Summer 2011

The KEY2PKI

Network Access Made Easy and Secure with the New SIPRNet Hardware Token

Are you tired of managing complex usernames and passwords for access on the Secret Internet Protocol Router Network (SIPRNet)? The new SIPRNet hardware token makes logon to the SIPRNet as easy as logon to the Non-classified Internet Protocol Router Network (NIPRNet).

Air Force members from select units and combatant commands are already using the new smart cards, as participants in DoD's SIPRNet hardware token Initial Operational Test and Evaluation (IOT&E). The IOT&E is a limited fielding phase that began 1 March and continues DoD-wide through fall 2011. The rest of the Air Force will begin to see SIPRNet hardware tokens available by the end of 2011.

Are you interested in getting your own SIPRNet hardware token? Here's what you need to know first.

What is a SIPRNet hardware token? The SIPRNet hardware token, for exclusive use on the SIPRNet, is a separate and distinct card from a CAC and Alternative Token, and cannot be used as an ID card. It leverages Public Key Infrastructure (PKI) certificates to make the way you work on the SIPRNet as convenient as conducting business on the NIPRNet. For example, the SIPRNet hardware token gives you the ability to:

- Log on to DoD classified networks with the token and a Personal Identification Number (PIN)
- Authenticate to restricted Web sites
- Digitally sign and encrypt e-mail

Am I eligible for a SIPRNet hardware token? The SIPRNet hardware token is only issued to users with a valid account on the SIPRNet and an active "smil.mil" e-mail address.

Where can I get a SIPRNet hardware token? You will be scheduled to receive your token in the near future. The SIPRNet hardware token will be issued by your National Security Systems (NSS)-certified Local Registration Authority (LRA). SIPRNet hardware tokens will *not* be available from DEERS/RAPIDS stations, where CACs are issued. Find your designated NSS-credentialed LRA at: https://afpki.lackland.af.mil/html/lracontacts.cfm.

How do I use the SIPRNet hardware token? Once your network and terminal are enabled, use of the SIPRNet hardware token is similar to use of the CAC on unclassified networks. Simply insert it into the designated card reader installed on your SIPRNet terminal (pictured on back page) and enter your SIPRNet hardware token PIN. The SIPRNet hardware token contains three PKI certificates, which allow it to operate like the CAC: the Identity certificate, the E-mail

INSIDE

Continued on Back Page

HTTPS://AFPKI.LACKLAND.AF.MIL

Calling All Air Force LRAs: Get Your NSS Credential Today!

Local Registration Authorities (LRAs) play a critical and valued role in network security and information assurance as the issuers of multiple types of DoD Public Key Infrastructure (PKI) certificates. The introduction of the SIPRNet hardware token (see pages 1, 4 for additional details) has added an important, new smart card to the network defense arsenal, which LRAs will also issue. **Due to evolving network security and credential issuance requirements, all LRAs trained *prior* to August 2010 must obtain the new National Security Systems (NSS) certification to be able to issue the SIPRNet hardware token.** LRAs trained *after* August 2010 are already NSS-credentialed, as pertinent training was incorporated into the LRA class during this period.

What is NSS? There are currently two different PKI infrastructures actively supporting the SIPRNet. The infrastructure in place until recently issues certificates under the DoD X.509 Certificate Policy in both unclassified and classified domains. The new federally mandated PKI infrastructure for the SIPRNet, referred to as the National Security Systems (NSS), issues certificates in the classified domain only, which includes the SIPRNet hardware tokens. While both infrastructures can process Non-Person Entity (NPE) Secure Sockets Layer (SSL) Device Certificates, NSS PKI is the preferred source, as issuance of certificates in the classified domain under the DoD X.509 certificate policy will diminish over time as migration to the NSS infrastructure occurs.

How do I get NSS credentialed? Are you already an LRA? Remember, LRAs trained *after* August 2010 should already be NSS qualified. If you received your LRA training and appointment *prior* to August 2010, obtaining your NSS credential is a simple process. It involves face-to-face validation, updating your documentation, and completing a quick and easy 30-minute Web-based training course. Once your training is complete, send a copy of the course completion certificate to the AF Registration Authority (RA). You will then receive your credentials.

For additional details, visit:
https://afpki.lackland.af.mil/html/lra_trg.cfm.

To find NSS-credentialed LRAs at your base, check out the Air Force published list at:
https://afpki.lackland.af.mil/html/lracontacts.cfm.

Interested in becoming a *new* LRA? Check out the links above for requirements, which include a Designation Letter, LRA Affidavit, security vetting, and on-site training.

