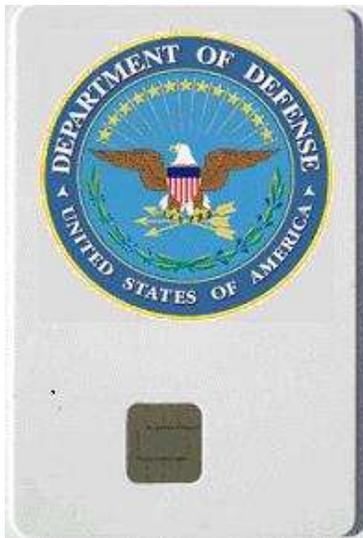


The PKE Quarterly Post

SIPRNET Hardware Token Pilot Begins

by Sam Schaen



SIPRNET users will soon be able to easily and securely use their software credentials on any machine, using a SIPRNET Hardware Token like the one pictured above.

In the decade since its inception, the SIPRNET Public Key Infrastructure has issued a fraction of the number of certificates issued on NIPRNET. To date, approximately 55,000 certificates have been issued on SIPRNET. By comparison, nearly 50,000,000 certificates have been issued on the NIPRNET. Aside from the fact that there are fewer SIPRNET users, one other reason for this difference is that the process of obtaining and using certificates on SIPRNET has been cumbersome and lacking in flexibility. In August, the Department of Defense began the SIPRNET Token Pilot, an initiative aimed at greatly improving the way PKI software certificates are issued and used on SIPRNET.

Currently, only software credentials are available to SIPRNET users. A software credential consists of a private key and a corresponding certificate; it is securely stored on the user's desktop. The user can take his/her credential to another machine by exporting it to a storage medium such as a CD, but doing so involves several difficulties. First, the storage medium must be handled at the Secret level. Second, it takes several steps to perform the export and import processes. Third, a copy of the user's credentials exists on every machine to which the credential has been imported, creating potential security vulnerabilities.

For the SIPRNET Token Pilot, users' credentials will be stored on smart cards manufactured by SafeNet, Inc. The cards will have no customization when they are issued, except for the DoD logo and some printing on the reverse side. A

major benefit is that the card will be Unclassified when not inserted in a card reader and thus can be moved from place to place without the need to handle classified media.

The pilot will test three alternative forms of issuance: centralized, kiosk, and user desktop. With centralized issuance, a user will receive a token with certificates and keys already on the card from a Trusted Agent (TA). The user will need to sign a form acknowledging receipt of the token. A Personal Identification Number (PIN) to unlock the card will be sent directly to the user.

Except for location, the kiosk and user desktop processes are quite similar. The process starts with a face-to-face meeting between the user and the Registration Authority (RA)/Local Registration Authority (LRA) where the user can be properly validated with multiple forms of ID. Using his/her SIPRNET token for authentication, the LRA registers the user into the SIPRNET Token Pilot system. The authenticated user information is automatically retrieved from S/DEERS and populated into the LRA's registration form. The LRA reviews the information, submits the form and then prints the Certificate Request Information (CRI) which contains the user's unique Enrollment UserID and one-time password.

In This Issue

Microsoft PKE TIM to be held in January	2
Certificate Validation Checking for External Partners	3
Using CRLAutoCache: Creating Local CRL Caches	3
Next PKE TIM Agenda	3
The Non-Person Entity (NPE) Initiative	4
Using Your BlackBerry to Exchange Secure Email	5

In Every Issue

Notes from DoD PKE	2
Ask the Expert	2
RA/LRA/TA Corner	4
In the Pipeline	6
Latest Updates	6
Upcoming Events	6

Continued on Page 2



Ask the Expert

I am a network administrator for a contractor and want to ensure that our Outlook clients are performing revocation checking. What is the best way to perform revocation checking for these clients? Our network is not a DoD network.

The DoD PKE Team recommends that email clients should be configured to use Online Certificate Status Protocol (OCSP) for revocation checking. Although, the DoD PKI supports Certificate Revocation List (CRL) checking, this method presents challenges for DoD, as well as our external partners, due to the large size of our CRLs. Windows XP supports Certificate Revocation List (CRL) checking out of the box, but does not support OCSP natively. A plug-in is required to enable OCSP on Windows XP. Both CoreStreet and Tumbleweed provide plug-ins that enable OCSP checking for Outlook. There is a cost associated with these plug-ins, if your enterprise has not already negotiated an enterprise license.

