**NSTISSI No. 3028**
**December 2001**


# Operational Security Doctrine for the FORTEZZA User PCMCIA Card

**THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER INFORMATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.**

# National Manager

## FOREWORD

1. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 3028 "Operational Security Doctrine for the FORTEZZA User Personal Computer Memory Card International Association (PCMCIA) Card" prescribes the minimum security standards for the protection and use of FORTEZZA Personal Computer cards. This doctrine contains **no** policy or procedures for use of FORTEZZA cards in remote applications. Doctrine for remote user applications shall be provided separately.

2. NSTISSI No. 3028 is effective upon receipt. It supersedes all Interim Operational Systems Security Doctrine for the FORTEZZA PC Card, which should be destroyed.

3. Comments and suggestions regarding this NSTISSI may be sent directly to the National Security Agency, Information Assurance (IA) Policy, Procedures, and Insecurities Division (I41), telephone (410) 854-6831 (STU-III capable).

4. U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

5. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this NSTISSI at the address listed below.

MICHAEL V. HAYDEN
Lieutenant General, USAF

**NSTISSC Secretariat (I42). National Security Agency.9800 Savage Road STE 6716. Ft Meade MD 20755-6716**
**(410) 854-6805.UFAX: (410) 854-6814**
**nstissc@radium.ncsc.mil**

# OPERATIONAL SECURITY DOCTRINE
# FOR THE FORTEZZA USER PCMCIA CARD



## SECTION I - PURPOSE

1. This doctrine contains minimum security standards for the protection, handling, accounting, use, and destruction of the FORTEZZA® User Personal Computer Memory Card International Association (PCMCIA) Card.* It supersedes all Interim Operational Security Doctrine for the FORTEZZA Card.

2. The combination of the FORTEZZA card, FORTEZZA-enabled software, and Public Key Infrastructure (PKI) provides the security services FORTEZZA offers. Users must take the approved measures as outlined in this doctrine to maintain the security of both the FORTEZZA card and associated PKI.

## SECTION II - SCOPE

3. The requirements of this instruction apply to all U.S. Government Executive Branch departments, agencies and their contractors, consultants, and licensees who handle, distribute, account for, store, or use the FORTEZZA card and associated PKI certificates. Implementation can be accomplished by issuing this instruction in its entirety or by incorporating its provisions into department or agency directives. Where joint or unified commands or programs encounter conflicting communications security (COMSEC) implementing directives, this instruction will take precedence. When the requirements or terms of this instruction appear to substantially conflict with the requirements or terms of any other national-level issuance, the conflict will be identified and guidance requested, through organizational channels, from the National Manager, National Security Telecommunications and Information Systems Security Committee (NSTISSC) (Director, National Security Agency, ATTN: IA Policy, Procedures, and Insecurities Division).

---

* FORTEZZA® is a registered trademark of the National Security Agency.

4. This doctrine applies to FORTEZZA user PCMCIA cards employing the Type 2 suite of algorithms (e.g., SKIPJACK, Key Encryption Algorithm (KEA), Secure Hash Algorithm (SHA), Digital Signature Algorithm (DSA), and commercial algorithms) only, and includes crypto cards and FORTEZZA-enabled PCMCIA modem cards. This doctrine does not apply to PCMCIA cards employing a Type 1 suite of algorithms (e.g., FORTEZZA Plus). As other FORTEZZA implementations (e.g., smart cards) evolve, additional guidance will be promulgated either through amending this document or through separate issuances. These minimum security standards for the protection and use of the FORTEZZA user PCMCIA card apply to cards loaded with either X.509 version 1 or version 3 certificates. Differences in card labeling due to certificate version are described in paragraph 8.

> **NOTE:** The minimum security standards for the protection and use of the Certification Authority (CA) cards are specified in the Certificate Practice Statement for the department or agency (e.g., reference c for the Department of Defense {DoD}), and are beyond the scope of this instruction.

## SECTION III - POLICY

5. The FORTEZZA card provides cryptographic functionality and storage of keying material, authorization, and user identification. When combined with FORTEZZA-enabled applications, the card, employing a Type 2 suite of algorithms, provides confidentiality, user identification, authentication, and nonrepudiation (proof of origin and receipt) in unclassified and classified environments.

a. Unclassified Environment - The FORTEZZA card with FORTEZZA-enabled applications provides confidentiality, user identification, authentication, and non-repudiation sufficient to protect unclassified and/or sensitive information.

> **NOTE:** The Multilevel Information Systems Security Initiative (MISSI) program formerly referred to this information as “Sensitive-But-Unclassified” (SBU).

b. Classified Environment - The FORTEZZA for Classified (FFC) card is a FORTEZZA card programmed with PKI X.509 certificate(s) configured to protect classified information. The FFC card, with FORTEZZA-enabled applications, may be used on a secure network to provide user identification, authentication, nonrepudiation, and secondary confidentiality of classified information if primary confidentiality of the network is ensured by a Type 1 product, or a Protected Distribution System, or if the network exists completely within a secure enclave (see ANNEX A, paragraph i). The FFC card with FORTEZZA-enabled applications alone shall not be used as the primary means of providing confidentiality for classified information in any medium. A FORTEZZA for Classified card with certificates configured for use in a SECRET environment is called a “FFC card with certificates for

SECRET." A FORTEZZA card with FFC certificates configured for use in a TOP SECRET environment is called a "FFC card with certificates for TOP SECRET."

## SECTION IV - FORTEZZA CARD IMPLEMENTATION

6. Under the DoD Information Assurance Solutions (IAS) Program, formerly known as the MISSI, technology and components are being deployed in large numbers to protect valuable government information. The FORTEZZA card is a component of a network security solution and is intended to be used in conjunction with other IAS components (e.g., firewalls, high-assurance guards (HAGs), and trusted data base servers) to provide an appropriate and comprehensive network security solution.

