external entities and organizations conducting secure communications with DoD and Army partners may obtain authorized certificates from either of these approved ECA venders. Adding the ECA Root and subordinate root CA certificates to one's DoD PK enabled applications or to one's computer's PKI trust store allows one to trust ECA PKI individual certificates to establish a direct trust relationship.

b. U.S. Federal agency Public Key Infrastructure.

(1) For Federal agencies' PKIs to be approved for interoperability with the DoD NIPRNet, the PKIs must have successfully been tested by the Joint Interoperability Test Command (JITC) Laboratory and either of the following conditions must be met:

(a) The certificate was issued by a PKI that is operated by a U.S. Federal agency and is cross-certified with the Federal Bridge at Medium Hardware Assurance or High Assurance. A listing of Federal agency PKIs that are cross-certified with the FBCA is available at the following website: https://www.idmanagement.gov/buy/trust-services/#trust-audit-services.

(b) The certificate was issued by a certified PKI shared service provider (SSP) operating under the X.509 Certificate Policy for the Common Policy Framework and asserts one of three specific object identifiers (OIDs): id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-High. A listing of certified SSPs is available at the following website: https://www.idmanagement.gov/buy/trust-services/.

(c) Federal agencies approved for interoperation with DoD are listed on the IASE website https://cyber.mil/pki-pke/interoperability.

(2) The DoD PKE team will collaborate with DoD SOs to initiate initial interoperability testing, establish trust paths, and use of DoD approved PKIs in their logical access control procedures. The DISA PKE team will establish a trusted DoD repository of all DoD approved root certification authority certificates that can be used by DoD relying parties to establish trust relationships.

(3) The External PKI Interoperability Working Group (EIWG) will review listed requirements and the results of JITC testing. To begin cross certification process, contact—

(a) Approval of external PKIs: EIWG via email at externalpki.interoperability@osd.mil.

(b) Technical questions: DoD PKE team via email at pke_support@disa.mil.

(c) DoD External Interoperability Plan at website https://dl.cyber.mil/pki-pke/pdf/unclass-fouo-dod_external_interoperability_plan_26aug2010.pdf.

c. Nonfederal agency Public Key Infrastructure.

(1) A nonfederal agency entity must have purchased certificates from one of the three approved ECA vendors, have PIV–I credential from one of the nonfederal issuers (NFIs) SSPs, or have been approved through the FBCA cross certification process.

(2) For the FBCA process, all of the following conditions must be met:

(a) The certificate was issued by a PKI that is cross-certified with the FBCA at the Medium Hardware Level of Assurance.

(b) The PKI has a DoD sponsor that has established a business or mission need for secure communications with the nonfederal agency entity.

(c) The JITC has successfully completed reasonable interoperability testing of the PKI to ensure that certificates are technically interoperable with DoD systems, including web servers and email clients, and that certificate revocation information can be obtained by DoD systems.

(3) For the PIV–I process, all of the following conditions must be met:

(a) The PIV–I certificate was issued by an NFI SSP credential providers that have been approved in accordance with the DoD External Interoperability Plan.

(b) The PKI has a DoD sponsor that has established a business or mission need for secure communications with the nonfederal agency entity.

(c) The JITC has successfully completed reasonable interoperability testing of the PKI to ensure that certificates are technically interoperable with DoD systems, including web servers and email clients, and that certificate revocation information can be obtained by DoD systems.

(4) Nonfederal agencies that meet these conditions and are approved for interoperation with DoD are listed on the DoD CYBER EXCHANGE website https://cyber.mil/pki-pke/interoperability/.

(5) The IASE website for external and Federal PKI Interoperability lists the DoD approved external PKIs and provides links to an information page for each commercial entity that has been approved. This information page generally contains the "Memorandum of Agreement" executed between the commercial entity and the DoD CIO acting as the DoD Policy Management Authority, summary of FBCA test results, certificate files, and implementation notes.

(6) The DoD PKE team will collaborate with nonfederal agencies to initiate initial interoperability testing, establish of trust paths, and use DoD approved PKIs in their logical access control procedures. The DISA PKE team will establish a trusted DoD repository of all DoD approved root certification authority certificates that can be used by DoD relying parties to establish specific relationships.

(7) The EIWG will review listed requirements and the results of JITC testing. To begin cross certification process, contact—

(a) Approval of external PKIs: EIWG via email at externalpki.interoperability@osd.mil.

(b) Technical questions: DoD PKE team via email at pke_support@disa.mil.

(c) DoD External Interoperability Plan at website https://dl.cyber.mil/pki-pke/pdf/unclass-fouo-dod_external_interoperability_plan_26aug2010.pdf.

d. Other. For foreign, allied, coalition partner PKIs, or other PKIs not covered in paragraphs E–6*a* through E–6*c*, all of the following conditions must be met:

(1) A DoD service or agency system or application owner has identified that they require interoperability with the PKI and has established a business case or mission need to authenticate external PKI certificates.

(2) The foreign, allied, coalition policy, or other PKI CP has been mapped to the DoD PKI in accordance with the DoD cross certification vetting process. The DoD Certificate Policy Management Working Group (CPMWG) or its designated authority has not identified critical risks to the EIWG that would prevent certificate validation or authentication at all required levels of assurance.

(3) JITC has successfully completed reasonable interoperability testing of the foreign, allied, coalition partner, or other PKI to ensure that certificates are technically interoperable with DoD systems, including web servers and email clients, and that certificate revocation information can be obtained by DoD systems.