Windows Vista has a native OCSP capability. However, the DoD's Robust Certificate Validation Service (RCVS) does not yet support Vista. The DoD PKE Team is working closely with DoD PKI to test and configure RCVS to support the Vista OCSP client.

If your network is unable to support OCSP, then we recommend that you locally cache CRL files on your network. CRLs can be cached by properly configuring network proxies or by establishing a local CRL cache. The DoD PKE Team has posted tools and guidance for CRL caching in our online knowledgebase: <http://iase.disa.mil/pki/pke>.

Thanks for asking,
PKE Expert

If you have a question or comment for the PKE Expert, please send it to PKE_support@disa.mil. Be sure to type "Ask the Expert" in the *Subject* field.

Notes from the DoD PKE

by Carmella Webster, PKE Team Lead

It's been a busy few months for the DoD PKE team.

I want to share with you the DoD PKE team's forward-looking focus and what you can expect to see from us in terms of expanded customer support. Our philosophy and operations will always center on the guiding principle of delivering excellent customer support. As of late, we have focused our energy and resources on answering the immediate needs of our customers: ensuring that the PKI supports the Operations tempo of the DoD. This mission critical support will not be diminished in any way and will remain a priority. However, we owe it to our customers to look to the future and to "prepare the battlefield" as PKI implementers and maintainers plan, design, and deploy a healthy and robust PKI. Specifically, we have two initiatives in our sights: Federal PKI interoperability (aka "Federal Bridge") and Identity Management in the Classified environment.

The DoD PKE team has been actively engaged in Federal Bridge activities. We see it as our role to assist DoD users in understanding this technology, the benefits it offers as well as the implications it presents. Over the last few months, we have focused on testing how well applications operate

on the cross-certificate trust model. Our goal is to present a realistic recommendation on how DoD should implement this trust model. In addition to testing, we volunteered to co-chair the Identity, Credential, and Access Management Logical Access Working Group (ICAM LAWG). Allison Scogin is leading this effort to produce logical access implementation guidance for the Federal Community. As an early adopter of logical access, DoD will be able to influence the final guidance by sharing lessons learned as well as policy and implementation recommendations.

On the horizon for the DoD PKE team is supporting the implementation of identity management enhancements on the SIPRNET. As details and specifications of the infrastructure evolve through pilot programs and architecture development, the DoD PKE team will support our customers with guidance that leverages the community lessons learned from our successful NIPRNET implementation. Our goal is to get out in front of the SIPRNET deployment by providing our customers with current situational awareness of the program's development and by distributing technical guidance to our customers to help you make informed plans and prepare for this new capability.

Continued from Front Page

As with the centralized issuance approach, the user will be required to acknowledge receipt of the token.

Upon inserting the card in the card reader, the workstation will automatically connect to the Token Pilot Certification Authority (CA). The CA will prompt the user for his/her one-time password and user ID. The user will also be asked to create a PIN. At that point, the keys and certificates will be generated. The token will then be ready for use.

Site-specific procedures may be required to register for applications such as certificate-based logon, email, or access to web servers requiring identification (similar to what is currently required for use of a CAC on the NIPRNET.)

The SIPRNET Token Pilot began in August 2009 and will include 2,500 users from ten CC/S/As. Existing RAs and LRAs will be recruited to create these tokens for users. Assuming the pilot is successful, limited production will start at the beginning of CY 2010. The DoD PKI anticipates the population of SIPRNET users with these tokens to reach 500,000 in the future.

PKE TIM with Microsoft Slated for January, Send Us Your Topic Requests



In January, the DoD PKE Team will hold a Technical Interchange Meeting (TIM) with Microsoft representatives. At these meetings, Microsoft learns more about the features DoD would like to see implemented in Microsoft's current and future products, and DoD gets an overview

of what's in development at Microsoft. In the past, these TIMs have led to increased support of functionalities critical to DoD, such as enhanced CAC support, improved PKI certificate selection at authentication prompts, and enhanced OCSP client capabilities.

