Air Force Public Key Infrastructure
System Program Office (ESC/HNCDP)
Phone: 210-925-2562 / DSN: 945-2562
Web: https://afpki.lackland.af.mil

Frequently Asked Questions (FAQs)
SIPRNet Hardware Token

Updated: March 2011

1. What is a "hardware" token?

In general, a security token is a physical device, typically small and portable, that acts like an electronic key to access computer services. It is used to electronically prove one's identity and may be used in place of or in conjunction with a password or personal identification number (PIN). The term "hardware" refers to token types where credentials are cryptographically encoded and stored on a dedicated hardware device, such as a smart card containing a microchip. This is in contrast to a "software" token, which stores credentials on general purpose electronic devices (e.g., a desktop, laptop, mobile device, and removable storage media). Credentials stored on hardware tokens cannot be exported and are only accessible via specialized software, called middleware, and a card reader connected to a computing device.

2. Why use a hardware token?

Hardware tokens provide a secure means of network authentication. In the DoD, PKI credentials stored on hardware tokens are protected by a user's personal identification number (PIN). When presented to a network device, the combined use of the hardware token (something you have) and the PIN (something you know) provides what is known as two-factor authentication, a method far more robust than just a username and password. Unlike the username/password method, use of hardware tokens avoid the possibility of passing clear-text passwords over the network, providing stronger assurance that login details are not captured and used illicitly.

3. What is the purpose of the SIPRNet hardware token?

The primary purposes of the SIPRNet hardware token are to provide trusted user identification and authentication on SIPRNet and to provide improved interoperability across the DoD enterprise through PK-enabled applications. Target applications include smart card logon to the SIPRNet, Web site authentication, and secure e-mail. Currently, authentication to the SIPRNet is accomplished with a username/password. This single-factor authentication method creates security gaps for users, and difficult password generation schemes, complex password rules, and the requirement to frequently change the password hampers the end user's ability to effectively use the network. Additionally, because the SIPRNet hardware token is populated with a full complement of PKI certificates (i.e., identity, e-mail signing, and e-mail encryption), it may be used to digitally sign and encrypt e-mail on the SIPRNet, thereby providing PKI assurances of identification, data integrity, non-repudiation, and confidentiality to electronic transactions.

4. Is the SIPRNet hardware token a classified item?

Yes and no. The SIPRNet hardware token architecture is uniquely designed to be classified (to the classification level of the workstation in which it is used) **only** when it is inserted into a SIPRNet card reader attached to a SIPRNet workstation ***AND*** when the user has unlocked it with the associated Personal Identification Number (PIN). The PIN is referred to as activation data. The token, therefore, is classified only when the hardware and software come together in concert with activation data, thereby allowing the SIPRNet hardware token to be UNCLASSIFIED when removed from the card reader. This enables the user to securely carry their credentials from location to location without special requirements. To the warfighter, this is especially advantageous during highly mobile missions and in operations where securing a credential is impractical and a burden on their ability to rapidly respond to the mission. Another benefit of a secure, portable hardware token is that the warfighter's credentials are always available for use.

5. What are the PIN rules for the SIPRNet hardware token and how often do I have to change the PIN?

The PKI credentials encoded in the microchip of the SIPRNet hardware token are protected by a personal identification number (PIN); not a password. The 8-16 digit numeric PIN is chosen by and known only to the token holder. The PIN is encoded and stored only in the token's microchip; it is not cached, stored in a database on the network, or to be shared with anyone else. Currently, policy considers the PIN to be classified and does not require the PIN to be changed unless it has been compromised, but the user can easily change the PIN at their discretion from their SIPRNet workstation.

6. Which PKI certificates are on the SIPRNet hardware token?

The SIPRNet hardware token contains three PKI certificates: the Identity certificate and the E-mail Signing certificate, both of which facilitate the PKI assurances of identification and authentication, data integrity, and non-repudiation; and the E-mail Encryption certificate, which facilitates confidentiality. The Identity certificate is also used for smart card logon to the SIPRNet.

