



AIR FORCE PUBLIC KEY INFRASTRUCTURE SYSTEM PROGRAM OFFICE

SIPRNET HARDWARE TOKEN



SAMPLE



A new smart card, known as a *hardware token*, is being evaluated for use on the Secret Internet Protocol Router Network (SIPRNet).

Similar to the CAC, the SIPRNet token contains individual PKI certificates used for network logon, Web site authentication, and secure e-mail.

The Air Force plans to issue the token to valid SIPRNet account users beginning mid-2011.

TOKEN BENEFITS

- ◆ **Higher security posture on DoD SIPRNet**
 - Facilitates smart card logon for a more robust method of authentication; eliminates the need for usernames/passwords
- ◆ **More efficient for the warfighter**
 - Users can securely carry credentials from location to location

TOKEN FEATURES

- ◆ **A smart card**
 - Microchip is encoded with PKI certificates issued by the National Security System (NSS) Certification Authority (CA)
- ◆ **A distinctively different token**
 - Neither a CAC nor an Alternative Token
- ◆ **Not an ID card**
 - Does not facilitate common access
 - Contains no photo, printed data, bar codes, or biometrics



The AF PKI SPO is a component of the Cryptologic Systems Division, Information Assurance Branch, Public Key Infrastructure Section (ESC/HNCDP), located on Lackland AFB, TX. Phone: 210-925-2562 / DSN: 945-2562



SIPRNET HARDWARE TOKEN FACTS

- ◆ **A high-value, UNCLASSIFIED item when removed from the SIPRNet card reader**
 - Only considered CLASSIFIED (to the level of the workstation in which it is used) when inserted into a SIPRNet card reader (attached to a DoD SIPRNet workstation) **AND** when successfully unlocked with the associated PIN
- ◆ **Issued by a NSS-certified Local Registration Authority (LRA)**
 - Not obtained at a personnel center or other CAC issuance facility
- ◆ **Specific use cases**
 - Smart card logon to the DoD SIPRNet
 - Applying PKI security services of authentication, data integrity, encryption, and non-repudiation to classified e-mail
- ◆ **Controlled item**
 - Users must return it to an NSS LRA upon PCS, separation, retirement, or changes in duty that no longer necessitate a need for the token
- ◆ **Reusable**
 - Non-personalized card can be securely re-initialized and reissued
- ◆ **Not an identification card**
 - Cannot be used to access military installations or secure facilities
- ◆ **Uses different resources**
 - The unique microchip architecture functions with specified card readers and middleware different from those used on unclassified networks; mitigates risk of cross-domain compromise



SECURITY MEASURES AND USER RESPONSIBILITIES

- ◆ **Protect the SIPRNet token with the same diligence as the CAC**
 - Do not leave the SIPRNet token unattended in a card reader connected to a SIPRNet workstation
 - Maintain positive control, and keep it out of possession of unauthorized users. **IT IS NOT TO BE SHARED!**
- ◆ **Do not use the SIPRNet token, CAC, or Alternative Token on unauthorized workstations**
 - Introduction of the SIPRNet token into unclassified environments is not authorized. Likewise, introduction of unclassified tokens into the SIPRNet environment is not authorized. Either incident may result in a reportable security violation (*per CNSS-014-2011 Decision Memorandum: Approval of Continued Use of SC650 Token, 17 Feb 11*)
 - ◇ If the SIPRNet token is accidentally inserted into a card reader connected to a NIPRNet workstation, do not enter the PIN and remove it immediately; entering the PIN may result in a security violation where the token must be returned to an LRA for revocation and the incident reported to a security manager for investigation
 - ◇ If a CAC or Alternative Token is accidentally inserted into a card reader connected to a SIPRNet workstation, do not enter the PIN; remove it immediately.

LEARN MORE

For additional information, visit:

AF PKI SPO Web Site:

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

Your Key to Information Assurance

Your Air Force | Your Country | Your World | Your PKI