(4) Approved PKIs in this category will be listed on the DoD website https://cyber.mil/pki-pke/interoperability/.

(5) The EIWG will review the CP mapping performed by the CPMWG and the results of JITC testing.

(6) To begin cross certification process, contact—

(a) Approval of external PKIs: EIWG via email at externalpki.interoperability@osd.mil.

(b) Technical questions: DoD PKE team via email at pke_support@disa.mil.

(c) DoD External Interoperability Plans at website https://dl.cyber.mil/pki-pke/pdf/unclass-fouo-dod_external_interoperability_plan_26aug2010.pdf.

(7) DoD has established the Combined Communications Electronics Board (CCEB) Root CA under a separate process from that specified in the External Interoperability Plan. The CCEB Root is designed for interoperability with CCEB partners (that is, allied). The CCEB Root is currently operating using a separate root CA from the DoD root and a separately negotiated memorandum of agreement. The CCEB Root is one-way cross-certified with the DoD and has issued cross certificates to DoD Root 1 (legacy 1024-bit RSA key size) and DoD Root 2 (2048-bit RSA key size). The CCEB Root is two-way cross-certified with the other CCEB partners.

E–7. Federal and nonfederal interoperability guidelines

Administrators are encouraged to review the risks, address the concerns, and implement best practice guidelines.

a. Personal identity verification and personal identity verification–interoperable. PIV and PIV–I credential acceptance requires the Army infrastructure transition to support secure hash algorithm (SHA) bit length-256 (SHA–256). The current infrastructure relies on SHA bit length 128 (SHA–1) while the Federal agencies issue SHA–256 based certificates.

b. Department of Defense Public Key Enabling websites. According to DoDI 8520.2, DoD private web servers providing access to DoD sensitive information, except those protecting access to personal information by information-privileged individuals, must be PK enabled to rely on certificates issued by DoD PKIs for client authentication. ISs requiring PKE that include users who are DoD partners not eligible for DoD PKI certificates must support certificates issued by DoD approved external PKIs. DoD PKI eligible users are active duty military personnel, members of the Selected Reserve, DoD Civilian employees, and authorized contractor personnel working on site at DoD facilities using DoD network and email services. Web servers that require PKE and have users who are not eligible for certificates issued by the DoD PKI must be configured to validate certificates issued by ECAs.

(1) *General Public Key Enabling guidelines.* To allow access to certificate holders from external PKIs to a secure website, first verify that the site meets the following best practices:

(a) Supports management of the site trust store; the trust store or Certificate Trust List should only contain DoD approved CA certificates.

(b) Supports Secure Socket Layer/Transport Layer Security.

(c) Requires and accepts authorized client certificates.

(d) Supports validation of client certificates in accordance with IETF RFC 5280.

(e) Supports protection of sensitive content through attribute-based or risk-adaptive access control protocols.

(2) *Certificate policy object identifiers filtering.* Determine if certificate holders from external PKI applications are capable of OID filtering. The CP mapping feature contained in the cross certificates are not available in a direct trust approach. DoD applications and systems using a direct trust model must recognize and filter out unapproved CP OIDs of other domains to ensure that lower assurance certificates are not allowed access to their resources.

(3) *Access control.* Requiring client certificates for access rights to a website and protected data is a key component to increasing the security posture of the DoD. Access control enables a resource to be restricted based on assigned access rights and requires an explicit decision on an individual basis rather than blanket acceptance based on a credential.

(4) *Verification of external Public Key Infrastructure.* The website administrator should verify and review the JITC report for the external PKI prior to allowing access to their site. The external PKI should be DoD approved for interoperation and specific details from the report should be noted—

(a) Certificate and CRL repository locations points of contact for the PKI.

(b) Procedures for revocation requests.

(c) CA serial numbers and thumbprint should be verified prior to installation.

(5) *Method of interoperation.* The site administrator and data owner should discuss trust method options and make an educated decision that weighs the associated risks against the potential gains in interoperability and ease-of-use of the site. Site administrators are to review specific instructions on how to implement cross certification path processing. Instructions are available in the DoD PKI Partner PKI Interoperability Test Plan. When configuring trust for external PKI certificates in a production system, administrators will test each application's ability to process the certificates and CRL repositories.

(6) *System verification.* After the system has been configured to allow access to designated users with valid certificates issued from the external PKIs, the system administrator should—

(a) Verify that external PKI users can access the site.

(b) Verify the system is configured and capable to deny access to users with revoked external PKI certificates.

(c) Verify that access controls perform properly with external PKI users - that registration and usage of community of interest sites are possible with these partner certificates.

(d) Verify that the valid certificate holders from the external PKI who are not registered users cannot access the designated resources.

(e) Verify that valid certificate holders from the external PKI who are registered, or authorized users are only allowed to access resources designated to them.