> **NOTE:** The specification or description of other IAS components, including firewalls, HAGs, and trusted data base servers, is beyond the scope of this instruction.

a. FORTEZZA - The FORTEZZA card, combined with FORTEZZA-enabled applications, provides security services appropriate for protecting unclassified and/or sensitive data. Additional IAS components (e.g., firewalls, guards, and trusted data base servers) may be required to protect sensitive information in a networked environment, and are encouraged whenever accessing the public internet. These additional components may be mandated by the cognizant Designated Approving Authority (DAA).

b. FORTEZZA for Classified (FFC) - This paragraph provides the minimum system architecture requirements needed to securely process classified information with the FFC card. It is not intended to describe all system architecture requirements that must be met to create an approved system environment.

(1) Information Segregation on a Secure Network - The DAA for a secure network may approve the use of the FFC card to segregate classified information for privacy or need-to-know. This application includes use of the FFC card to maintain segregation between compartments or special handling categories on a common network approved to process information at any level up to TOP SECRET under conditions detailed in ANNEX E. However, the secure network must already be protected with Type 1 encryption or a protected distribution system.

(2) Secret Enclave to Sensitive Enclave over Unclassified Network - The DAA for a FORTEZZA supported workstation processing information classified up through SECRET in a protected enclave may authorize the exchange of sensitive or unclassified information over an unclassified network (e.g., the internet) with FORTEZZA supported workstation processing sensitive information within a sensitive enclave, provided all of the following conditions are met:

(a) A HAG is interposed between the classified enclave and the unclassified network. The HAG must perform a Crypto Invocation Check on any message leaving the classified enclave.

(b) A firewall is interposed between the sensitive enclave and the unclassified network.

(c) All communication from the classified enclave is encrypted with an unclassified certificate on the FFC card. That certificate must have been loaded on the FFC card by an unclassified Certification Authority Workstation (CAW).

(d) FORTEZZA-enabled applications must be used.

(e) A virus check must be performed prior to transferring information from an unclassified enclave to a classified enclave.

## SECTION V - SECURITY AND ACCOUNTABILITY

7. Card Classification

a. FORTEZZA - The FORTEZZA card is unclassified both when locked and unlocked. The FORTEZZA card shall not be marked or handled as CRYPTO or a Controlled Cryptographic Item (as defined in reference a).

> **NOTE:** A FORTEZZA PCMCIA card is considered locked when the card is not in use. It is unlocked when the card is inserted into the PCMCIA reader, and its Personal Identification Number (PIN) is entered into the FORTEZZA-enabled application to activate the card. Closing the application and removing the card from the PCMCIA reader will lock it.

b. FFC - The FFC card is unclassified when locked. When unlocked by the PIN, the FFC card will be classified at the level of the highest classification able to be protected by certificates on the card.

(1) The implementing organization may, in order to further mitigate risk to its information, elect to handle the FFC card as classified material when not in use and locked with the PIN. Any change from the default marking of UNCLASSIFIED assigned to all user cards by the CAW (see paragraph 8) would require that custom labeling be placed on the FFC card.

(2) A FFC card with both certificates for classified information from a classified CAW and certificates for unclassified information from an unclassified CAW is called a “dual-certificate” card. A dual-certificate card is classified when unlocked, and can only be

used on a computer authorized to process classified information. A dual-certificate card supports the environment described in paragraph 6b(2).

(3) Each user's public key certificates for FFC use which are stored on the workstation remain unclassified. The FFC card shall not be marked or handled as CRYPTO or Controlled Cryptographic Item (as defined in reference a).

8. Card Nomenclature and Marking

a. Nomenclature - KOV-11 is both the NSA assigned short title and the Federal Stock System nomenclature for all FORTEZZA user cards. Since the FORTEZZA user card is not controlled within the COMSEC Material Control System (CMCS), this instruction will refer to "KOV-11" as a nomenclature.

**NOTE:** The FORTEZZA card and the FFC card are identical except for the classification of certificates loaded onto each. Therefore, the nomenclature "KOV-11" applies to both.

(1) FORTEZZA nomenclature use evolved during its deployment. FORTEZZA and FFC cards with X.509 Version 1 certificates were assigned nomenclatures as shown in Table 1. However, the multiple nomenclatures created inventory and accounting difficulties. As a result, the KOV-12 nomenclature is no longer used and cards bearing this nomenclature shall be phased out. (See paragraph 8a(2) below.)

(2) As the FORTEZZA PKI transitions to X.509 Version 3 certificates, user card nomenclature is standardized to KOV-11. Old labels not reflecting Version 3 certificate nomenclature should be replaced when the user card is returned to the CA for rekey/certificate renewal, but no later than December 31, 2004.

b. KOV-11 Label - The CAW prints a card label that uniquely identifies each card. This label contains the nomenclature (KOV-11), unique internal chip serial number, user name, card classification, and indicates if it is programmed with certificates for unclassified or classified information. A FORTEZZA card with certificates to protect UNCLASSIFIED information has a white label, and a FFC card with certificates for SECRET information has a red label. A FFC card with certificates for TOP SECRET information has a yellow label. Label colors follow the same scheme regardless of which X.509 certificate version is loaded on the card. The user shall not remove the card label. Table 1 (below) provides approved nomenclature and labeling guidance for FORTEZZA user cards.