To submit a topic for the upcoming Microsoft TIM agenda, send an email to pke_support@disa.mil with the subject line, "January PKE TIM with Microsoft."

Did you know...

...about the *JTF-GNO InfoSpot Mailing List*?

The JTF-GNO InfoSpot is a mailing list that informs technical leads throughout the CC/S/As of the latest developments in DoD IT infrastructure assurance]. Visit https://www.jtfgno.mil/misc/new_subscribe.htm#formSection to subscribe.

(NOTE: CAC/PKI certificates are required to access this Web site.)



DISA Deputy Director to Release Point Paper on Revocation Checking Guidance for External Partners

One of the most pressing issues facing the DoD Public Key Infrastructure (PKI) is managing the demand for Certificate Revocation List (CRL) checking throughout DoD CC/S/As and our external partners. The Department of Defense (DoD) network infrastructure is reaching near capacity during peak times due to the number of customer requests for CRLs. The size of the CRL files and the number of simultaneous connections attempting to download them during peak hours is putting a strain on Global Directory Service (GDS). This issue is having a negative impact on our ability to deliver this service efficiently, and could begin to cause a denial of service for users to some networks and applications.

The DoD PKE and GDS Teams are working together to address the bandwidth and availability challenges that GDS faces due to

CRL retrieval. One of these initiatives is to reach out to DoD external business partners to educate them on more efficient methods for revocation checking. DISA will soon release a memo to our business partners from the DISA Deputy Director, identifying the challenges and requesting assistance in this matter. A point paper entitled *DoD PKI Revocation Checking Guidance for External Partners* will be attached to the memo that identifies recommended guidance for our external partners.

If you have external partners that are having difficulties with revocation checking, then feel free to distribute the point paper. The point paper can be found on the DoD PKE Web site: <https://www.us.army.mil/suite/doc/18295718>.

Using CRLAutoCache to Locally Cache CRLs

What is CRLAutoCache?

CRLAutoCache is a tool developed by DoD PKE Engineering Support to help system administrators in the CC/S/As to better manage the way their organizations perform certificate validation checking. CRLAutoCache can be configured to pull Certificate Revocation List (CRL) data in multiple formats from multiple sources and to publish that data to web servers or to Lightweight Directory Access Protocol (LDAP) directory servers.

In environments that use Online Certificate Status Protocol (OCSP) for certificate validation, CRLAutoCache can download OCSP Pre-signed Proof Sets from the Robust Certificate Validation Service (RCVS) as a primary source of revocation data. In the event that a connection to RCVS cannot be made, the Global Directory Service (GDS) can be configured as a secondary source of revocation data.

Who should use CRLAutoCache?

Any system administrator, whether in a CC/S/A or DoD Federal or Industry Partner organization, should use CRLAutoCache to download and distribute the latest CRLs from GDS.

Why use CRLAutoCache?

Every day, GDS bears an enormous load as thousands of users in DoD and partner enclaves connect to GDS to download the latest CRLs during peak network traffic hours. The sheer number of simultaneous connections, combined with the ever-increasing size of the CRL files, clogs network bandwidth causing latency (delays) and unavailability for users on DoD and partner networks.

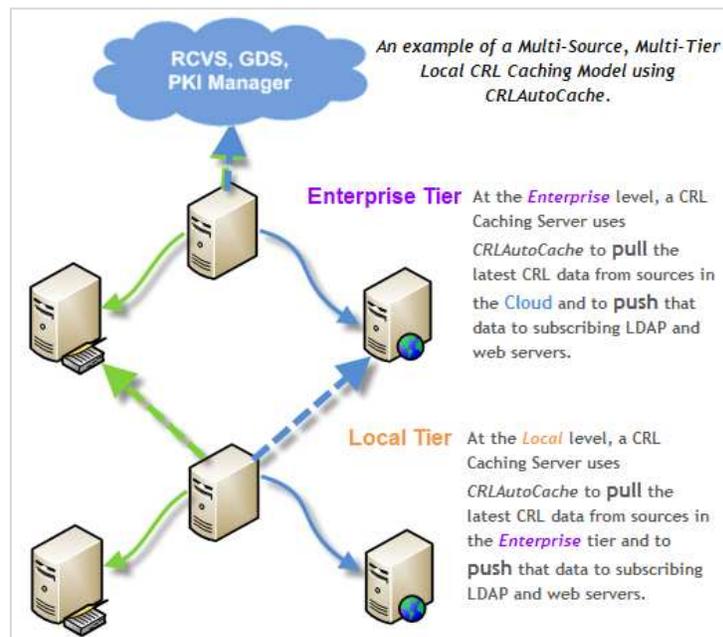
What is the latest version of CRLAutoCache?