E–8. Signed and encrypted email

DoD relying parties that exchange digitally signed or encrypted email with certificate holders from external PKIs are required to take certain precautions as follows:

a. Signed email. DoD email clients are configured to automatically sign all outgoing email with DoD PKI credentials. However, incoming email may not be signed with DoD credentials and may require manual validation. To validate a signed certificate in Microsoft Outlook, open the email in question and look for a ribbon symbol above the upper right corner of the email message test area. If no ribbon symbol is present, the email is unsigned. If present, click the ribbon symbol to display the signature validity data in a separate window. If the digital signature validity window indicates that the signature is valid and trusted, the identity of its source may be trusted. If not valid, the identity of the source is questionable.

b. Encrypted email. DoD email clients are configured to optionally encrypt outgoing email with DoD PKI credentials. Encryption of incoming email to DoD systems requires the sender to have access to the recipient's DoD public encryption key. Encrypted email should only be opened from a known and trusted source as encryption alone provides no assurance of the validity of safety of the content. (It is possible for malware to be embedded in encrypted email allowing it to pass through email scanning and protection steps to recipient. An attachment included with any email should not be invoked directly; it should be saved to disk first to enable system virus scanners to check for viruses.)

Appendix F

Lost/Stolen Token Report Format

F–1. General

Any suspected loss or theft of any PKI token must be reported to a supporting TA or ETA using the memorandum format provided in figure F–1.

F–2. Discretion of use

Additional material may be added at the discretion of the subscriber/user or the commander. Appropriate text to be selected for SIPRNet or NIPRNet is indicated as [SIPRNet | NIPRNet].

Figure F–1. Sample memorandum for reporting lost/stolen token

Appendix G

Token Request/Issuance Process

G–1. General

The DoD implements the DoD PKI, DoD portion of the NSS PKI, and the DoD Coalition PKI to satisfy operational needs and requirements. These PKIs are operated by the DoD PKI Program Management Office and issue certificates to all subscribers to support DoD missions and business operations. Figure G–1 provides an overview of the request/issuance process.

G–2. Secure Internet Protocol Router Network users

The DoD-operated portion of the NSS PKI issues certificates to DoD SIPRNet users for authentication and logon to SIPRNet resources.

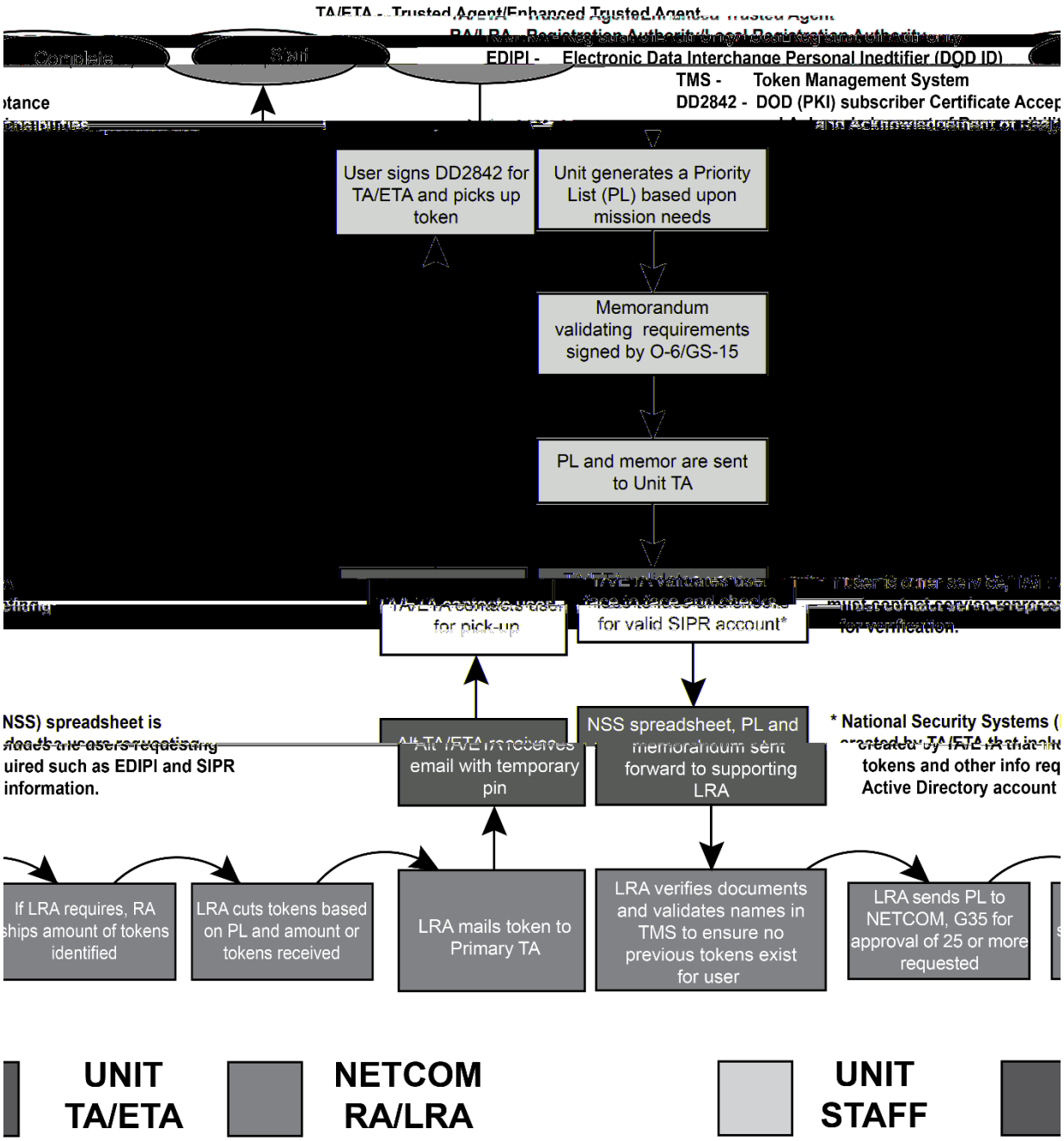

Figure G–1. Token request/issuance process

Appendix H

Example Registration Officer Nomination Memoranda

H–1. General

Figure H–1 and figure H–2 are templates for the memoranda used to designate RAs and LRAs.