## TABLE 1. FORTEZZA CARD MARKING

| Type | X.509 Ver. 1 Nomenclature | X.509 Ver. 3 Nomenclature | Label and Type Color | Marking |
|---|---|---|---|---|
| Organizational and personal FORTEZZA user card | none | KOV-11 | White Label Black Type | UNCLASSIFIED |
| Organizational and personal FFC user (with FFC certificates up through SECRET) card | KOV-11 or KOV-12 | KOV-11 | Red Label Black Type | UNCLASSIFIED (see 9b) |
| Organizational and personal FFC user (for compartmentation on TOP SECRET networks - see ANNEX D) card | KOV-12 | KOV-11 | Yellow Label Black Type | UNCLASSIFIED (see 9b) |

**NOTE:** FORTEZZA card labeling is distinct and different from federal magnetic media labeling. The FFC card is classified only when unlocked and in use, so a federal standard magnetic media label indicating a permanent classification (e.g., the orange SF-706) is inappropriate.

c. FORTEZZA-Enabled PCMCIA Modem - The FORTEZZA-enabled PCMCIA modem (i.e., the Palladium modem card) uses the same PKI certificates as a FORTEZZA card, and must have these certificates loaded by a CAW in the same manner as a FORTEZZA or FFC user card. The CAW treats the FORTEZZA modem card as a standard FORTEZZA or FFC card, and so prints a label as discussed above.

d. Certification Authority Cards - The procedures and policy for use of the FORTEZZA CA cards, to include the KOV-13, are specified in the Certificate Practice Statement for the department or agency (e.g., reference c for DoD), and are beyond the scope of this instruction.

9. Safeguarding FORTEZZA and FFC Cards

a. Unclassified - FORTEZZA cards (KOV-11s with only unclassified certificates loaded) must be protected in a manner similar to a credit card or high value item to limit the possibility of loss, unauthorized use, substitution, tampering or breakage. KOV-11s may be carried by individuals, provided the cards are given the level of protection discussed in this paragraph.

b. FORTEZZA for Classified

(1) A locked FFC card (i.e., a card that is not in use) is UNCLASSIFIED and must be physically protected by either being in the personal possession of

the authorized, cleared user, or stored in a manner that will minimize the possibility of loss, unauthorized use, substitution, tampering, or breakage. (See paragraph 22 for additional information.)

(2) An unlocked FFC card (i.e., a FFC card that is in use) is classified to the level of the information that can be protected by its certificates and must be afforded commensurate protection (e.g., a FFC with certificates for SECRET is classified SECRET when unlocked; a FFC with certificates for TOP SECRET is classified TOP SECRET when unlocked). When leaving the workstation, the user must remove the FFC card from its reader and protect it as described in paragraph 9b(1).

(3) A FFC card may be left unlocked in a continuously operating, unstaffed infrastructure component (e.g., a Defense Message System Message Transfer Agent) provided the component or the space in which it is located provides protection commensurate with the classification of the information the component is authorized to process.

c. FORTEZZA PCMCIA Modem Card - A FORTEZZA or FFC modem card inside a secure facility shall be afforded protection at least equal to that given the same type of user card.

10. Personal Identification Number Length - The minimum requirement for a FORTEZZA/FFC user card (any KOV-11) PIN is seven numeric characters. The maximum length is 12 numeric characters.

11. Safeguarding PINs

a. PINs should be memorized. PINs shall not be written on the KOV-11 card or recorded in any manner in the vicinity of the host system for any reason. The user must securely store the PIN or PIN letter separate from the card to prevent loss or unauthorized access.

b. PINs shall not be shared, except in cases of organizational cards.

c. The PIN for a FORTEZZA card is unclassified.

d. The PIN for a FFC card is normally unclassified, and the PIN letter is printed without classification. The implementing organization may, in order to further mitigate risk to its information, elect to classify the PIN (and PIN letter), but only when the PIN is directly associated with a specific card. The PIN may be classified up to the level of the highest classification able to be protected by certificates on the card, but is not to be marked or handled as CRYPTO (as defined in reference a).

12. Automatic Disabling - The KOV-11 will disable itself after 10 consecutive failed attempts to enter the PIN. Users must then provide their card to the CA who initially

programmed a certificate onto the card. This CA will provide a new PIN and reactivate the card.

13. Accountability - The KOV-11 is locally accountable to the CA, who must be able to determine the status and location of the FORTEZZA cards and certificates he or she has produced. Programmed cards will be tracked and identified to the CA by means of the card's internal chip serial number and user name, printed on the card label by the CAW as described above. KOV-11s shall not be tracked by the manufacturer's external serial numbers, because these numbers are not unique. The department, service, or agency issuing and using the KOV-11 shall employ appropriate means to account for its cards.

a. Inventory - KOV-11s containing unclassified and/or classified certificates must be regularly inventoried.

(1) The inventory may be performed by physical means (e.g., the CA or Registration Authority (RA) sights each card) or electronic means (e.g., each user sends the issuing CA a digitally-signed message verifying possession).

(2) KOV-11s with only unclassified certificates shall be inventoried at the implementing organization's discretion, but not less than once every three years.

(3) Each personal user FFC KOV-11 (including duplicate cards) shall be inventoried at least annually. Organizational FFC KOV-11s shall be inventoried at least every three years. If a KOV-11 cannot be accounted for within 15 days of the required inventory, then the certificates associated with the missing KOV-11 will be added to the Certificate Revocation List (CRL).

b. Additional Accountability - KOV-11s normally remain the property of the issuing organization. Local policy may also require additional accountability of the cards.

14. Classified Information Security - Users must safeguard and control all U.S. Government classified information processed by the FFC card in accordance with department, service, or agency directives.

15. Disposal/Destruction

a. Routine Disposal - KOV-11s that are excess or no longer required must be returned to the issuing CA who will determine if the card can be reused. If cards are not returned in person to the CA, the cards must be returned via controlled methods (those methods which provide a continuous chain of accountability, as described in ANNEX D).

b. Emergency Destruction - KOV-11s may be destroyed by smashing or breaking to be rendered as unusable as practical. Organizational cards must be destroyed

prior to individual user cards. If the capability exists and the time is available, the KOV-11 may be zeroized by the CA as an alternative to physical destruction.

