

The PKE Quarterly Post



PIV-I: A Primer

Background

The term PIV-I (or Personal Identity Verification Interoperable) was first formally introduced in 2009 as a part of a standardized terminology for categorizing credentials issued by commercial providers that were modeled after government-issued PIV cards (similar to the Common Access Card or CAC). The intended meaning of PIV-I was that these credentials would be technically interoperable with PIV cards, would meet security requirements that would enable government agencies to trust them, and could be distinguished both visually and electronically from PIV cards. Although the initial definition of PIV-I simply identified requirements, in 2010 these requirements were formalized through combining them with the certification process already performed by the Federal Public Key Infrastructure (PKI) Policy Authority to approve government and commercial PKIs.

In adapting the federal government PIV requirements to a commercial PIV-I model, there were two challenges that had to be addressed. First, the issuance of a PIV card requires the successful adjudication of a National Agency Check with Inquiries (NACI). Adjudication of a NACI is a strictly

government function. As a result, PIV-I dropped this requirement entirely. Second, the mechanism used by PIV cards to develop unique identifiers relies on the Federal Agency Smart Credential Number (FASC-N), which is only defined for federal agencies. Rather than attempting to expand the FASC-N numbering system, PIV-I leveraged the Universally Unique Identifier (UUID) standard.

The full set of requirements for PIV-I credentials are detailed in the following two documents:

- Personal Identity Verification for Non-Federal Issuers, Version 1.1, July 2010 ¹
- X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) ²

continued on page 3

In This Issue

Evaluating Thin Clients for SIPRNet 4

New Rich Revocation Checking Capabilities for Weblogic Server 6

Wireless Update 7

In Every Issue

Ask the Expert 2

Notes from DoD PKE 2

In the Pipeline 3

RA/LRA/KRA Corner 4

Latest Document Releases 5

About DoD PKE 8

PKE Puzzle Corner 8



Ask the Expert

I received a new CAC and have verified that my new issuing CA is installed in the domain controller certificate store, but I still can't log on to my workstation. What's the issue?

Smart card logon (SCL) issues can have a number of different causes; however, one of the common ones DoD PKE has seen recently is SCL failure due to the absence of the issuing CA in the Windows NTAAuth store on the domain controller. Users may receive errors such as:

"Your credentials could not be verified."

"The system could not log you on. You cannot use a smart card to log on because smart card logon is not supported for your user account. Contact your system administrator to ensure that smart card logon is configured for your organization."

Windows Server 2008, 2008 R2, Vista and 7 are dependent on several scheduled tasks run by the Task Scheduler service to properly replicate certificates in the NTAAuth store, so disabling the Task Scheduler service causes domain NTAAuth replication to fail. However, the Windows STIGs recommend that the Task Scheduler service be disabled as a means to mitigate a Task Scheduler vulnerability reported by Microsoft, resulting in the Task Scheduler service being disabled on many domain controllers. To enable replication to succeed while maintaining the security profile of the system, in lieu of disabling the Task Scheduler, the MS10-092 security update from Microsoft can be applied to permanently address the Task Scheduler vulnerability. More information on the security update can be found at <http://technet.microsoft.com/en-us/security/bulletin/MS10-092>. More information on the issue can be found in *FAQ: Smart Card Logon Fails Due to Certificates Missing from the NTAAuth Store* on the DoD PKE website at <http://iase.disa.mil/pki-pke>.

When I try to log on to my machine, I receive the error message "Insufficient resources exist to complete the requested service". What's going on?

The Windows Server 2008 R2 Domain Controller (DC) STIG requires that the "Force Strong Key Protection" group policy setting be set to "User must enter a password each time they use a key". When this setting is enabled on a DC at the time of the DC certificate request, a password is set to be required for access to the DC's private key. However, since the smart card logon authentication process is silent, there can be no prompt for a password for the domain controller's private key. As a result, the private key cannot be accessed during logon negotiation, causing logon to fail.

There are two options to resolve this issue:

1. Request a new DC certificate while "Force strong key protection" is configured to "User input is not required when new keys are stored and used".
2. Export and re-import the existing DC certificate while "Force strong key protection" is configured to "User input is not required when new keys are stored and used".