CRLAutoCache was released in September

2009. In its latest version, CRLAutoCache now supports:

- Redundant retrieval sources so primary and backup sources can be used for fail-over.
- Dynamic HTTP URLs so local CRL caches are not forced to use static URLs.
- Downloads of any file type, not just CRLs from HTTP/HTTPS resources. OCSP proof-sets, compressed CRLs, etc can also utilize non-standard ports.
- Filtering the certificates downloaded from web servers, so that you do not have to download files your enclave does not need.
- Publishing CRLs to multiple destinations.
- Pulling from any http/https source.

For more information on creating a distributed CRL approach for your organization, a System Administration Guide for CRLAutoCache 2.0 is in the works. It will be titled *SAG: CRLAutoCache 2.0* available from the DoD PKE DKO Web site soon.



IPMC Highlights

The Identity Protection and Management Conference (IPMC) was held in April in Miami, Florida. Organizers of the IPMC have made the briefings available at a secure Web site. Many briefs were presented, covering a range of topics, including:

- Evolution and Emerging Technologies
- Beyond the Warfighter
- Global Interoperability
- Implementation, Enablement, and Usage
- DoD and Industry Integration
- Working through the Issues

To access these presentations, visit:

<http://iase.disa.mil/conferences-workshops/index.html>. A DoD PKI certificate is required to access this Web site and to view individual presentations.

Agenda for Upcoming PKE TIM

Join us November 4th from 1400-1600 for our next PKE TIM. PKE TIMs are held as virtual public meetings on DCO. To attend this PKE TIM, visit

<https://connect.dco.dod.mil/r54517884>.

Teleconference information is displayed when you login. Items on the agenda for this TIM include:

- *BlackBerry* (Best Practices, Issues and Concerns)
- *Certificate Validation in the DoD*. Current issues with validating certificates, downloading CRLs, the role of external partners, and where OCSP, DTM, and RCVS fit in the Certificate Validation world.
- *CRL size*—why are they so big and how can we make them smaller?
- *Round Table*—Open Forum. Attendees can volunteer to present a topic at the next TIM.



RA/LRA/TA Corner



This marks the first appearance of what will be a regular feature of The PKE Quarterly Post: the RA/LRA/TA Corner. Here you will find all the latest news and useful tips for the RA/LRA/TA community. As always, we welcome your comments, suggestions and questions.

Certification Authority (CA) News

The table below lists Certification Authorities (CAs) that have recently been retired or are about to retire or stop issuing certificates.

Software CAs	Retired	CA-7 (02 Jun 09)
	Retiring	CA-8 (09 Sep 09)
	Ended Issuance	CA-13 (31 Jan 09)
		CA-14 (31 Jan 09)
SIPRNET CAs	Ended Issuance	CA-17 (14 Jun 09)
		CA-18 (14 Jun 09)
	Ended Issuance	CA-18 (19 Jun 09)

Remember that users will not be able to complete their software certificate registration after issuance is stopped. New user data files should not be uploaded to CAs that are close to their retirement date. Any issuance that is not completed before the issuing CA's retirement date will need to be reissued on a new CA. To avoid this scenario, we recommend using the LRA thin client. New online are CA-21, CA-22, CA-23, and CA-24. CA-21 and CA-22 issue user software certificates, alternate tokens, code signing certificates, and RA/LRA certificates. CA-23 and CA-24 issue CAC certificates.