## SECTION VI - RESTRICTIONS

16. FORTEZZA and FFC Incompatibility - Certificates loaded by an unclassified CAW are not cryptographically compatible with any certificates loaded by a FFC CAW.

17. Individual Certificates - KOV-11s with certificates programmed for individual messaging accounts must not be shared. The authenticity of messages is based on individuals' using only the card assigned to them.

18. Organizational Certificates - KOV-11s with certificates programmed for organizational use ("organizational certificates") carry additional restrictions, as follows:

a. The user must ensure control of these certificates and their private keys, including accounting for which individual had control of the keys at a given time. The user or designated representative will prepare a list identifying personnel authorized to have access to the certificates and private keys. A custody log will be maintained to identify KOV-11(s) serial number, the name of the individual who had temporary custody of the KOV-11, date and time issued/received and returned/turned over. The organization shall retain the custody log for three years from the date of the last entry; after which the logs shall be forwarded to the cognizant CA for archiving, which will be kept for twenty years and six months.

b. The CA and RA must track the names of individuals identified on the X.509 Certificate Request Form as the user and the individual to whom organizational certificate(s) were issued.

c. The organization Information Systems Security Officer (ISSO) must ensure control of these certificates and their private keys, including accounting for which individual had control of the keys at a given time. The ISSO will ensure that the user (see paragraph a above) prepares a list identifying personnel authorized to have access to the card, and also maintain a custody log which will identify KOV-11(s) serial number, the name of the user, date and time issued/received and returned/turned over. The organization shall retain the custody log for three years from the date of the last entry, after which the logs shall be forwarded to the cognizant CA for archiving, which will be kept for twenty years and six months.

19. KOV-11 Storage - Storage on the KOV-11 is limited to certificates, keying material, and security-critical information. The user must not use the KOV-11 as a general-purpose data storage device.

## SECTION VII - CONTROL REQUIREMENTS

20. Access Controls - KOV-11s will be issued only to authorized personnel. FFC KOV-11s will be issued only to properly cleared personnel with a valid access requirement. The FFC KOV-11 user must be cleared to a level equal to or greater than the card's highest certificate clearance.

a. U.S. Citizen User - Users must demonstrate operational need for the KOV-11, as validated by their supervisor.

b. Non-U.S. Citizen User

(1) Employed by the U.S. Government - In certain situations, KOV-11s may be issued to permanently admitted resident aliens who are civilian employees of the U.S. Government, or are active duty or reserve component members of the U.S. Armed Forces. The decision to issue a KOV-11 shall be made by the cognizant security authority based on a determination that the official duties of the resident alien require this access.

(2) Employed by a U.S. Government Contractor or Vendor - Any non-U.S. citizen, employed by a U.S. Government contractor or vendor, may only be issued FORTEZZA cards with the prior written approval of the appropriate Government Contracting Office. Requests for FORTEZZA card issue must be fully justified and must be based on essential operational need.

(3) Supporting U.S. or Combined Exercises and Operations - Non-U.S. citizens may be issued KOV-11s when the cognizant U.S. authority determines an operational need. Additional handling restrictions may be levied on foreign national users at the discretion of the issuing department, service, or agency. Examples of situations in which non-U.S. users may be issued KOV-11s include:

(a) foreign liaison officers granted access to information systems in their extended visit authorization;

(b) foreign exchange officers granted access to information systems in their position authorization; or

(c) allies or coalition partners in a comanned environment; allies or coalition partners in combined exercises or operations.

21. Transporting Programmed Cards - KOV-11s should only be transported in a locked condition. (See paragraph 25 below if KOV-11s cannot be locked.) Specific guidance for transporting programmed KOV-11s is found in ANNEX D.

22. Removing FFC Card from Secure Enclave - Users who have an operational requirement to remove the FFC KOV-11 from a classified system-high enclave, must be authorized by the cognizant DAA and reminded of their responsibility to safeguard the card outside the secure enclave. Users without such a requirement should satisfy paragraph 9b by securing their FFC KOV-11s within the secure enclave. Users who have additional requirements to conduct unclassified transactions outside of an environment approved for classified information processing must be issued a separate unclassified-only KOV-11. In general, the FFC card should not be removed from the secure enclave except for administrative purposes (e.g., to transport card from issuing location to user's location).

23. Tampering - No attempt should be made to copy or tamper with the KOV-11. It is the user's responsibility to report any suspected tampering attempts in accordance with Section X.

24. Loaning Cards - KOV-11s programmed and assigned to one individual user will not be loaned to any other individual.

25. Inoperable KOV-11

a. Users must not attempt to repair or reprogram an inoperable KOV-11. An inoperable card must be returned to the issuing CA, in person when possible, who will determine if the card can be reused. If an inoperable FFC KOV-11 fails and cannot be locked, it must be returned to the issuing CA by means authorized for its unlocked classification.

b. If the KOV-11 cannot be returned in person to the CA, the card must be returned via controlled methods that provide a continuous chain of accountability, as described in ANNEX D.

c. If the card itself is defective, a new card, new certificate, and new PIN will be programmed for the user. The old certificates from inoperable KOV-11s must be revoked. The user must notify all CAs who placed certificates on their inoperable KOV-11 so that those certificates may be revoked. To allow recovery of existing information (e.g., back traffic, text files, databases) encrypted with the old certificate, the old certificate will be reprogrammed onto the new card. The CA must revoke the old certificates 30 days after re-issue.

26. Duplicate Cards - Duplicate programming of an individual or organizational user's KOV-11 is not encouraged due to the additional burden of safeguarding and management (see paragraph 20 for additional requirements for KOV-11s with organizational certificates). When dictated by operational necessity, one duplicate card may be issued to the individual identified as the user of the card on the original X.509 Certificate Request Form. Users must be reminded of their responsibility to properly safeguard the duplicate cards and should return the duplicate cards to the CA when no longer needed.