Once the certificate has been imported, the "Force strong key protection" setting should be restored to "User must enter a password each time they use a key".

Detailed instructions for this issue can be found in the *FAQ: Logon error "Insufficient system resources exist to complete the requested service"* on the DoD PKE website at <http://iase.disa.mil/pki-pke>.

Why can't I find the SIPRNet self-signed OCSP responder certificate in InstallRoot-S?

In October 2011 the SIPRNet Robust Certificate Validation Service (RCVS) OCSP infrastructure was migrated from the Explicit (self-signed) Trust Model to the Delegated Trust Model (DTM). As a result, the previous self-signed OCSP certificate is no longer needed in trust stores for certificate validation. New versions of InstallRoot, beginning with 3.15.2S, will no longer contain this certificate. You can find more information on the different OCSP trust models in the OCSP slick sheet on the A-Z page of the DoD PKE website at <http://iase.disa.mil/pki-pke>. Information on updating Tumbleweed Desktop Validator configurations to support the new model is available in the Preliminary Configuration Actions section of the *Tumbleweed Desktop Validator Workstation and Server Configuration* guides on the *Tools* page of the DoD PKE website.

Notes from DoD PKE

Welcome to the spring/summer edition of the DoD PKE Post. As always, it's been a busy time in the PKI community. Some recent hot topics have included PKI capabilities for mobile devices, PKE of SIPRNet and thin clients, and interoperability with DoD partners.

Speaking of interoperability with DoD partners, this issue's cover story is all about the facts surrounding PIV-Interoperable, or PIV-I, credentials. The article covers why we have PIV-I, the DoD policy governing the use of PIV-I, how PIV-I compares to PIV, and how DoD systems can use PIV-I. The big take-away is that PIV-I credentials provide for added security and cost savings while reducing DoD's credential issuance overhead. A full list of DoD-approved PIV-I issuers is available on the DoD PKE Interoperability page on IASE. In addition, a new draft of FIPS 201, which updates the PIV specification, is out for comment. DMDC is coordinating DoD's comments and will be sending feedback to NIST by August 10th.

Another major initiative is PKI capabilities for mobile devices. Some of you may have attended our first DoD PKI Mobility TIM in June. It was a very valuable forum in which we exchanged information on on-going pilots, capability gaps, and implementation challenges. DoD PKE has taken that feedback and is working with DMDC to explore possible future PKI deployment solutions that would be more user-friendly for mobile. As part of our support to the DISA Mobility Pilot, we have also developed pairing instructions in PDF and video forms for the baiMobile SC3000 smart card reader with the iPhone, iPad and DROID RAZR as well as for the BlackBerry second generation smart card reader with the BlackBerry.

In our ongoing effort to improve communications, DoD PKE now offers RSS feeds to notify the community when new items and updates are posted to our web site. Feeds are currently available for *Tools*, *Interoperability* and *Newsletters*. To subscribe, simply click the RSS feed icon in the upper right of the corresponding page on our site.

We've also migrated to Defense Enterprise Email – our new email address is dodpke@mail.mil. Our old pke_support@disa.mil address will stop forwarding sometime in November, so please update your contact record. We hope to hear from you soon!



PIV-I and DoD Policy

DoD Instruction 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*³, specifies that: “The DoD shall only rely on certificates that are issued by the DoD PKI or by a DoD-approved PKI for authentication, digital signature, or encryption.” While most vendors who have been given PIV-I certification by the Federal PKI Policy Authority or by a cross certified bridge have applied for DoD approval, it is important for relying parties to verify that a given provider has been approved by DoD prior to accepting PIV-I credentials issued by that vendor. Relying parties may find the authoritative list of DoD-approved external PKIs at <http://iase.disa.mil/pki-pke/interoperability>.

DoD Instruction 8520.03, *Identity Authentication for Information Systems*⁴, identifies specific requirements for the use of credentials for authentication to access DoD resources. PIV-I cards issued by DoD-approved external PKIs are considered to be credential strength D as defined by this instruction. As a result, they can be used as authentication credentials for access to information or other resources up to sensitivity level 3 from any user environment. PIV-I cards cannot be used to authenticate for access to

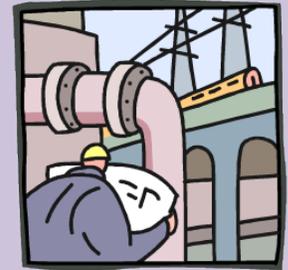
resources that have been designated sensitivity level 4, network logon, system administrator accounts, or any classified resources.