Software CAs	New Online	CA-21
		CA-22
CAC CAs	New Online	CA-23
		CA-24

OKC URLs have migrated to the <ca-name>.csd.disa.mil DNS tree, but Chambersburg URLs are still using <ca-name>.c3pki.chamb.disa.mil (at this writing).

NIPRNET ID:	https://ca-21.c3pki.chamb.disa.mil
	https://ca-22.csd.disa.mil
NIPRNET Email :	https://email-ca-21.c3pki.chamb.disa.mil
	https://email-ca-22.csd.disa.mil
SIPRNET ID:	https://ca-21.c3pki.chamb.disa.smil.mil
	https://ca-22.csd.disa.smil.mil
SIPRNET Email :	https://email-ca-21.c3pki.chamb.disa.smil.mil
	https://email-ca-22.csd.disa.smil.mil
	(if the 22 series doesn't work, try <a href="https://<CA-NAME>.okc.disa.smil.mil">https://<CA-NAME>.okc.disa.smil.mil instead)

The Non-Person Entity (NPE) Initiative: The Next Step in Securing DoD Infrastructure

by Stan Naudus

To enhance the cyber security of DoD networks, improvements are being made to the DoD Public Key Infrastructure to support device certificates. This will eventually allow X.509 certificates to be installed onto every computer and networking device attached the Department of Defense's network. This new functionality is called the Non-Person Entity (NPE) initiative.

The term NPE refers to equipment, software, applications or services that can be assigned an X.509 certificate—in other words, non-humans. NPEs are constantly communicating information to each other, making them potential targets of cyber attack. While there are now security mechanisms in place to protect these NPEs, they are not deployed as extensively and centrally as the Public Key Infrastructure. So, it can be said that the NPE initiative will provide the additional security to machine users that CAC/PKI logon now provides to human users.

The first phase of the NPE Initiative will involve Microsoft base products to include Domain Controller, workstation, and server certificates. Microsoft domains have a service called auto-enrollment that automates the secure request, transfer and usage of device X.509 certificates. Auto-enrollment determines when certificates will expire and will automatically request and install updated certificates. The first release of the DoD NPE initiative is to leverage this auto-enrollment functionality to automate the deployment of device certificates on DoD Microsoft workstations and servers.

NPE development is on schedule and the CC/S/As are in the process of determining when they will begin rolling out this new functionality. The PKI PMO

Ways Device Certificates Can Be Used

Network Access Control. Prevent unauthorized or unhealthy devices from connecting to the network even if they have physical access, whether the network is wired or wireless (supports 802.1x standards).

Encrypting machine-to-machine communication. Encrypting SQL Server databases and connections, or encrypting mail flow between Exchange and other SMTP servers, and within custom line of business applications.

Benefits of Microsoft's Auto-Enrollment feature

Automates the distribution of device certificates to all Microsoft devices that now use X.509 certificates (e.g. Device Controllers).

Allows IPSEC tunnels to be formed between nodes (using device certificates), providing the capability to authenticate and encrypt the information streams.

Provides a stronger initial layer of authentication (e.g. before user login via CAC cards is performed).

Removes need to use user ID/passwords to generate Microsoft-based VPNs. (e.g. use device certificates to form VPNs).

is engineering the solution and will deploy the needed infrastructure into the Defense Enterprise Computing Centers (DECCs). Every effort is being made to ensure that NPE will provide significant improvements in security along with minimal levels

The 2048-bit Migration Begins...

In preparation for compliance with Homeland Security Presidential Directive (HSPD)-12, the Department of Defense is migrating to 2048-bit credentials. Last month, the DoD Public Key Infrastructure began issuing 2048-bit credentials on Common Access Cards (CAC) and 2048-bit Secure Socket Layer (SSL) certificates from software CAs. Support for 2048-bit credentials is on NIPRNET only; SIPRNET will keep using the 1024-bit tokens pending a 2048-bit token approved for SIPRNET use.

The PKI Program Management Office (PMO) has forward deployed 2048-bit Registration Authority (RA) credentials. Each Service/Agency RA Office has been issued one 2048-bit RA token for requesting and issuing certificates. Only

RAs with 2048-bit credentials will be allowed to issue and approve certificate requests. RAs should first issue new 2048-bit certificates to existing RAs and LRAs in their districts to ensure that they can continue requesting and issuing certificates for their users.