27. Protecting Workstations

a. Workstation(s) with FORTEZZA associated software installed should be protected in a manner sufficient to prevent loss, tampering, or unauthorized use of the system. To prevent possible unauthorized use, users must not leave a terminal unattended after the PIN has been successfully entered and the KOV-11 and associated software is available for use. An exception is allowed for continuously operating systems protected in accordance with paragraph 9b(3).

b. Lockscreens and screensavers are not acceptable means to protect an unlocked KOV-11 in a workstation.

## SECTION VII - INFORMATION SYSTEM SECURITY

28. Virus Detection - The KOV-11, in and of itself, offers no protection from viruses. Appropriate virus detection software must be identified for each workstation on which the FORTEZZA application will be operated.

29. Configuration Management - Users should use the most current version of FORTEZZA-enabled software. If the user receives software and hardware changes, the local System Administrator (SA) and ISSO should be contacted to assist in confirming the authenticity and ensure the installation is compliant with the DAA approval.

30. FFC Architectural Approval - Implementation of the FFC KOV-11, along with other necessary IAS/FFC components, for protecting classified or compartmented information must be approved by the appropriate DAA prior to use.

31. Authorized Computers

a. FORTEZZA Card - A FORTEZZA card and FORTEZZA-enabled software may only be used with a computer authorized to process unclassified or sensitive information.

b. FFC Card

(1) FFC cards with certificates for classified information (SECRET, TOP SECRET, etc.) shall only be used with a computer, and within an environment that has been authorized for the processing of comparably classified and below information (e.g., a FFC card with certificates for SECRET information must be used on a system authorized to process SECRET and below information).

(2) FFC cards with both classified certificates from a classified CAW and unclassified certificates from an unclassified CAW (a “dual-certificate” card) shall only be used within a computer and an environment that is authorized to process information at the level of the highest classification able to be protected by certificates on the card. A FFC card

with an unclassified certificate from an unclassified CAW shall not be used in an unclassified computer/environment.

32. Classification Labeling - FORTEZZA-enabled applications must provide appropriate security labeling for the data being processed. That is, the FORTEZZA-enabled software must require the user to insert the classification level of the data and it must ensure that the correct certificate is used based on the chosen classification and the cryptographic environment of the recipient.

## SECTION IX - PUBLIC KEY INFRASTRUCTURE REQUIREMENTS

33. User Registration - The prospective user must provide at least one official picture identification to the CA/RA upon registration for the FORTEZZA card. (Note paragraph 20 for specific qualifications of a user.) Specific user registration procedures are the responsibility of the Policy Creation Authority (PCA) and implementing department or agency.

34. Card and PIN Distribution - The KOV-11 and the associated PIN letter must be kept separate from the time they are produced by the CA until the intended user receives them. If the implementing organization elects to classify the PIN, it must classify the PIN letter and distribute it appropriately.

a. Direct Distribution – Hand delivery of both the KOV-11 and PIN letter directly to users is allowed if separation of the KOV-11 and PIN letter is maintained. This separation may be achieved by having separate distribution locations for the KOV-11 and PIN letter. A single distribution point may be used if the intended user uses tamper-evident packaging to seal the PIN letter from viewing until receipt. Positive identification of the user is required in hand delivery. In the event of hand delivery, and if the distribution facility is separate from the user's working facility, the user may carry both KOV-11 and PIN letter back to the working facility, provided measures are taken to minimize the risk of the loss or compromise of both card and PIN letter.

b. Mail Distribution - When mailed, KOV-11s must be shipped to the user via an approved method that provides continuous accountability during distribution, and requires that a signed receipt is returned to the generating CA by the intended user. Within the United States, U.S. Registered Mail and Federal Express are known to meet these requirements. (See ANNEX D.) Separation of KOV-11 and PIN letter may be maintained by:

(1) mailing the KOV-11 to either the user's work or home address and the PIN letter to the other address;

(2) separating the mailing of both KOV-11 and PIN letter to the same address by more than three days; and

(3) placing one (or both) of card and PIN letter in separate tamper-evident packaging within the same shipping container.

c. Courier Distribution - The RA or designated individual may courier properly packaged KOV-11s and PIN letters from the CA to distant users with the cognizant approving authority's authorization. Separation of KOV-11 and PIN letter must be maintained through the use of tamper-evident packaging while in the courier's custody.

35. FORTEZZA/FFC User Advisory Statement and Receipt - Upon receiving the KOV-11, the user must sign a User Advisory Statement in the format of ANNEX C, and return it to the CA who created the card. By signing this FORTEZZA User Advisory Statement and Receipt, the user acknowledges receipt of the KOV-11 and agrees to accept the certificates listed on documentation provided with the KOV-11. If the user does not return the User Advisory Statement to the issuing CA within the appropriate interval set by the CA and/or PCA, the CA will revoke all the user certificates on that KOV-11.

**NOTE:** The CA's archive requirements and other operating procedures are specified in the Certificate Practice Statement for the department or agency (e.g., reference c for DoD), and are beyond the scope of this instruction.

36. KOV-11 Rekey and Certificate Renewal

a. KOV-11 Rekey - The FORTEZZA/FFC user card must be rekeyed at least every three years. The user's PIN is changed when the card is rekeyed. The FORTEZZA card must be returned to the issuing CA for rekey using transportation methods specified in ANNEX D.

b. Certificate Renewal - The user's certificates are renewed and validated at least every three years.

c. Notification - Notification of pending key, PIN or certificate expiration may occur in one of two ways:

(1) The FORTEZZA-enabled application, or User Agent, alerts the user when the key or certificate is expiring, and the user must request rekey and certificate renewal from the appropriate CA(s).