Description

A PIV-I card is a smart card form factor that incorporates all of the identifying characteristics of a PIV card or a CAC. It has a name, photo, and expiration date printed on the card. It contains a chip that has authentication, encryption, and signature certificates along with digitally signed biometric templates for two fingerprints. In addition, it contains a special card authentication certificate that can be accessed using a contactless interface and that does not require a PIN to be entered to use the private key. This certificate is designed to provide PKI anti-cloning capability for physical access. The table below provides a summary of similarities and differences between PIV and PIV-I.

Authenticating PIV-I

For DoD relying parties, there are three critical aspects of PIV-I. First, as noted in the table, the PIV-I issuance process itself does not include a background check. Relying parties who require an adjudicated background check will need to



In the Pipeline

InstallRoot GUI Tool for SIPRNet

DoD PKE is currently developing a GUI version of the InstallRoot tool for SIPRNet. This version will provide users with the option to install the DoD legacy SIPRNet PKI and/or NSS PKI Certification Authority (CA) certificates to their Microsoft and Firefox certificates stores. The tool is targeted for release in summer 2012.

DoD Identity and Email CAs 15-18 to be Retired

In June 2012, DoD Certification Authorities (CAs) and EMAIL CAs 15 – 18 will expire and be decommissioned. It is recommended that DoD relying parties remove these CAs from their trust stores. These expiring CAs are also the last remaining CAs which do not include the DoD OCSP responder URL in their Authority Information Access (AIA) fields; once they have expired, organizations may fully rely on the location listed in the AIA field to perform OCSP-based revocation checking, and will no longer need to explicitly specify the responder location for any CAs.

New DoD PKE RSS Feeds

DoD PKE now offers RSS feeds to notify users when new items and updates are posted to our web site. Feeds are currently available for *Tools, Interoperability* and *Newsletters*. To subscribe, simply click the RSS feed icon in the upper right of the corresponding page on our site.

DoD PKE has a New Email Address

With our migration to Defense Enterprise Email, the DoD PKE support email address is now dodpke@mail.mil. Our old pke_support@disa.mil address will stop forwarding sometime in November, so please update your contact record! We'll be updating all of our documentation to reflect the new address over the coming months.

PIV and PIV-I Comparison		
Requirement	FIPS 201 PIV	FBCA PIV-I
Identity Proofing	<ul style="list-style-type: none"> In-person using two forms of ID from Form I-9 	<ul style="list-style-type: none"> In-person using two forms of ID from Form I-9
Identity Vetting	<ul style="list-style-type: none"> Completion of NAC-I background check 	<ul style="list-style-type: none"> Not applicable
OCSP Support	<ul style="list-style-type: none"> PKI must support OCSP and include responder pointer in certificates 	<ul style="list-style-type: none"> PKI must support OCSP and include responder pointer in certificates
Cryptographic Module	<ul style="list-style-type: none"> FIPS-140 Level 2 Hardware validated 	<ul style="list-style-type: none"> FIPS-140 Level 2 Hardware validated
Cryptographic Algorithm	<ul style="list-style-type: none"> RSA 2048 asymmetric keys SHA-256 signature hashes* 	<ul style="list-style-type: none"> RSA 2048 asymmetric keys SHA-256 signature hashes
Card Technology	<ul style="list-style-type: none"> Meet all technical requirements defined in NIST SP 800-73 	<ul style="list-style-type: none"> Meet all technical requirements defined in NIST SP 800-73
Printed Card Topology	<ul style="list-style-type: none"> Must contain name, photo, expiration date, organizational affiliation Format must be as specified in FIPS-201 	<ul style="list-style-type: none"> Must contain name, photo, expiration date, organizational affiliation Must not contain “U.S. Government” or federal agency logo
Chip Data Elements	<ul style="list-style-type: none"> Authentication certificate, FASC-N, two fingerprint images 	<ul style="list-style-type: none"> Authentication certificate, card authentication certificate, UUID, two fingerprint images
Trust Chain	<ul style="list-style-type: none"> Issuing CA is subordinate to the Federal Common Policy Root CA OR has a cross-certification relationship with the Federal Bridge at the PIV-auth policy OID level of assurance 	<ul style="list-style-type: none"> Issuing CA has a cross certification relationship with the Federal Bridge at the PIV-I policy OID level of assurance
Sponsoring Organization	<ul style="list-style-type: none"> Government agency 	<ul style="list-style-type: none"> Employer or other affiliated party (such as membership in volunteer organization)