> "Just like with the CAC, migrating away from lengthy, complex passwords to a token and a PIN will be a welcomed change for SIPRNet users."
>
> Colonel Christopher Kinne
> Chief, Cryptologic Systems Division

New AF Baseline Middleware

ActivClient (AC) v6.2 Build 119 Air Force Release (AFR) is the new baseline middleware for the Non-classified Internet Protocol Router Network (NIPRNet).

Much like the previous release (Build 101), AC v6.2 Build 119 enables critical middleware features to function with Microsoft Outlook 2010, and supports both 32 and 64-bit systems. Benefits include automated publication of PKI certificates to the Air Force Global Address List (GAL) for Outlook 2010, and automated updates to users' Microsoft Outlook security profiles with their PKI certificates. Build 119 additionally resolves Logon and Unlock Errors discovered in Build 101.

System Administrators should note that ActivClient v6.2 Build 119 is not included in forthcoming Standard Desktop Configurations (SDCs) 3.2 and 2.6, and take action in accordance with MTO 2011-165-002.

For additional details, check out the AF PKI SPO Knowledge Base, Article 423, at:
https://afpki.lackland.af.mil/html/kbsearch.cfm.

CPR to Support MS Windows Vista

Attention CPR Trusted Agent Security Managers (TASMs) and CPR Trusted Agents (CTAs): A critical update is on its way for your Common Access Card (CAC) Personal Identification Number (PIN) Reset (CPR) workstation.

CPR v2.2, to be released the end of the summer, allows you to reset CAC PINs from a workstation running the Microsoft Windows Vista Operating System (OS). Be sure to see your System Administrator to upgrade your workstation (reserved exclusively for CPR) to the Air Force Standard Desktop Configuration (SDC) 2.x, running Windows Vista. The update allows you to take advantage of the latest CPR software upgrades, and provide ongoing support to those needing to reset their CAC PINs.

Watch for additional information at:
https://afpki.lackland.af.mil/html/cpr.cfm.

GOT MULTIPLE SMART CARDS? SMART CARD LOGON / NEXT GENERATION TO MINIMIZE NEED FOR ALTERNATIVE TOKENS

Do you have multiple smart cards to log on to Air Force networks? Would you love to be able to log on to the network with a single card that enables all of your accounts, access rights, and permissions? Smart Card Logon / Next Generation (SCL/NG) is evolving technology that will soon empower you with the ability to log on to more than one unclassified network account with a *single* card.

Smart cards, including Common Access Cards (CACs) and Alternative (Alt) Tokens, contain PKI certificates and functions for network logon. Existing technology, however, has not fully accommodated network users with *multiple* accounts within the *same* Active Directory forest. Up to this point, Active Directory only allows *one* CAC to log on to *one* network account within an Active Directory forest. This scenario frequently affects individuals like network administrators, Client Support Administrators, Help Desk personnel, and Air Force medical staff. Alt Tokens were developed, as a short term solution, for specific use cases to overcome this limitation.

Alt Tokens, however, are cumbersome for users and costly to the Air Force. With the advent of SCL/NG, in conjunction with Windows 2008 Server-based Active Directory and Windows Vista (and later) operating systems, Alt Token requirements will be dramatically reduced, even eliminated, for many use cases.

What does SCL/NG mean for you? When you, an Air Force network user, currently log on to your Air Force standard desktop with your primary network account, you are actually logging on with your DoD E-mail Signature Certificate on your CAC. The capability to log on to multiple accounts with the same CAC will be enabled by SCL/NG. SCL/NG will be rolled out in two phases:

- SCL/NG Phase 1: The Personal Identity Verification (PIV) Certificate on you CAC will be used to log on to a single alternate account
  (e.g., Administrator Account)
- SCL/NG Phase 2: The DoD Identity Certificate on the CAC will be used to log on to as many accounts as you require (e.g., group and role based accounts)

What will SCL/NG look like on your Air Force computer? Most can expect to experience SCL/NG Phase 1 roll-out at an unclassified Air Force desktop near you by the end of 2011. When logging on to your Air Force desktop with your CAC, you will likely see two PKI certificates displayed; one that's your DoD E-mail Signing Certificate, and one that's your DoD Identity Certificate. Select your E-mail Signature Certificate to successfully log on to your workstation. Should you accidently select the DoD Identity Certificate, logon in most cases will fail, and you'll have an opportunity to then choose your E-mail Signature Certificate.

How can you tell the difference between your two certificates? You may notice from the above image that both certificate icons appear identical. Your DoD E-mail Signing Certificate will be on the left in most cases. To verify, select the certificate, and you will be prompted for your CAC Personal Identification Number (PIN), as pictured below. If your User Primary Name (UPN), circled in red, is followed by "@mil," you have successfully selected your E-mail Signing Certificate. If instead you see a relatively lengthy amount of information, you have chosen the Identity Certificate. Click *Switch User* to go back and select the E-mail Signing Certificate.