The PKI certificates on the Common Access Card (CAC) and the Alternative Token are issued by Department of Defense (DoD) Medium Assurance PKI Certification Authorities (CAs). They are for use on unclassified systems only. The PKI certificates on the SIPRNet hardware token, however, are issued by the National Security System (NSS). NSS CAs are approved by the National Security Agency to issue PKI certificates for use on DoD classified systems.

7. Who is issued a SIPRNet hardware token?

The SIPRNet hardware token is only issued to users who have a valid e-mail account on the SIPRNet and an active "smil.mil" e-mail address.

8. How do SIPRNet account users obtain a hardware token?

Unlike the Common Access Card (CAC), the SIPRNet hardware token is not issued at a personnel center or other CAC issuance facility; however, issuance does employ a secure version of the Defense Eligibility Enrollment Reporting System (S-DEERS) to obtain the user's personal identification information. The user's identity information is then bound to the PKI certificates to facilitate identification, authentication, and non-repudiation. A Local Registration Authority (LRA) obtains the user's identity information via a dedicated workstation.

The vast majority of SIPRNet account users will obtain their token through an LRA-managed kiosk workstation described above. The LRA verifies the user's identity face to face and initiates the enrollment process. The LRA issues the token, provides the user a one-time password, and then directs the user to a kiosk workstation to complete the enrollment and set their 8-16 digit numeric PIN.

SIPRNet account users at smaller, geographically separate locations may receive their tokens through a centralized issuance process via a remote Trusted Agent (TA). The TA verifies the user's identity face to face and submits a token request to an LRA. The LRA issues the token, and then securely ships the token and sends an initial PIN via encrypted e-mail to the TA. The TA distributes the token and PIN to the SIPRNet account user, who is then required to change the PIN. The centralized issuance process may take 10 business days or more to complete.

9. How is the SIPRNet hardware token similar to or different from the CAC and Alternative Token?

The SIPRNet hardware token is a new token in the hardware token inventory. It is a separate card, distinct from the Common Access Card (CAC) and the Alternative (Alt) Token. However, the SIPRNet hardware token is like both the CAC and Alt Token in that it is also a hardware token cryptographically encoded with PKI credentials that are used for secure e-mail and smart card logon to a DoD network. That's where the similarities end.

The CAC and Alt Token are for unclassified use only and are populated with PKI certificates issued by DoD Medium Assurance PKI Certification Authorities (CAs). The SIPRNet hardware token is for use on the SIPRNet only and uses PKI certificates issued by the National Security System (NSS) CA. NSS CAs are approved by the National Security Agency to issue PKI certificates for DoD classified systems.

Additionally, the CAC is the DoD identification card. The SIPRNet hardware token does not have a photo of the card holder, does not include printed personal data (not even the name of the card holder), contains no biometrics, and does not have bar codes. As such, it cannot be used as an identification card of any kind or used to access military installations or secure facilities, and it cannot be used at facilities that rely on bar code data for identification purposes to access sensitive records, such as at medical and personnel facilities. Since the SIPRNet hardware token does not facilitate common access, it is NOT referred to as a SIPRNet CAC.

10. Can the SIPRNet hardware token be used as an ID card?

No, the SIPRNet hardware token cannot be used as an identification card of any kind or used to access military installations or secure facilities. It does not have a photo of the card holder, does not include printed personal data (not even the name of the card holder), contains no biometrics, nor does it have bar codes, so it may not be used at facilities that rely on bar code data for identification purposes, such as at medical and personnel facilities.

11. When will the token be available to SIPRNet account users?

1 March through 15 April 2011, the Air Force will participate in activities in support of DoD's Initial Operational Test and Evaluation (IOT&E). During the IOT&E, DoD components will evaluate token issuance, management, and usage at select locations and collect valuable information toward full production. Under the current schedule, the Air Force will begin issuing tokens to all SIPRNet account users during the Initial Operational Capability (IOC) in mid-2011. Full Operational Capability (FOC) is projected by the end of 2012.