*Note: Although the PIV standard requires the use of SHA-256, DoD CACs are currently issued with SHA-1 signature hashes.

continued on page 7



Evaluating Thin Clients for SIPRNet



RA/LRA/KRA Corner

New RA/LRA/KRA Training Dates

The DoD PKI PMO provides monthly training to DoD personnel who will perform the duties of DoD PKI Registration Authorities (RAs), Local Registration Authorities (LRAs), and Key Recovery Agents (KRAs) on NIPRNet and/or SIPRNet. A new training schedule has been released and is posted on the DoD PKE website at <http://iase.disa.mil/pki-pke>. The schedule can be located on both the home page and the *For RAs, LRAs, KRAs & TAs* page of the site.

All students must register before attending any of the training sessions. Additionally, students receiving RA and/or KRA credentials in the classroom will require a nomination letter from their home CC/S/A. The optional NSS session is utilized for RA credential issuance to students who do not currently have an existing NSS RA at their home CC/S/A.

For questions regarding training, please reach out to your RA help desk. Contact information is available on the *Contact Us* page of the DoD PKE website at <http://iase.disa.mil/pki-pke/contact.html> under *Combatant Command/Service/Agency Registration Authority (RA) Operations Offices*.

Thin clients are small, light, simple devices (sometimes also called “dumb terminals”) that can be used as gateways to centralized computing environments. They possess very little to no local storage capacity, and are attractive in part due to the decreased attack vector that the scaled-back client provides. In addition to the security advantages, organizations may consider thin clients due to their scalability, which can result in a lower total cost of ownership.

Clients can be divided into three general categories: Thin, proprietary thin, and zero clients. Thin clients contain an embedded version of a standard operating system (OS), such as Windows Embedded 7 or XP. Proprietary thin clients contain a non-standard proprietary vendor operating system, such as Wyse Thin OS or HP ThinPro. Zero clients have no traditional OS and contain no local storage.

Clients can be configured to connect to a centralized computing environment called a Virtual Desktop Infrastructure (VDI). VDIs typically include virtualized desktop images and connection broker, and may have other components. Different VDIs have different deployment models and capabilities, and not all thin clients are designed to work with all VDIs. DoD PKE has evaluated clients with three popular VDIs: Windows Remote Desktop Services, Citrix XenDesktop, and VMWare View.

In evaluating thin clients for use on SIPRNet with the new NSS PKI and SIPRNet token, three primary questions were considered:

- 1. Can the thin client read the SIPRNet token?** If the client has an embedded reader, does it recognize the token? If not (or in addition), can an external card reader be connected and expose the token to the client.
- 2. Can the client support smart card logon to the target VDI?**

- 3. Can the client support standard PKI operations?** Once the client has connected to the VDI via smart card logon, do operations such as web site client authentication, document signing, and email signing and encryption work properly?

Common issues that prevent clients from being able to interact with the SIPRNet token include old firmware unable to support the token, old card reader drivers, use of 90meter Smart Card Manager (SCM) card reader middleware versions earlier than 1.2.22S, and insufficient storage space to install the card reader middleware.

The results of DoD PKE’s testing to date are shown in the tables on the next page. For each client that has been tested, the **Client Token Support Overview** lists whether it is able to read the token with embedded and/or external card readers (as well as notes any special conditions or status), and the **VDI Support Overview** lists which VDIs the client was able to use with PKI.

Guides containing detailed directions for configuring zero clients, Windows XP Embedded, Windows Embedded Standard 7, and Wyse Thin OS clients to function with the SIPRNet hardware token and various virtual desktop infrastructures (Citrix XenDesktop/XenApp, VMWare View, and Microsoft Remote Desktop Services (RDS)) are currently in review and will be available on the DoD PKE website at <http://iase.disa.mil/pki-pke> once approved. Reference guides for configuring VDIs to function with the DoD PKI, meant to compliment the configuration guides developed for the thin clients, will also be published once approved.