H–2. Guidance

All memoranda must be prepared on organizational letterhead and may include multiple individuals. Separate memoranda are required for RAs and LRAs.

DEPARTMENT OF THE ARMY
ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

OFFICE SYMBOL [Date]

MEMORANDUM FOR Defense Information Systems Agency (DOD PKI PMA, IA4)
P.O. Box 549 Ft. Meade, MD 20755-0549

SUBJECT: Designation of NIPRNet Registration Authority (RA)

1. References:

a. United States Department of Defense X.509 Certificate Policy, Version 10.5, 23 January 2013.

b. DOD RA /LRA CPS, Version 1, 25 July 2012.

c. CNSS Instruction No. 1300 NSS PKI X.509 Certificate Policy 18 September 2013, ver. 1.2.3.

d. NSS PKI Registration Practice Statement (RPS) 22 May 2013, ver. 6.

2. In accordance with the references above, the following individuals are hereby designated as Registration Authorities (RAs); they are charged with executing the responsibility of an RA.

Name: [Last, First, MI]

ADP Category: [Civilian, Contractor, Military]

Grade/Rank: [Civilian, Contractor, Military]

Unique Identification Number [DOD Identification Number located back of CAC]

Email: [Insert email address]

Commercial Phone: [Insert commercial phone number]

Defense Switched Network (DSN) Phone: [Insert DSN number]

ailing address]

h designee.)

Mailing Address: [Insert ma

(Repeat information for eac

of the requirements of Section 5.3.1 of reference (a).

3. The above individuals meet all

an individual is relieved of duties or leaves the Service/Agency, whichever

4. This authority is rescinded whe
occurs first.

tance is required, the point of contact for this action is as follows:

5. If additional information or assis
(Insert POC and phone number).

[Insert Signature]

Army CIO/G-6

Figure H–1. Sample Registration Authority nomination memorandum

DEPARTMENT OF THE ARMY
ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

OFFICE SYMBOL [Date]

MEMORANDUM FOR United States Army Registration Authority

SUBJECT: Designation of Local Registration Authority (LRA)

1. References:

a. United States Department of Defense X.509 Certificate Policy, Version 10.5, 23 January 2013.

b. DOD RA /LRA CPS, Version 1, 25 July 2012.

d. NSS PKI Registration Practice Statement (RPS) 22 May 2015, ver. 3.

tration

2. In accordance with the references above, the following individuals are hereby designated as Local Regis Authorities (LRAs); they are charged with executing the responsibility of an LRA.

Name: [Last, First, MI]

ADP Category: [Civilian, Contractor, or Military]

Grade/Rank: [Contractor, Civilian, Soldier]

Unique Identification Number [DOD Identification Number located back of CAC]

Email: [Insert email address]

Commercial Phone: [Insert commercial phone number]

Defense Switched Network (DSN) Phone: [Insert DSN phone number]

Mailing Address: [Insert mailing address]

(Repeat information for each designee.)

ference (a).

3. The above individuals meet all of the requirements of Section 5.3.1 of re

4. This authority is rescinded when an individual is relieved of duties or lea occurs first.

5. If additional information or assistance is required, the point [Insert POC and phone number]

[Signature]
Army CIO/G-6

Figure H–2. Sample Local Registration Authority nomination memorandum

Appendix I

Army Identity Attribute Standard Change Request Template

I–1. Purpose

The intent of this document is to standardize all “DoD Enterprise and Army Specific Attributes” across the strategic and tactical environments. Army Specific Attributes are defined as all attributes used by Army Programs of Record (PORs), systems, and applications for information sharing, collaboration, access control decisions, and data replication in the strategic and tactical environment. All fields in the “Source” and “Attribute Specification” sections are mandatory.

I–2. Instructions

The current attributes in this document are just “DRAFT.” Therefore, any attribute that is not present can be added, and any attribute that is present can be modified or deleted. See table I–1.

Table I–1
Attribute template-

Source	
Authoritative Provider	Identifies the authoritative provider for this attribute. The Authoritative Provider is the store that is trusted with hosting a given attribute.
Authoritative Source	Identifies the Authoritative Source of the attribute. The Authoritative Source is the data store that is trusted with generating an accurate value for a given attribute.
Attribute Source	For example, Active Directory, Exchange, manually by Admin, PM, and so forth.
Attribute Specification	
Fieldname	This element identifies the field name in the DISS feed where the data for this attribute is stored.
Definition	Defines the attribute.
Display Type	Identifies the data type characteristics of the attribute.
Display Length	Identifies the available field length of the attribute.
Value	Identifies if the attribute has a single value or allows multiple values.
LDAP	
Reference	Provides the attribute’s LDAP reference and definition.
Name	Provides the attribute’s descriptive name.
Backus-Naur form	Attribute LDAP definitions in Backus-Naur Form of Attribute Type Description as provided in RFC–2252.
Business Rules/Workflow Notes	
	Rules the identity store follows for the attribute.

I–3. Authoritative Data Sources

Authoritative data sources can have one of the following values in table I–2.