12. What type of equipment do I need on my SIPRNet workstation to use the token?

The SIPRNet hardware token microchip is set to a voltage level different from the Common Access Card (CAC) and Alternative Token. Therefore, to leverage the unique design features and secure architecture of the SIPRNet hardware token, SIPRNet workstations must be equipped with an approved card reader and reader driver compatible with the SIPRNet hardware token **AND** must have an approved middleware loaded. The only approved reader is the Omnikey 3121 reader, which must be ordered through the Air Force PKI SPO. The 90-Meter Smart Card Manager (SCM), a client-based application that provides token use services for smart card logon, secure e-mail, and Web site authentication, is the approved middleware for SIPRNet user workstations. 90meter Certificate Issuance Workstation, a client-based application that formats,

enrolls, and resets and unblocks PINs on the SIPRNet token, is the approved middleware for LRA workstations. **NOTE:** ActivClient 6.2 Air Force Release (AFR) middleware installed on NIPRNet workstations is **NOT** approved for use with the SIPRNet hardware token.

13. What should I do if the SIPRNet hardware token is lost or stolen?

The SIPRNet hardware token should be considered and treated like a high-value, unclassified item; protect it as you do the Common Access Card (CAC). In other words, don't leave it unattended in the SIPRNet card reader, and keep it out of possession of unauthorized users. In fact, it's highly recommended that the user keep it in their control at all times. If it is lost or stolen, do not report it to the personnel facility or other CAC issuance location. The user must report it as soon as possible to a Local Registration Authority (LRA), Trusted Agent (TA), or the Air Force Registration Authority (RA) to initiate certificate revocation and token reissuance. This action renders the lost/stolen card useless to anyone who may find it or try to use it for illicit purposes.

14. Can the SIPRNet hardware token be reused/reissued?

Yes. Because the face of the token is not personalized, it can be recycled, providing a significant cost benefit to the DoD. When a SIPRNet hardware token user no longer needs the card or is permanently transferred to a new location, they are required to return it to a Local Registration Authority (LRA) or Trusted Agent (TA), who then requests certificate revocation and reinitializes the token. The re-initialization process eliminates encoded data from the microchip and prepares the card for issuance to another user.

15. What happens if I inadvertently insert the SIPRNet hardware token into a card reader connected to a NIPRNet workstation?

Introduction of SIPRNet tokens on unclassified workstations is not authorized. If a SIPRNet token is inserted into an unauthorized workstation, do not enter the PIN. If the PIN is entered, it is a potential security violation. In such instances, the token shall be returned to an NSS LRA where the certificates will be revoked, and the incident shall be reported to the local information security officer for investigation.

(Ref: CNSS-014-2011 Decision Memorandum, Approval of Continued Use of SC650 Token, 17 Feb 11)

16. What happens if I inadvertently insert my CAC into a card reader connected to a SIPRNet workstation?

Introduction of NIPRNet tokens (i.e., CAC and Alternative Token, PIV, or PIV-I) on SIPRNet is not authorized. When properly configured on SIPRNet workstations, domain middleware only reads SIPRNet tokens; therefore, inserting a NIPRNet token into a card reader connected to a SIPRNet workstation is not a security violation unless it is apparent the NIPRNet token becomes active (by the entrance and acceptance of the token PIN). Correctly configured middleware would detect the NIPRNet token as unauthorized and block PIN entry as well as block any service applets that don't require PIN entry.

Middleware that is not properly configured on a SIPRNet workstation is not capable of blocking activation; therefore, introduction of a NIPRNet token into the SIPRNet is a potential security violation, regardless of whether the PIN is entered. Such instances shall be reported to the local information security officer and the incident investigated to determine if classified data was written to the token or if malicious code was introduced into the network.

(Ref: CNSS-014-2011 Decision Memorandum, Approval of Continued Use of SC650 Token, 17 Feb 11)

17. Why isn't the SIPRNet token classified after using on SIPRNet workstation?

Due to the uniquely-designed SIPRNet hardware token architecture and card operating system, the National Security Agency (NSA) determined sufficient security capabilities are provided and released the following statements: “The token is considered a high-value unclassified item. It should be maintained in the user's possession at all times;” and “The token is classified Secret when unlocked and in use and is considered unclassified when removed from its reader and not in use.”