Interested in a thin client not listed? Contact dodpke@mail.mil to request an evaluation.

continued on page 5

RA/LRA/KRA Training Dates				
Dates	LRA Training	RA Training	KRA Training	Optional NSS Session (half day)
June 26 - 29	06/26/2012	06/27/2012	06/28/2012	06/29/2012
Jul 24 - 27	07/24/2012	07/25/2012	07/26/2012	07/27/2012
Aug 28 - 31	08/28/2012	08/29/2012	08/30/2012	8/31/2012
Sep 25 - 28	09/25/2012	09/26/2012	09/27/2012	09/28/2012
Oct 23 - 26	10/23/2012	10/24/2012	10/25/2012	10/26/2012
Nov 13 - 16	11/13/2012	11/14/2012	11/15/2012	11/16/2012
Dec 11 - 14	12/11/2012	12/12/2012	12/13/2012	12/14/2012
Jan 15 - 18	01/15/2013	01/16/2013	01/17/2012	01/18/2012
Feb 19 - 22	02/19/2013	02/20/2012	02/21/2012	02/22/2013



Evaluating Thin Clients for SIPRNet – *continued*

Client Token Support Overview					
Vendor	Model	Thin Client OS	Integrated Smart Card Reader	Ability to read SPRINet Token V/N	Notes
Oracle SunRay	2FS	None	✓	✓	Connects successfully to MS RDS. Connectivity to VMWare View still to be evaluated
	3+	None	✓	✓	Connects successfully to MS RDS. Connectivity to VMWare View still to be evaluated
Wyse	C10	Wyse Thin OS	✗	✓	Connects successfully to MS RDS and Citrix XenDesktop. Connectivity to Citrix XenDesktop requires upgrade.
	R90	Windows XPe	✗	✓	
ClearCube	19424	None	✓	✓	Requires firmware 3.5.1 External card reader only (reader does not support the SIPRNet token).
	19424ST	None	✓	✓	Requires firmware 3.5.1
HP	5740	Windows XPe	✗	✓	
	5740e	Windows 7e	✗	✓	
	gt7725	HP ThinPro	✗	✗	Awaiting firmware update supporting SIPRNet token for new units. No support for legacy units.
GD Tadpole	M1500	None	✓	✓	Connects successfully to MS RDS. Connectivity to VMWare View still to be evaluated.

✓ Positive Test Result ✗ Negative Test Result

VDI Support Overview					
Vendor	Model	Thin Client OS	Remote Desktop Services	Citrix XenDesktop	VMWARE View
Oracle SunRay	2FS	SRSS	✓	N/A	?
	3+	SRSS	✓	N/A	?
Wyse	C10	Wyse Thin OS	✓	✓	N/A
	R90	Windows XPe	✓	✓	✓
ClearCube	19424	None	N/A	N/A	✓
	19424ST	None	N/A	N/A	✓
HP	5740	Windows XPe	✓	✓	✓
	5740e	Windows 7e	✓	✓	✓
	gt7725	HP ThinPro	✗	✗	✗
GD Tadpole	M1500	SRSS	✓	N/A	?

✓ Client supports and works with VDI ? Testing in Progress
 ✗ Client supports VDI type but does not function with SIPRNet Hardware Token N/A Client does not support VDI type

Latest Document Releases

All documents are available from the DoD PKE site at <http://iase.disa.mil/pki-pke> unless otherwise noted.

New

FAQ: Smart Card Logon Fails Due to Certificates Missing from the NTAAuth Store: This FAQ discusses an issue with the disablement of Windows Task Scheduler preventing proper certificate replication to the NTAAuth store, causing smart card logon failure.

FAQ: “Insufficient system resources exist to complete the requested service” Smart Card Logon Error:

This FAQ discusses the cause of the “Insufficient system resources exist to complete the requested service” error and the solutions for this issue.

Major Updates

Microsoft Internet Information Services (IIS) 6.0: Public Key Enabling: Instructions for public key enabling Microsoft IIS 6.0 on SIPRNet have been incorporated into the guide.