What makes SCL/NG such a benefit for the Air Force? SCL/NG delivers tremendous cost AND manpower savings associated with procuring, issuing, shipping, distributing, managing, and recovering thousands of smart cards. Secondly, for Alt Token users, there is the convenience of not having to manage multiple tokens. There is a security benefit, as well. Compromise or loss of an IT administrator Alt Token, for example, can have serious consequences, as it requires immediate revocation of the PKI credential and could possibly result in the affected administrator's account being disabled.

SCL/NG implementation on the *SIPRNet* is currently under consideration for the near future. Stay tuned for updates and additional information at https://afpki.lackland.af.mil.

CONTINUED FROM PAGE 1

NETWORK ACCESS MADE EASY AND SECURE WITH THE NEW SIPRNET HARDWARE TOKEN

Signing certificate, and the E-mail Encryption certificate.

Is the SIPRNet hardware token a classified item? Yes and no. The SIPRNet hardware token architecture is uniquely designed to be classified ***ONLY*** when it is inserted into a SIPRNet card reader attached to a SIPRNet workstation (pictured right), ***AND*** when the user has unlocked it with the associated 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. As a result, the SIPRNet hardware token is UNCLASSIFIED when removed from the card reader. This allows you to securely carry your SIPRNet hardware token from location to location without special requirements.

Do I have any responsibilities with the SIPRNET hardware token? The token is considered a high-value unclassified item and should be maintained in your possession at all times. All Air Force members operating in both classified and unclassified environments must also take caution and ensure use of the correct smart card for the correct environment. The SIPRNet token is not authorized for use on the unclassified network. Conversely, the CAC is not to be used on the classified network. Introduction of an unclassified token, to include a CAC or Alternative Token, into a classified environment may result in a security violation, subject to reporting and investigation. Likewise, inserting a SIPRNet token into an unclassified system could also lead to a security violation. The good news is that a technical security control exists, known as "domain aware middleware," to help us all avoid using the wrong Smart Card in the wrong system.

For additional information, visit the AF PKI SPO SIPRNet Initiatives page at: https://afpki.lackland.af.mil/html/siprnet.cfm.

CHANGES TO THE AF PKI COP

Effective 23 March 2011, a great deal of content was removed from the Air Force PKI Community of Practice (CoP) as part of the overarching Air Force Knowledge Now migration. Air Force PKI Training, however, remains available exclusively on the Air Force PKI CoP for credentialed Local Registration Authorities (LRAs) who require NSS SIPRNet upgrade training, and those assigned to fulfill duties as a CAC PIN Reset TASM or CTA.

REMINDER! You can always find Air Force PKI information, tools, downloads, and other solutions on the AF PKI SPO Web Site. Visit us today at https://afpki.lackland.af.mil.

RESOURCE CENTER

AF PKI SPO WEB SITE
https://afpki.lackland.af.mil

AF PKI COP ON THE NIPRNET
https://afkm.wpafb.af.mil/pki
For all of your Air Force PKI Training needs!

AF PKI COP ON THE SIPRNET
https://afkm.wrightpatterson.af.smil.mil/pki

AF PKI HELP DESK
Phone: 210-925-2521
DSN: 945-2521
E-mail: afpkihelpdesk@us.af.mil

AF PKI TOOLBOX
DOWNLOADS
https://afpki.lackland.af.mil/html/downloads.asp

TOOLS, SCRIPTS, & UTILITIES
https://afpki.lackland.af.mil/html/scriptsutils.asp

AF PKI KNOWLEDGE BASE
https://afpki.lackland.af.mil/html/kbsearch.cfm
RECENT POSTINGS:

#422 UMP/PIP ERROR: UMP -1020: An incompatibility exists with your browser/JRE and ActivClient middleware installed

#410 INFORMATION— Home Use (Personal) CAC Options for Air Force Users

MTOS
MTO 2011-066-003 (8 MARCH 2011)
SIPRNet Smart Card Logon (SCL) Configuration Change (Domain Controller and Workstation

MTO 2011-066-003A (26 MAY 2011)
Updated SIPRNet Smart Card Logon (SCL) Configuration Change (Domain Controller, Workstation, and Active Directory)

MTO 2011-165-002 (14 JUNE 2011)
Upgrade of ActivClient (AC) v6.2 Air Force Release (AFR) Smart Card Middleware Baseline to Build 119

"THE KEY TO PKI" is published quarterly with the approval of the AF PKI SPO Program Manager. Direct questions or comments to the AF PKI Help Desk or to pki.outreach@us.af.mil. The AF PKI SPO (ESC/HNCDP) is the Public Key Infrastructure Section of the Information Assurance Branch, Cryptologic Systems Division, Hanscom Cyber/Netcentric Directorate, Lackland AFB, TX.