Table I–2
Data source template-

Value	Meaning
Component HR Systems	The data element was created within an approved HR system, usually during on-boarding.
DMDC	Defense Manpower Data Center is the creator of the data element.
Provisioning Admin Interface	The data element is created by an approved Army administrator for these functional attributes.

Table I–2
Data source template—Continued

Enterprise Email/Component Email Systems	The data element is related to email and is created by an email system. If the user has migrated to Enterprise Email, then EE is the source of the data. If not, then the data comes from the Exchange organization that the user belongs to.
MilConnect/User	The user is responsible for updating the attribute value whenever it changes. The milConnect Portal is used to do so.

Glossary of Terms

Access
Ability to make use of any IS resource. (See CNSSI 4009.) Also, ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. (See AR 25–2.)

Applicant
A party undergoing the processes of registration and identity proofing (see NIST SP 800–63A). Also, a subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. (See American Bar Association Digital Signature Guidelines, footnote 32.)

Assertion
A statement from a verifier to an RP that contains identity information about a subscriber. Assertions may also contain verified attributes. (See NIST SP 800–63C.)

Assurance level
A characteristic associated with a certificate that is an assertion by a CA of the degree of confidence that others may reasonably place in the binding of a PK to the identity and privileges asserted in the certificate. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a certificate management system. Assurance levels are defined in applicable PKI certificate policies. (See DoDI 8520.03.)

Assurance level 1
Credentials that require no identity proofing. At this level, the authentication mechanism or protocol provides little or no assurance that the claimant is accessing the protected transaction or data. Level 1 identity credentials are not approved for use in DoD ISs. (See DoDI 8520.03.)

Assurance level 2
Credentials that provide single-factor authentication. There is specific identity proofing, registration, issuance, and CSP requirements that must be met for identity credentials to be used in identity authentication processes that are considered level 2. These types of identity credentials can be used if issued from a DoD approved identity credential provider. (See DoDI 8520.03.)

Assurance level 3
Credentials that provide identity authentication using at least two authentication factors. There are specified identity proofing, registration, issuance, and CSP requirements that must be met for identity credentials to be used in identity authentication processes that are considered e-authentication assurance level 3. Level 3 authentication processes must use credentials that use one-time password (OTP) or PKI certificate technology solutions and must include proof of possession of approved types of identity credentials through a cryptographic protocol. (See DoDI 8520.03.)

Assurance level 4
Credentials that provide identity authentication using at least two authentication factors. There are specified identity proofing, registration, issuance, and CSP requirements that must be met for identity credentials to be used in identity authentication processes that are considered level 4. Level 4 authentication processes must use credentials that use OTP or PKI certificate technology solutions and must include proof of possession of an approved hardware cryptographic token through a cryptographic protocol. (See DoDI 8520.03.)

Authentication
a. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. (See CNSSI 4009.)
b. A process used to confirm the identity of a person or to prove the integrity of specific information. (See CNSSI 4009.)
c. A process that matches presented information to the established origin of that information (DoD Security Lexicon). The process of validating that a claimed identity is genuine and based on valid credentials. (See FICAM guidance.)

Authenticator
The value or data object (for example, a password, a biometric template, or a cryptographic key) used to prove the claimant possesses and controls the identity credential. Assertion-based authenticators (for example, a PIN, a password, or a passphrase) are data with no associated physical characteristics or device. Cryptographic-based authenticators are cryptographically generated data or keys (usually only machine readable) carried or stored on a physical device such as the crypto-module on a smartcard. (See DoDI 8520.03.)

Authorization
The process of granting or denying specific requests for obtaining and using information processing services or data and to enter specific physical facilities. (See FICAM guidance.)

Binding
Process of associating two related elements of information. (See CNSSI 4009.)

Certificate
a. A computer-generated record that ties the user's ID with the user's PK in a trusted bond. The trust is based on registration/ID policy enforced by a third party certification authority. The certificate contains the following: ID of the certification authority issuing the certification; the user; the user's PK; and is digitally signed by the issuing certification authority.
b. A digital representation of information which at least: identifies the certification authority issuing it, names or identifies its subscriber, contains the subscriber's PK, identifies its operational period, and is digitally signed by the certification authority issuing it. (See American Bar Association Digital Signature Guidelines.)

Certificate authority
Also known as a certification authority, an entity that issues digital certificates. The digital certificate certifies the ownership of a PK by the named subject of the certificate. This allows others (RPs) to rely upon signatures or assertions made by the private key that corresponds to the PK that is certified. An authority trusted by one or more users to create and assign certificates. (See ISO 9594–8.)

Certificate policy
A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A CP addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a CP can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications. (See CNSSI 1300.)

Certificate revocation list
a. A computer-generated record that identifies certificates that have been revoked or suspended prior to their expiration dates. It is periodically issued by each certification authority and posted to the directory.
b. A complete CRL lists all unexpired certificates, within its scope, that have been revoked for one of the revocation reasons covered by the CRL scope. A full and complete CRL lists all unexpired certificates issued by a CA that have been revoked for any reason.
Note. Since CAs and CRL issuers are identified by name, the scope of a CRL is not affected by the key used to sign the CRL or the key(s) used to sign certificates. (See IETF RFC 5280.)

Certification authority system
The collection of hardware, software, and operating personnel that create, sign, and issue PK certificates to subscribers. (See CNSSI 1300.)