(2) At the discretion of the service, department, or agency, the CA responsible for programming specific cards will notify each user when their certificate, key, and PIN are about to expire. Should a user fail to present their card for rekey and certificate renewal to the appropriate CA when notified to do so, their certificate may be added to the CRL, thereby alerting users that the certificate is no longer valid even if the expiration date has not been reached.

37. Loss/Compromise Requirements - The loss or suspected compromise of a KOV-11 must be reported to the cognizant CA no later than one working day after discovery. Information required by the CA is described in paragraph 42. Users with KOV-11s programmed with certificates from multiple CAs must report to each CA.

38. CRL and CKL Posting - CAs post a new CRL every 28 days, or as necessary due to certificate revocation. Users are responsible to ensure their workstation always contains the most recent CRL/Compromised Key List (CKL) listings.

39. User Departure - Prior to departing an organization, the user must return personal user KOV-11s to the CA or authorized agent. Failure to return the KOV-11 will result in the CA reporting a compromise of user FORTEZZA keys to the PCA. Individuals responsible for organizational cards and equipment sponsors who depart an organization will notify the CA of the new responsible individual. The CA may enter the new name on the X.509 Certificate Request Form and the CAW database. The new responsible individual should sign a FORTEZZA Card User Advisory Statement and Receipt.

40. Digital Signature Verification - The sender's digital signature prepared by the sender's KOV-11 must be verified against the CRL listings to validate the authenticity of the transmitted data. If the sender's digital signature certificate has expired or cannot be verified, the transmission should not be accepted as valid.

## SECTION X - REPORTABLE EVENTS

41. The following events involving KOV-11 usage must be reported to the CA/RA and ISSO, no later than one working day after the event, for review and possible compromise recovery actions.

a. Loss of Card - The temporary or permanent loss of any KOV-11.

b. PIN Compromise - Actual or suspected compromise of PIN.

c. Card Misuse - Actual or suspected misuse of the KOV-11 and associated software (e.g., unauthorized modification to the FORTEZZA software installed on the host).

d. Card Tampering - Actual or suspected tampering with the KOV-11.

e. Duplicate Cards - Unauthorized use of an authorized duplicate card or an unauthorized duplication of a card.

f. Unreported Changes to Distinguished Name - User failure to notify the issuing CA of Distinguished Name (DN) changes.

g. User Departure - KOV-11 user leaving an organization without advising the CA(s) concerning the status of his/her card.

h. Card/PIN Not Received - If programmed KOV-11 or PIN or both are not received from the CA/RA.

i. Premature Disabling - Detection that a user's card is disabled prior to the user making 10 unsuccessful consecutive attempts to unlock his/her card.

j. Incorrect Certificate Use - The use of an unclassified certificate to protect classified information.

42. Reportable Events Report Format - Data required by the CA/RA and ISSO to assess the impact of the events detailed in paragraph 41 include the following:

a. user's name, distinguished name, card serial (chip internal serial number), and organization;

b. all certificates and CAs who programmed certificates on the card;

c. complete circumstances of incident, including physical security situation;

d. other personnel involved in incident;

e. what was potentially compromised (the card, PIN, or FORTEZZA software); and

f. user's assessment of degree of potential compromise. The user's cognizant security authority may require additional information.

## SECTION XI - REFERENCES

43. The following documents are referenced in this doctrine or are otherwise applicable:

a. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, dated September 2000.

b. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), dated January 1995.

**NOTE:** DoD 5220.22-M applies to U.S. Government contractors who are participants in the Defense Industrial Security Program (DISP). Cleared

U.S. Government contractors who are not participants in the DISP will use implementers of the governmental references provided by their U.S. Government sponsors.

c. NAG-69C, Information Security Policy and Procedures for FORTEZZA Card Certification Authority Workstation, dated February 2000.

5 Encls:

ANNEX A – Definitions
ANNEX B – Acronym List
ANNEX C - FORTEZZA User Card Advisory Statement and Receipt (Sample)
ANNEX D - Methods for Transporting the Programmed FORTEZZA Card (KOV-11)
ANNEX E - Use of the FFC Card to Separate Compartmented Data

ANNEX A

DEFINITIONS

For reader convenience, selected definitions from NSTISSI No. 4009 are quoted below, along with definitions for system unique, specialized terms used in this instruction. Additional items specific to the PKI are also defined here and noted as such.

a. Approving Authority – Senior-level official within the U.S. department, agency, or service who is responsible for approving the establishment of Certification Authority (CA) operations within their respective organizations. (PKI)

b. Certificate – A record holding security information about an information system user and vouches as to the truth and accuracy of the information it contains. (NSTISSI No. 4009)

> **NOTE:** A public key certificate contains the name of a user, the public key component of the user, and the identity of the user who vouches that the public key component is bound to the named user.
>
> **NOTE:** A public key certificate is normally issued to individuals. When several individuals act in one capacity for an organization, an "organizational certificate" may be issued with the identity of the organization.

c. Certificate Revocation List (CRL) – A list of invalid certificates that have been revoked by the issuer. (NSTISSI No. 4009)

> **NOTE:** It is periodically issued by each Certification Authority and posted to the directory.

d. Certification Authority (CA) – Certification Management Authority responsible for issuing and revoking user certificates, and exacting compliance with the PKI policy as defined by the parent Policy Creation Authority. (NSTISSI No. 4009)

> **NOTE:** The term CA refers to either the authoritative office or role, and the incumbent in that office.

e. Certification Authority Workstation (CAW) – Commercial-off-the-Shelf (COTS) workstation with a trusted operating system and special purpose application software that is used to issue certificates. (NSTISSI No. 4009)

**NOTE:** The CAW programs FORTEZZA cards with a user's security personality, including certificates and crytographic key. The CA operates the CAW.