In order for the new 2048-bit RA tokens to work, RAs must have the following hardware/software configuration:

- Approved Gemalto Cyberflex Access 64K V2c token
- SCR331 card reader
- ActivClient 6.1
- Firefox 2.x
- Latest root certificates installed in Firefox
- Updated Firefox profile with the *acpkcs201-ns.dll* security module loaded

PLEASE NOTE: NIPRNET RAs must have 2048-bit tokens to access CA-21, CA-22, CA-23 and CA-24.



Using Your BlackBerry: How to Send and Receive Secure Email

In recent weeks, DoD PKE Engineering Support has logged an increasing number of requests for guidance regarding BlackBerry's support of S/MIME. S/MIME is the protocol that allows BlackBerry users to send and receive signed or encrypted messages. Before a user can start sending S/MIME messages, a few changes need to be made to the BlackBerry Enterprise Server configuration as well as to the individual BlackBerry device. This article discusses the needed configuration changes and the basics of exchanging signed and encrypted S/MIME messages.

What Needs to Happen Before You Can Send S/MIME Messages

Before you can send or receive S/MIME email, a few prerequisites need to be performed by you and your BlackBerry Administrator.

On the BlackBerry Enterprise Server, the Administrator must:

- ✓ Enable S/MIME protocol
- ✓ Activate S/MIME for the users and/or groups that want to use S/MIME on their BlackBerry devices
- ✓ Deploy the DoD Root CA application to all users and/or groups with S/MIME Enabled (optional)
- ✓ Configure the default Certificate Revocation List (CRL), Lightweight Directory Access Protocol (LDAP), and Online Certificate Status Protocol (OCSP) settings (optional)

Though optional, these last two actions are highly recommended. Centrally administering the publication of DoD Roots and Certificate Validation settings will ensure that your users are able to correctly and efficiently exchange secure messages. If the DoD Root CA application is not pushed to the devices the users will have to manually add the DoD Roots and Intermediate CAs. Similarly, if the CRL, LDAP, and OCSP settings are not configured on the BlackBerry Enterprise Server, then each device will need to be configured individually. For more information on these topics, see the *Quick Reference Guide - BlackBerry Enterprise Server Wireless Push of DoD Root CA Application* and the *Wireless Security Technical Implementation Guide (STIG) BlackBerry Security Checklist* for the recommended DoD configurations for CRL, LDAP, and OCSP settings.

On the BlackBerry device, the User must:

- ✓ Verify the DoD Roots and Intermediate CAs are installed.
- ✓ Install and pair a smart card reader (for CAC users only)
- ✓ Import your certificates to the BlackBerry device.
- ✓ Configure the Signing Option and Encryption Option to use the corresponding certificates

If the DoD Roots and Intermediate CAs are not on your

device, use either the *BlackBerry Install-Root* application or the *BlackBerry Desktop Manager's Synchronize Certificate* application. To obtain BlackBerry InstallRoot, point your BlackBerry browser to <https://www.dodpke.com/blackberry> and download BlackBerry InstallRoot (net_rim_DoDRootCerts.jad).

To import CAC/PKI certificates, use the *Import Smart Card Certs* application. This application is installed along with the smart card reader software on the BlackBerry device. Once your certificates are imported and the corresponding certificate is set for the Signing Option and the Encryption Option, you will be able to utilize S/MIME email.

Getting Recipients' Public Certificates onto Your BlackBerry

In order to send an encrypted email, you first will need your recipient's public certificate. There are three ways to get your recipient's public certificates onto your BlackBerry device:

- Use the *BlackBerry Desktop Manager's Synchronize Certificate* application to import recipient certificates from your desktop to your BlackBerry device.
- Save the certificate when that individual sends a signed email to your BlackBerry device, OR
- Use an LDAP server configured on your BlackBerry Enterprise Server or BlackBerry device to search for the recipient's certificate and save the certificate to your device.

Sending S/MIME Email

To send a signed, encrypted, or signed and encrypted email, select the encoding method when you compose or reply to an email.