Certification Practice Statement
A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (in other words, requirements specified in this CP, or requirements specified in a contract for services). (See CNSSI 1300.)

Claimant
A party whose identity is to be verified using an authentication protocol. (See CNSSI 4009.)

Closed restricted network
A closed system enclave that is not logically connected to any other global system or network such as the internet, commercial internet service provider, Defense Research and Engineering Network (DREN), secret DREN, NIPRNet, or SIPRNet, but cryptographically tunnels over one or more of these networks for transport purposes. CRN traffic must be encrypted end-to-end over the transport network using DoD approved cryptographic means appropriate to the information type being transported. Approved cryptography includes but is not limited to FIPS 140–2 accredited Internet Protocol Security for FOUO information or NSA Type 1 encryption (for example, Tactical Local Area Network Encryption for classified information). (See U.S. Army NETCOM, "Stand-Alone Information System and Closed Restricted Network Assessment and Authorization Operational Tactics, Techniques, and Procedures.")

Code signing certificate
A certificate issued for the purpose of digitally signing executables, drivers, and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed by use of a cryptographic hash. (See CNSSI 1300.)

Common access card
Standard ID/smart card issued by DoD that has an embedded integrated chip storing PKI certificates.
Note. Per DoDI 1000.13, the CAC, a form of DoD ID card, will serve as the Federal PIV card for DoD implementation of HSPD–12. (See CNSSI 4009.)

Confidentiality
Assurance that information is not disclosed to unauthorized entities or processes. (See CNSSI 4009.)

Credential service provider
A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass RAs and verifiers that it operates. A CSP may be an independent third party or may issue credentials for its own use. (See CNSSI 4009.)

Credential strength
The resistance of the identity credential to forgery or fraud, taking into account the strength of the credential technology used (for example, resistance to copying or brute force attacks), the identity proofing performed prior to issuance of the identity credential, and the protections incorporated into the system issuing and managing the identity credential. Credential strengths are defined for both unclassified and classified environments.

Defense Enrollment Eligibility Reporting System
DMDC uses DEERS, also known as the Person Data Repository (PDR), to provide timely and accurate information on those eligible for DoD benefits and entitlements and to authenticate identity via RAPIDS.

Department of Defense identification number (formerly Electronic Data Interchange Personal Identifier)
a. A unique personal identifier created within DEERS for each person who has a direct relationship with DoD. (See DoDI 1000.30.)
b. A unique 10-digit number assigned to a PE in the PDR 15 by the DMDC when that PE is first associated with the DoD.16 The number is permanently assigned and unchanging.

Department of Defense Information Network
The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The DoDIN includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and NSS. (See DoD Dictionary of Military and Associated Terms.)

Derived credential
A credential issued based on proof of possession and control of a token associated with a previously issued credential, so as not to duplicate the identity proofing process. (See NIST SP 800–63A.)
Note. The derived credential will have an assurance level equal to or lower than the previously issued credential on which it is based.

Digital identity
The unique set of enterprise attributes by which an entity can be distinguished from any other entity.

Digital signature
a. The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory nonrepudiation. (See FIPS 186–4.)
b. An electronic analogue of a written signature in that the digital signature can be used in proving to the recipient or a third part that the message was, in fact, signed by the originator.

Dynamic access control
The automated management and use of the ICAM data to, in turn, automate access control.

Electronic authentication
The process of establishing confidence in user identities electronically presented to an IS. (See CNSSI 4009.)

Encryption
Transforming a text into code in order to conceal its meaning. The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process.

Enhanced trusted agent
An individual with the same capabilities and functions of a TA (which see), plus the ability to load credentials to tokens and issue them to users. ETAs are also authorized to maintain a small stock of blank tokens on hand to support this activity. ETAs perform other functions as directed, with additional training by an RA/LRA.

Exception
A determination approved by the Secretary of the Army or designee waiving for a limited time or purpose a policy or procedure contained in a DA publication. Also known as a waiver. (See AR 25–30.)

Identifier
Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. (See CNSSI 4009.)

Identity credential
An object (for example, a user ID or a smartcard) that authoritatively binds an identity (and optionally, additional attributes) to an authenticator that is possessed and controlled by a person. (See DoDI 8520.03.)

Identity credential provider
A source that issues credential(s) used for identity authentication. (See DoDI 8520.03.)

Identity proofing
Verification that the entity is the enrolled entity.

Information system security officer
Individual assigned responsibility by the senior agency information security officer, AO, management official, or IS owner for maintaining the appropriate operational security posture for an IS or program. (See CNSSI 4009.) (Formerly the information assurance officer.)

Integrity
Protection against unauthorized modification or destruction of information. Also, assurance that digital material is unaltered at the bit level and that the stated authorship is irrefutable. (See CNSSI 4009.)

Internet protocol
Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. (See CNSSI 4009.)

Lightweight Directory Access Protocol
An internet protocol that emails and other programs use to look up information from a server. The LDAP protocol is also used to look up the status of encryption certificates.

Local Registration Authority
a. The local (on site) point of contact that provides the user with their password and unique ID. The LRA provides this information to the certification authority. The LRA is the location on the post, camp, or station where information about user's transfer, death, name change, and so on, is collected and then relayed to the CA.
b. An RA with responsibility for a local community. (See CNSSI 4009.)

National Security Systems
Any telecommunications or IS operated by the U.S. Government; the function, operation, or use of which involves intelligence activities, involves cryptologic activities related to national security, involves command and control of military forces, involves equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (See CNSSI 4009.)