f. Compromised Key List (CKL) – A list generated periodically by a Policy Creation Authority (PCA) that contains the Key Material Identifiers (KMIDs) of keys believed by the PCA to be compromised (i.e., that can no longer be trusted). (PKI)

g. Designated Approving Authority (DAA) – Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority. (NSTISSI No. 4009)

h. Distinguished Name (DN) – Globally unique identifier representing an individual's identity. (NSTISSI No. 4009)

**NOTE:** "Globally unique" means unique within a given PKI certificate management infrastructure.

i. Enclave – A general computing term used to describe an interconnected collection of some subset of an organization's local computing resources. An enclave is often comprised of heterogeneous platforms that operate in a multiprotocol environment sharing common characteristics. These characteristics may include, but are not limited to, common ownership/management, common mission, definable physical boundary, common security policy, controllable access point(s) to the enclave, and heterogeneous levels of trust. (PKI)

j. FORTEZZA for Classified (FFC) – (Classified Card) – A PCMCIA card that uses algorithms and procedures approved by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to provide network related security services for enclaves up to and including TOP SECRET. Also identified as the KOV-11, the card, when used in conjunction with the proper applications and network infrastructure, provides confidentiality of user information. (PKI)

k. FORTEZZA Card - (Unclassified Card) – A PCMCIA card that uses algorithms and procedures approved by NIST and NSA to provide network related security services. Also identified as the KOV-11, the card, when used in conjunction with the proper applications and network infrastructure, provides data integrity, access control, authentication, nonrepudiation and confidentiality of user information. (PKI)

l. FORTEZZA-Enabled Application – Any software application that has been designed (or enabled) to use FORTEZZA cryptography when providing security services. This can be client software running locally on a user's workstation (i.e., File Transfer Protocol (FTP)

clients, electronic mail clients, web browsers) or server software running unattended on a server (i.e., FTP servers, web servers, Directory System Agents). (PKI)

m. Information Systems Security Officer (ISSO) – Person responsible to the Designated Approving Authority for ensuring the security of an information system throughout its life cycle, from design through disposal. (NSTISSI No. 4009)

n. Key Material Identifier (KMID) – The KMID is a unique field contained in a X.509 certificate that identifies a specific set of private key material. The KMID is unique within the Policy Approving Authority (PAA) hierarchy. (PKI)

o. Personal Identification Number (PIN) - A randomly generated character string assigned to each card that is used by the FORTEZZA-enabled application to unlock and activate the FORTEZZA card. (PKI)

p. Policy Approving Authority (PAA) – The first level of the PKI Certification Management Authority that approves the security policy of each PCA. (NSTISSI No. 4009)

**NOTE:** The term PAA refers both to that authoritative office or role, and to the incumbent in that office.

q. Policy Creation Authority (PCA) – The second level of the PKI Certification Management Authority that formulates the security policy under which it and its subordinate CAs will issue public key certificates. Also known as Policy Certification Authority. (NSTISSI No. 4009)

**NOTE:** The term PCA refers both to that authoritative office or role, and to the incumbant in that office.

r. Public Key Infrastructure (PKI) – The framework established to issue, maintain, and revoke public key certificates. (NSTISSI No. 4009)

s. Resignation Authority (RA) – The person who assists the CA by collecting and verifying the users' identity and information which is to be entered into public key certificates. (PKI)

t. Sensitive Information – Sensitive information is information the loss, misuse, or modification of which, or unauthorized access to, could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or Act of Congress to be kept classified in the interests of national defense or foreign policy. (NSTISSI No. 4009)

**NOTE:** Departments or agencies within the U.S. Government should apply handling caveats or warning notices. The responsibility for determining the applicability of the handling caveat or warning notice lies with the originating organization. (Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of Public Law 100-235, the Computer Security Act of 1987.)

**NOTE:** The MISSI program formerly referred to this information as "Sensitive-But-Unclassified" (SBU).

u. Service/Agency Sub-Registration Authority (SRA) – An individual with primary responsibility for managing the distinguished name process. (PKI)

**NOTE:** The SRA works with the CA in developing a unique DN for the end-entity on a FORTEZZA card, and creates an entry in the directory for each security personality associated with the end-entity. In some organizations, the SRA may also perform the duties of a RA.

v. System Administrator (SA) – Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established INFOSEC policy and procedures. (NSTISSI No. 4009)

## ANNEX B

## ACRONYM LIST

| ACRONYM | EXPANSION |
|---|---|
| AA | Approving Authority |
| APO | Army/Air Force Post Office |
| ACL | Access Control List |
| CA | Certification Authority |
| CAW | Certification Authority Workstation |
| CKL | Compromised Key List |
| CMCS | COMSEC Material Control System |
| COMSEC | Communications Security |
| COTS | Commercial-Off-The-Shelf |
| CRL | Certificate Revocation List |
| DAA | Designated Approving Authority |
| DISP | Defense Industrial Security Program |
| DN | Distinguished Name |
| DoD | Department of Defense |
| DSA | Digital Signature Algorithm |
| FFC | FORTEZZA for Classified |
| FPO | Fleet Post Office |
| HAG | High Assurance Guard |
| IAS | Information Assurance Solutions |

| | |
|---|---|
| INFOSEC | Information Systems Security |
| ISSO | Information Systems Security Officer |
| KEA | Key Encryption Algorithm |
| KMID | Key Material Identifier |
| MISSI | Multilevel Information Systems Security Initiative |
| NIPRNET | Unclassified But Sensitive Internet Protocol Router Network |
| NISPOM | National Industrial Security Program Operating Manual |
| NSA | National Security Agency |
| NSTISSI | National Security Telecommunications and Information Systems Security Instruction |
| PAA | Policy Approving Authority |
| PCA | Policy Creation Authority |
| PCMCIA | Personal Computer Memory Card International Association |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PSTN | Public Switched Telephone Network |
| RA | Registration Authority |
| SA | System Administrator |
| SAP | Special Access Program |
| SAR | Special Access Required |
| SBU | Sensitive-But-Unclassified |

| | |
|---|---|
| SCI | Sensitive Compartmented Information |
| SHA | Secure Hash Algorithm |
| SIPRNET | SECRET Internet Protocol Router Network |
| SRA | Sub-Registration Authority |
| TS | TOP SECRET |
| U.S.C. | United States Code |
| USPS | U.S. Postal Service |