- SIGNED EMAIL: To send a signed email, select **Sign** from the *Encoding* dropdown menu. Compose the email and select **Send**. You will then be prompted to enter the PIN or Password for your signing certificate.
- ENCRYPTED EMAIL: To send an encrypted email, select **Encrypt** from the *Encoding* dropdown menu. If the recipient's public certificate is stored on your BlackBerry device, then the email will be sent encrypted. However, if the recipient's certificate is NOT stored on your device, then you will be prompted to select an action: **Do not send, Remove from message, Send unencrypted, or Fetch certificate.**



cate. Fetching the certificate searches the default LDAP server for a certificate that matches the email address you are trying to send to.

- SIGNED AND ENCRYPTED EMAIL: To send a signed and encrypted email, select **Sign and Encrypt** from the *Encoding* dropdown menu. You will need the recipient's public certificate to send the email encrypted and will be prompted to enter your PIN or Password to sign the email.

Receiving S/MIME Email

- SIGNED EMAIL: When a signed email is received on the BlackBerry device, the certificate status and the certificate chain to determine if the sender's signature is valid and can be trusted.
- ENCRYPTED EMAIL: When an encrypted email is received on the BlackBerry device, you will be prompted to enter your PIN or Password to decrypt the email.
- SIGNED AND ENCRYPTED EMAIL: When a signed and encrypted email is received on the BlackBerry device, you will be prompted to enter your PIN or Password to decrypt the email. After the email is decrypted, the certificate status and the certificate chain are verified to determine if the sender's signature is valid and can be trusted.

NOTE: Before performing LDAP queries, OCSP requests, or downloading an encrypted email, make sure that you have adequate signal strength from your carrier.

BlackBerry User Tips

Quickly Add Contacts

Use the Injector to automatically add contacts just by adding their certificates to your device keystore. To enable this setting on your device, select **Options > Security Options > Key Stores >** and change **Key Store Address Injector** to Enabled.

Stay Connected to Your Key Store Longer

Frustrated by constant key store password timeouts? Ask your BlackBerry Administrator if they can lengthen the minimum timeout for your key store password timeout.



About DoD PKE



The DoD Public Key Enabling (PKE) Team is chartered with helping DoD customers leverage existing and emerging PKI capabilities for increased productivity and an improved Information Assurance posture.

We provide engineering consultations, develop enterprise solutions, create collaboration environments, and work to make commercial products interoperate with the DoD PKI.

We are committed to increasing the security posture of the DoD by providing a seamless security environment supporting Identity Management efforts with the overarching goal of defending and protecting the United States of America.

DoD PKE is the **Key** to operationalizing PKI.

Visit us on DKO:

<http://iase.disa.mil/pki/pke>

Send your questions and feedback to:
PKE_Support@disa.mil

Upcoming Events

PKE TIM—BlackBerry, Certificate Validation

Date: 04 November 2009

Time: 1400-1600 EDT

- BlackBerry—Best Practices, Q&A
- Certificate Validation in the DoD World
- CRL—Why are they so big and how can we make them smaller?
- Round Table—Open Forum. Attendees can volunteer to present a topic at the next TIM.

This DCO meeting is set to Public. Visit

<https://connect.dco.dod.mil/r54517884>

Fall PKE TIM— Agenda TBD

Date: TBD— Fall 2009

Time: TBD

To submit a topic for this PKE TIM, send an email to PKE_Support@disa.mil with "FALL PKE TIM" in the Subject line.

Microsoft PKE TIM

Date: January 2009

Time: TBD

Send an email to pke_support@disa.mil with "January PKE TIM with Microsoft" in the Subject line.



In the Pipeline...

Beginning this issue, we will update you on other initiatives we are exploring for the DoD user community. This issue's In the Pipeline we feature updates on Cryptographic Migration Testing (CMT), the Delegated Trust Model (DTM), and PKI Interoperability.