National Security Systems Public Key Infrastructure
A PKI for secret-high collateral classified networks. (See CNSSI 1300.) (See Secure Internet Protocol Router Network.)

Near/real–time system
System in which the correctness of the system depends not only on the logical result of computations, but also on the time at which the results are produced or the sense of urgency of the systems information processing and the information processed by the system to completion of the platform's mission, for example, air traffic control systems.

Network logon
The process that enables logical access to a fully provisioned DoD network account; an account that provides access to DoD network resources such as domain file shares. Identity authentication and authorization to access a DoD web server or other DoD IS that is hosted on a DoD network or in an approved demilitarized zone is not considered network logon. (See DoDI 8520.03.)

Non–classified Internet Protocol Routing Network
Unclassified router-based data network system, part of the Defense Information Infrastructure (DII).

Non–person entity
An entity with a digital identity that acts in cyberspace but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts. (See CNSSI 4009.)

Online Certificate Status Protocol
An internet protocol used for obtaining the revocation status of an X.509 digital certificate, an alternative to CRLs.

Person Data Repository
A DMDC managed database and associated services that contains information for each military personnel (active duty, retired, or a member of a Reserve Component), U.S.-sponsored foreign military, DoD and uniformed Services civilians, other personnel as directed by the DoD (including patients serviced through the Military Health Services System), and their eligible Family members. PDR is the DoD ICAM data store for most DoD-level PE attributes. DMDC, through multiple ingest, analytical, and reporting capabilities that are part of PDR, or are otherwise associated to DEERS, manages the necessary attributes to create digital identities for DoD and approved DoD mission partner person entities.

Person entity
An entity with a digital identity that acts in cyberspace and is a human actor. (See CNSSI 4009.)

Persona
a. An electronic identity that can be unambiguously associated with a single person or NPE. A single person or NPE may have multiple personas, with each persona being managed by the same or different organizations. (See CNSSI 4009.)
b. In military cyberspace operations, an abstraction of logical cyberspace with digital representations of individuals or entities in cyberspace, used to enable analysis and targeting. May be associated with a single or multiple entities. (See CNSSI 4009.)

Personal identity verification
A physical artifact (for example, identity card, “smart” card) issued to a government individual that contains stored identity credentials (for example, photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). PIV requirements are defined in FIPS 201. (See CNSSI 1300.)

Personal identity verification–interoperable
A PIV–I initiative to enable nonfederal organizations to issue employee identity cards that are technically interoperable with U.S. government PIV systems and issued in a manner that allows government and RPs to trust the cards. PIV–I requirements are defined in the FBCA CP. (See CNSSI 1300.)

Plan of action and milestones
A tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. (See OMB Memorandum 02–01.)

Public Key Cryptography Standard
Private Key Information Syntax Standard. Used to carry private certificate key pairs (encrypted or unencrypted). The DoD CA only exports key pairs in encrypted form. The filename extension is .p12.

Public key enabled
The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and nonrepudiation. (See CNSSI 4009.)

Public Key Infrastructure
a. A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke PK certificates. (See CNSSI 1300.)
b. The framework and services that provide for the generation, production, distribution, control, and accounting of PK certificates; a system with multiple components coupled with management which provides security services. This will ensure the following services over the DII at a reasonably high level of assurance (trust of information): authentication (proof that the sender is whom he claims to be (public/private key)); nonrepudiation (assurance that the person sending cannot deny participation (digital signature)); integrity (verification that no unauthorized modification of data has occurred (hash)); and confidentiality (assurance that the person receiving is the intended recipient (encrypt/decrypt)).

Public Key Infrastructure sponsor
A person who is responsible for the private key associated with a certificate and who asserts that the certificate and associated private key are being used in accordance with a CP. (See CNSSI 1300.)

Real–Time Automated Personnel Identification System
RAPIDS is a DoD NIPRNet system that allows updating and modification of information in the DEERS database and is a component in the DoD NIPRNet issuance process.

Registration Authority
a. An official recognized by the certification authority to ensure that the subscriber’s appropriately present the necessary credentials for registration into the PKI. In the DoD PKI, RAs enroll devices into the PKI, revoke user certificates, and authorize the LRAs to enroll individual subscribers.
b. An entity authorized by the certification authority system (CAS) to collect, verify, and submit information provided by potential subscribers which is to be entered into PK certificates. The term RA refers to hardware, software, and individuals that collectively perform this function. (See CNSSI 4009.)

Registration Practice Statement
A document representing a statement of practices an RA employs when performing RA duties for a CAS. The RPS supplements the CPS with additional specifics for the accomplishment of registration actions. It may provide additional safeguards for the assurance level of the PKI, but may not reduce or eliminate any standards or requirements of either the CPS or the CP. (See CNSSI 1300.)

Relying party
a. Any entity that uses a digital certificate to identify the creator of digitally signed information, verify the integrity of digitally signed information, or establish confidential communication with the holder of a certificate by relying on the validity of the binding of the subscriber's name to the PK contained in the certificate. (See DoDI 8520.03.)
b. An entity that relies on the validity of the binding of the subscriber's name to a PK to verify or establish the identity and status of an individual, role, or system or device; the integrity of a digitally signed message; the identity of the creator of a message; or confidential communications with the subscriber. (See CNSSI 4009.)
c. A person who has received a certificate and a digital signature verifiable with reference to a PK listed in the certificate and is in a position to rely on them. (See American Bar Association Digital Signature Guidelines.)