(Ref: CNSS-014-2011 Decision Memorandum, Approval of Continued Use of SC650 Token, 17 Feb 11)

18. When will the SIPRNet token and CAC be merged into one token to be used on either NIPRNet or SIPRNet workstations?

Providing all the Common Access Card (CAC) capabilities and the SIPRNet hardware token capabilities in a single token with appropriate separation is not yet available from industry at an affordable price. The requirement for a single token is in the DoD PKI Increment 2 Capability Development Document (CDD) Key Performance Parameters (KPP) as an objective requirement. Currently, the SIPRNet hardware token is a capability requirement in Increment 2, Spiral 1; a token capable of supporting more than one domain will be addressed in a later spiral and evaluated as the technology evolves.

19. What is the difference between the SIPRNet hardware token microchip and the CAC microchip?

The SC650 microchip on the SIPRNet hardware token and the microchip on the Common Access Card (CAC) are different physical architectures. This difference and the difference in the token’s operating system permit the use of the SC650 token as a SIPRNet token.

20. Can a SIPRNet card reader be connected to a NIPRNet workstation for use with the CAC?

Yes; with the appropriate middleware and drivers, a SIPRNet card reader can technically be used on a NIPRNet workstation, but this is neither advised nor supported.

21. Can a card reader used on a NIPRNet workstation be connected to a SIPRNet workstation for use with the SIPRNet hardware token?

Possibly; certain card readers with appropriate middleware and drivers installed on the SIPRNet workstation ***may*** work. However, card readers used on NIPRNet workstations are not authorized for use on SIPRNet workstation. In addition to evaluating various tokens and different vendors’ middleware during the pilot and operational assessment, card readers were also extensively tested and evaluated. They will be evaluated further during the Initial Operational Test and Evaluation (IOT&E) scheduled for early part of 2011. In preparation for the initial deployment of SIPRNet hardware tokens to Air Force SIPRNet account holders, approved card readers for the SIPRNet will be provided by the DoD PKI Program Management Office.

22. Why does the SIPRNet hardware token use a different middleware than the CAC?

ActivClient middleware is not authorized for use with the SIPRNet hardware token. One reason is the microchips on the SIPRNet hardware token and the Common Access Card (CAC) are of different architectures. 90-Meter Smart Card Manager (SCM), a client-based application that provides token use services for smart card logon, secure 2-mail, and Web site authentication, is the approved middleware for user workstations. 90meter Certificate Issuance Workstation, a client-based application that formats, enrolls, and resets and unblocks PINs on the SIPRNet token, is the approved middleware for LRA workstations.

23. What if I forget the SIPRNet hardware token PIN or lock the token? Can I reset the PIN at a CAC PIN Reset workstation?

CAC PIN Reset workstations do not support the National Security System (NSS) PKI-issued certificates encoded on the SIPRNet hardware token. If you forget your SIPRNet hardware token PIN or you inadvertently lock the token by entering the PIN erroneously five consecutive times, you must report to a NSS-certified Registration Authority, Local Registration Authority, or designated Trusted Agent. If the PIN is known, but you simply wish to change it, the 90-Meter Smart Card Manager (SCM) middleware installed on your SIPRNet workstation supports a PIN-change function. You can do this yourself without the assistance of outside personnel.

24. Does setting the SIPRNet Active Directory account to Smart Card Logon "enabled" allow only username/password OR only smart card authentication, or will it allow either method of authentication?

If an account is simply "enabled" for smart card logon (SCL) (i.e., the user logon name is populated with the EDI-PI and the domain is changed to @smil.mil), then a user can either log on with a username and password or with a smart card without restrictions **UNLESS**: 1) Administrators, when configuring the network, check the option "Smart card is required for interactive logon" and then uncheck it. This results in the system resetting the user's password to a 256-character password that the user does not know; thus he/she is unable to logon with a username and password; or 2) Administrators set a local policy at the workstation that requires smart card logon. In either of those two cases, users may not continue to log onto the SIPRNet with their username and password.

During the IOT&E, the SIPRNet at participating organizations' location will be "enabled" for SCL so that SIPRNet hardware token usage can be properly evaluated, yet still allow non-IOT&E participants to conduct business as usual.