Cryptographic Migration Testing (CMT)

As current implementations of secure hashing algorithms become more susceptible to attack, the DoD is evaluating ways to transition to stronger algorithms. CMT is a Joint initiative, comprised of various CC/S/A members and the Defense Manpower Data Center (DMDC) Working Group (WG); it involves testing stronger encryption algorithms and key lengths. Last year, testing began on the upgrade of CAC/PKI and SSL key lengths to 2048-bit and involved validating everything from CAC issuance and mobile device testing to PKE application and server support. This testing is critical to determining the changes that need to be made for the infrastructure to support stronger algorithms, and to estimate when the DoD can move to stronger algorithms.

Testing showed the user experience with the 2048-bit keys was not noticeably affected when signing documents or authenticating to secure web servers. Although, testing did find that issuance time for the larger keys took longer, by as much as two minutes or more. Support for the larger keys exists for some mobile devices, however, other mobile devices will require updates.

CMT testing of the secure hashing algorithm SHA-256 will be performed in the future. It is already known that the only Microsoft operating systems that will support verification using SHA-256 are Windows XP SP3 and Windows Vista or later. Elliptical Curve-based testing is also underway. Stay tuned for more information...

Delegated Trust Model (DTM)

DTM is coming to desktops throughout DoD this Fall. DTM refers to the way the DoD PKI Online Certificate Status Protocol (OCSP) responders are trusted by clients. Currently, OCSP responder certificates are self-signed certificates that must be pushed to user desktops every three years. With DTM, the chain of trust is derived from Certification Authority (CA) certificates, which are already pushed to desktops. DTM certificates will be issued more frequently (every 30 days) and the shorter lifetime will assure greater trust.

We are in the process of applying updates to the six Robust

Certificate Validation Service (RCVS) nodes in the coming weeks. User desktops will transition seamlessly. Some Cisco routers will require manual configuration.

External PKI Interoperability

In our April issue, we introduced the Federal Bridge Certification Authority (FBCA) and DoD's intent to interoperate with external partner PKIs. External Interoperability Testing continues at JITC; external partners should continue to schedule testing through the External Interoperability Working Group (EIWG). The Federal Aviation Administration (FAA) is the newest member on the list of approved External PKIs on DoD networks.

The PKE Support Team maintains its focus on two areas: (1) ensuring that applications and operating systems work with the Federal Bridge Cross Certificate Trust Model and providing best practices to the community; and (2) supporting DoD and non-DoD organizations to implement interoperable PKI solutions that enable information sharing.

Testing of applications and operating systems with the Federal Bridge Cross Certificate Trust model verifies an application's capabilities to build a trust path, to check certificate revocation information, and to check certificate policies and name constraints. Applications in the testing queue now are Outlook, Internet Information Server 6 and Internet Information Server 7. Look for test results and best practices in the coming months.

Implementations underway include enabling several DoD web servers to accept external PKIs. Several DoD sites today accept Department of State (DoS) certificates. DoS is now working with the DoD to enable network support for DoS users with DoD CACs. We are also working with customers to get sites enabled with the FAA PKI.

On efforts to coordinate HSPD-12 initiatives across the Federal Government, GSA recently stood up a Logical Access Working Group (LAWG). Its purpose is to document logical access implementation guidance for the Federal Community. DoDPKE is a co-chair of this working group.

Latest Updates from DoD PKE

Latest Document Releases

The following documents have been added or updated to the DoD PKE Knowledgebase.

- Deploying DoD PKI CA Certificates using Microsoft GPOs (New) <https://www.us.army.mil/suite/doc/18217726>
- Smart Card logon with PIV (New) - <https://www.us.army.mil/suite/doc/17967040>
- Requesting a Windows Certificate using Openssl (New) - <https://www.us.army.mil/suite/doc/16388184>
- Updated Group Role Certificate QRG (Update) - <https://www.us.army.mil/suite/doc/18284568>
- Configuring SQID to Cache DoD CRL - <https://www.us.army.mil/suite/doc/15639697>

www.us.army.mil/suite/doc/15639697

- Revocation Checking for External Partners (New) - <https://www.us.army.mil/suite/doc/18295718>

Latest Software Releases

The following software tools have new releases available for download from the DoD PKE DKO Web site.

- Linux CRL Download tar file (instructions included) <https://www.us.army.mil/suite/doc/18106327>