Secure Administration Authentication Gateway
The Army gateway solution that provides MFA capability for systems, devices, and applications that do not natively support MFA. Administrators connect to their devices by authenticating to the SAAG portal via DoD CAC/PKI.

Secure Internet Protocol Router Network
The worldwide secret-level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. (See DoD Dictionary of Military and Associated Terms.)

Stand–alone system
Types of enclaves that are not interconnected to any other network. Stand-alone systems do not transmit, receive, route, or exchange information outside of the system's authorization boundary. (See DoDI 8510.01.)

Subscriber
An entity that is the subject named or identified in a certificate issued to such an entity and holds a private key that corresponds to a PK listed in that certificate. Current subscribers possess valid DoD-issued certificates. (See CNSSI 1300 and CNSSI 4009.)

System or device
A system or device is an NPE that is capable of managing and using private keys and associated certificates. Examples of systems or devices are workstations, guards, firewalls, routers, web servers, and database servers. (See CNSSI 1300.)

Token
Something that the claimant possesses and controls (such as a key or password) that is used to authenticate a claim. (See CNSSI 4009.)

Trusted agent
An individual explicitly aligned with one or more RA officers who has been delegated the authority to perform a portion of the RA functions. A TA does not have privileged access to CAS components to authorize certificate issuance, certificate revocation, or key recovery. (See CNSSI 1300.)

User
A person who controls access to and use of a PKI token or other authentication credential. For other than individual credentials, this is the PKI sponsor.

Validation authority
An entity that provides a service used to verify the validity of a digital certificate per the mechanisms described in the X.509 standard by provision of CRLs or via OCSP response. (See IETF RFC 5280.)

Verifier
An entity that verifies the claimant's identity by verifying the claimant's possession and control of a token using an authentication protocol. To do this, the verifier may also need to validate credentials that link the token and identity and check their status. (See CNSSI 4009.)

Vetting
A part of target development that assesses the accuracy of the supporting intelligence to targeting. (See DoD Dictionary of Military and Associated Terms.)

Waiver
See definition for exception.

X.500 Directory Service
The X.500 Directory Service is a “white page” directory service that maintains specific information about people including names, email addresses, and other pertinent information on network directory servers. The model for directory service is based on a global directory model called LDAP. LDAP is a directory service protocol that runs over Transmission Control Protocol/Internet Protocol. The details of LDAP are defined in IETF RFC 1777.

X.509 Certificate
The certificate is the International Telecommunications Union–Telecommunication Standardization Section recommendation that defines a framework for the provision of authentication services under a central control paradigm represented by a “Directory”. The recommendation describes two levels: simple authentication, using a password as verification of claimed identity, and strong authentication, involving credentials formed by using cryptographic techniques; the “certificate”. The format of the certificate structure is defined along with responsibilities of the certification authority in regard to establishing and maintaining trust.

SUMMARY of CHANGE

DA PAM 25–2–13
Army Identity, Credential, and Access Management and Public Key Infrastructure Implementing Instructions

This major revision, dated 27 April 2023—

- Changes the proponent and exception authority from the Army Chief Information Officer to the Deputy Chief of Staff, G–6 (throughout).
- Identifies organizational split with the Chief Information Officer and the Deputy Chief of Staff, G–6 (throughout).
- Updates guidance on the use of the Army Master Identity Directory Service to obtain authoritative identity data, and requirements for all enterprise cloud-based services to use Enterprise Access Management Service–Army for authentication (para 3–3).
- Provides new guidance on the process to change an identity attribute standard used for identifying personnel on Army networks (para 3–4).
- Provides new guidance on the process to request a new identify, credential, and access management capability or an update to an existing capability within the Army (para 3–5).
- Provides new guidance on the management of Artificial Intelligence and Machine Learning technologies that are authorized to operate on Army networks and access information technology resources (para 3–6).
- Updates token retention guidance during duty assignment changes; creates two separate sections for Nonclassified Internet Protocol Router Network and Secure Internet Protocol Router Network to provide clarity (paras 4–13, 4–14).
- Updates guidance on the Nonclassified Internet Protocol Router Network Enterprise Alternate Token System and prohibits the issuance of the signature certificate on Nonclassified Internet Protocol Router Network Enterprise Alternate Token System and or the alternate smart card logon tokens (para 4–18).
- Updates guidance on requirements for senior official second Secure Internet Protocol Router Network token and use of the very important person's signing certificate (4–19).
- Provides new guidance on the issuance of public key infrastructure certificates for non-person entity devices (paras 5–4, 5–5).
- Updates guidance on requirements for personally owned devices to access unclassified information systems (para 5–6).
- Updates guidance for systems authorized to use user name and password authentication to transition to an Army approved alternative multi-factor authentication solution (para 5–7a).
- Provides guidance on the use of compensating controls to mitigate single-factor authentication to strengthen network security and on password standards (para 5–7b).
- Provides new guidance on the use of biometrics for logical access to Army Information Technology resources (para 6–2).
- Provides clarifying guidance on requesting approval to use alternate multi-factor authentication in place of direct public key infrastructure or the Army's Identity Federation Services Enterprise Access Management Service–Army (para 6–6).
- Updates Trusted Agent and Enhance Trusted Agent training website location (para 10–2c).