Microsoft Internet Information Services (IIS) 7.0: Public Key Enabling: Instructions for public key enabling Microsoft IIS 7.0 on SIPRNet have been incorporated into the guide.

Microsoft Windows Server 2003: Enabling Smart Card Logon: Configuration instructions for SIPRNet have been incorporated, and all procedures and URLs were updated in this guide.

Microsoft Windows Server 2008: Enabling Smart Card Logon: Configuration instructions for SIPRNet have been incorporated, all procedures and URLs were updated, and multiple account mapping information was removed.

continued on page 6



Tumbleweed Desktop Validator 4.9

Workstation and Server Configuration:

Configuration instructions for SIPRNet and DoD-Approved External PKIs have been incorporated. Four default configuration files – (1) DoD PKI ONLY, (2) DoD and ECA PKIs ONLY, (3) DoD PKI, ECA PKI and DoD Approved External PKIs, and (4) NSS and SIPRNet Legacy CAs – have also been provided for import into the tool.

Tumbleweed Desktop Validator 4.10

Workstation and Server Configuration:

Configuration instructions for SIPRNet and DoD-Approved External PKIs have been incorporated. Four default configuration files – (1) DoD PKI ONLY, (2) DoD and ECA PKIs ONLY, (3) DoD PKI, ECA PKI and DoD Approved External PKIs, and (4) NSS and SIPRNet Legacy CAs – have also been provided for import into the tool.

RA/LRA/KRA Contact Information

RA Operations			
Name	Organization	Contact Information	COCOMS Support
Army	Army CTNOSC Army NETCOM	ctnosc.pki@us.army.mil (Equipment Certificates) netcom-9sc.registration.authority@mail.mil (User Certificates)	USEUCOM USSOUTHCOM USAFRICOM
Air Force	Air Force PKI Help Desk	https://afpki.lackland.af.mil/html/lracontacts.asp (Local Registration Authority Base Contacts) afpki.ra@us.af.mil	USCENTCOM USSOCOM USTRANSCOM USNORTHCOM USSTRATCOM
Navy	Navy PKI Help Desk	https://infosec.navy.mil/PKI/lramain.html	USJFCOM USPACOM
Marine Corps	USMC PKI RA Operations	raoperations@mcnosc.usmc.mil	Not an Executive Agent
USCG	USCG RA Operations	cgra@uscg.mil	Not an Executive Agent
Joint Staff	Joint Staff RA Support	jsra@js.pentagon.mil	Not an Executive Agent
DeCA	DeCA RA Operations	PKI.RA@deca.mil	Not an Executive Agent
DISA	DISA RA Operations	disaraoperations@disa.mil	Not an Executive Agent
DLA	DISA RA Operations	dlapki@dla.mil	Not an Executive Agent
NOAA	NOAA RA Operations	ra@noaa.gov	Not an Executive Agent
WHS	WHS IPM Team	whsra@whs.mil	Not an Executive Agent

New Rich Revocation Checking Capabilities for Weblogic Server

For anyone who has struggled with public key enabling Weblogic server due to the lack of out-of-the-box revocation checking capabilities and resulting requirement for custom code or third-party plug-ins to perform full certificate validation, there's good news. With the release of Weblogic 11g R1 patch set 5 in February, Oracle introduced rich native revocation checking capabilities for the server. The new functionality is also included in the Weblogic 12.1.1 release. Some highlights include:

- CRL and OCSP support with local caching and failover capabilities. Cache times for both types of revocation data artifacts correspond to the validity period of the artifact, but can be customized to be shorter. Nonces can also be enabled for OCSP, and all OCSP trust models are supported.
- CRL distribution point (CRLDP) support, as well as the capability to disable dynamic fetching from CRLDPs and pre-load CRLs into a local directory cache.
- Configurable fetch timeouts for each type of artifact.
- A configuration option controlling whether the system fails open or closed if revocation data is unavailable.
- The option to apply the configuration to all CAs or override the standard configuration for particular CAs.