ANNEX C

FORTEZZA CARD USER ADVISORY STATEMENT AND RECEIPT
(SAMPLE)

The FORTEZZA®/FFC cryptographic card* is a self-contained security device which provides you, the user, with a digital certificate - a unique electronic "personality" - and all the cryptographic support functions you need to perform electronic digital signature, encryption, and decryption of your information, all in a flexible and compact package. Used properly, your cryptographic card will provide you with a high degree of security.

Because of its compact size, the cryptographic card can be carried readily in a pocket or purse. Be aware that loss of your card may place the information you have protected at risk. A hostile entity who has unauthorized access to your card could attempt to use the card to decrypt information protected by that card. Furthermore, it could enable an unauthorized person to electronically masquerade as you.

While the FORTEZZA/FFC card does employ a Personal Identification Number (PIN) to prevent use of the card by unauthorized parties, no PIN-based system is absolutely foolproof. You should, therefore, take precautions to protect your cryptographic card and PIN from loss or theft.

Loss, attempted theft, or any similar possible compromise of your cryptographic card or PIN must be reported to your Certification Authority (CA) or local registration authority.

By signing and returning this form to your CA, you agree to the following terms:

"I have read this statement and acknowledge receipt of the FORTEZZA/FFC card identified by serial number below, the associated PIN, and certificates noted on the PIN letter. I also agree to abide by the requirements of NSTISSI No. 3028, "Operational Security Doctrine for the FORTEZZA User PCMCIA Card" which was made available to me**."**

Card Serial Number: _____

Received by (printed name): _____

Signature: _____

Date: _____

* FORTEZZA is a registered trademark of the National Security Agency.

ANNEX D

METHODS FOR TRANSPORTING THE PROGRAMMED
FORTEZZA CARD (KOV-11)

1. Programmed KOV-11s may be transported within the U.S., its territories and possessions by:

a. the authorized user to whom the card is issued;

b. a designated U.S. Government courier;

c. the U.S. Postal Service (USPS) registered mail providing the material does not, at any time, pass out of U.S. control, pass through any foreign postal system, or be subject to any foreign postal inspection; or

d. a commercial shipping firm that meets the following criteria:

(1) incorporated in the U.S. and provides door-to-door service;

(2) guarantees delivery within a reasonable number of days based on the distance to be traveled;

(3) has a means of tracking individual packages within its system to the extent that, should a package become lost, the carrier can, within 24 hours following notification, provide information regarding the package's last known location;

(4) guarantees the integrity of the vehicle's contents at all times; and

(5) guarantees that the package will be afforded a reasonable degree of protection against theft (e.g., use of a security cage, video surveillance, etc.) should it become necessary for the carrier to make a prolonged stop at a carrier terminal.

2. Programmed KOV-11s may be transported outside the U.S., its territories and possessions in accordance with paragraph 1 of this annex, with the following additional restrictions:

a. USPS registered mail may be used to ship FFC cards to/from locations overseas, but only if the location is serviced by a Fleet Post Office (FPO) or Army/Air Force Post Office (APO) that is authorized to process USPS registered mail.

b. To the maximum extent possible, material shipped to/from locations outside the U.S., its territories and possessions should remain under continuous U.S. control. Although some limited handling of the material by foreign nationals may be unavoidable during aircraft loading and unloading operations, the material must be returned to U.S. control upon completion of these operations. Should the material subsequently show evidence of unauthorized access or tampering, a report should be filed in accordance with paragraph 42 of this document.

ANNEX E

THE USE OF THE FFC CARD TO SEPARATE COMPARTMENTED DATA

1. TS/SCI Network - The DAA for a TOP SECRET system handling sensitive compartmented information (SCI) (including various releasability caveats) and/or Special Access Required (SAP/SAR) information may, with the data owner's concurrence, approve the use of the FFC to separate and control access to that information. An electronic central Access Control List (ACL) for the compartment is established and maintained by the compartment's or program's Control Officer, and FORTEZZA provides Identification and Authentication of the individual users who are authorized access to the compartmented program. This technique employs the unique electronic "personality" (i.e., certificate) of the user stored in the FORTEZZA card as a positive method of identification. Access to SCI or SAP/SAR is controlled by either:

a. using FORTEZZA identification and authentication to verify a user against the ACL prior to allowing the user access to SCI or SAP/SAR information; or

b. having the sender and receiver of SCI or SAP/SAR information verify each other's personality against the ACL prior to exchanging the information.

2. SECRET or TOP SECRET Network - The FFC card may be used to enforce releasability caveats and need-to-know within a SECRET approved system or network (e.g., SECRET Internet Protocol Router Network (SIPRNET)) or a TOP SECRET approved system or network. This application of FFC must be approved by the DAA for the system. An electronic central Access Control List (ACL) for the caveat or need-to-know control is established and maintained by the cognizant authority, and FORTEZZA provides Identification and Authentication of the individual users who are authorized access to the information. Access to the need-to-know information is enforced by either:

a. using FORTEZZA identification and authentication to verify a user against the ACL prior to allowing the user access to the information; or

b. having the sender and receiver of compartmented information verify each other's personality against the ACL prior to exchanging the need-to-know information.