For more details on the new capabilities, see http://docs.oracle.com/cd/E23943_01/web.1111/e13707/ssl.htm#autold42.



implement secondary registration processes to link PIV-I credentials with background check information. Second, certificates issued for both PIV and PIV-I cards use the SHA-256 algorithm to generate hashes. Relying parties seeking to leverage PIV-I for authentication must ensure they can validate certificates with SHA-256 hashes. Finally, because of the similarities in required elements to be printed on the cards, and the relatively small area of the cards, PIV-I cards will look similar to PIV cards. An electronic check is the only sure way to verify that a presented PIV or PIV-I card is genuine, but PIV-I issuers are not allowed to use the term “U.S. Government” or a federal agency logo on PIV-I cards.

Leveraging PIV-I credentials provides for added security and cost savings. The cost of issuing and managing PIV-I cards is not directly charged back to the DoD. In addition, because the organizational affiliation of a PIV-I card is with the individual’s employer, PIV-I cards do not need to be re-issued as a result of contract expiration or staff turnover between different contracts.

Finally, if an employee leaves the affiliated organization, the organization is responsible for ensuring that the PIV-I card and certificates are revoked, which provides added assurance.

It is important to note that PIV-I, like PIV and CAC, is an identity credential, not an authorization token. Prior to providing access to a PIV-I card holder, relying parties remain responsible for verifying the authorizations of the PIV-I card holder and registering the authentication certificate for appropriate privileges. The overall process can be significantly shortened, however, since the DoD is not required to first issue a CAC prior to registering the user.

¹http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers.pdf
²http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf
³<http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf>
⁴<http://www.dtic.mil/whs/directives/corres/pdf/852003p.pdf>

Wireless Update

Using the CAC with a BlackBerry

Did you know you can use your CAC to sign, encrypt and decrypt email on your BlackBerry? All you need is a BlackBerry smart card reader such as the second-generation BlackBerry Smart Card Reader pictured.

As a reminder, you should digitally sign email if it:

- Includes a link or attachment
- Provides direction or tasking
- Requests or responds to requests for resources
- Promulgates organization position
- Contains information on operational, contract, finance or personnel management matters



BlackBerry Smart Card Reader 2.0

You should encrypt email if it contains:

- Privacy Act Information (PII)
- Health Insurance Portability and Accountability Act Information (HIPAA)
- Proprietary contract information
- Information classified as ‘for official use only’ (FOUO)

For an overview of when to digitally sign and encrypt email from your BlackBerry with your CAC certificates, please read the *Secure Email in DoD* slick sheet available on the DoD PKE web site at <http://iase.disa.mil/pki-pke> under *Mobile Devices*.

To use the digital signature and encryption capabilities available within your BlackBerry email, you will need to pair your BlackBerry with the card reader and import your CAC certificates into your phone. To pair your BlackBerry with a second-generation card reader such as the one pictured:

1. Turn the card reader on by pressing the **Action** key.
2. From your BlackBerry, navigate to **Options** → **Security Options** → **Smart Card**.

3. From the **Registered Reader Drivers** section, select **BlackBerry** and choose **Driver Settings**.
4. Press the **BlackBerry** menu key and chose **Connect**.
5. Press the **Action** key on the card reader.
On your BlackBerry, type the **SCR ID** that appears on the card reader’s screen and press **Enter**.
6. Press the **Action** key on the card reader. From your BlackBerry, type the **secure pairing key** shown on the card reader’s screen.
7. When prompted on your BlackBerry, type a **secure connection password** and click **OK**.

Your BlackBerry should now be paired with your card reader. When you insert your CAC into the reader, your BlackBerry will be able to see the certificates on your CAC. The next step is to import those certificates into the BlackBerry.

To import your CAC certificates into your BlackBerry:

1. Insert your **CAC** into the BlackBerry Smart Card Reader.
2. From your BlackBerry, navigate to **Options** → **Security Options** → **S/MIME**.
3. Press the **BlackBerry** menu key and select **Import Smart Card Certs**.
4. You will be prompted to choose the certificates you would like to import from your smart card. Make sure each of the certificates has a check mark next to it and click **OK**.
5. Enter the BlackBerry device’s **key store password** and click **OK**.
6. A message will confirm that the certificates were imported successfully to the device’s key store.

You are now ready to sign, encrypt and decrypt email from your BlackBerry. To digitally sign an email sent from your BlackBerry, select the **Sign** option in the **Encoding** field when composing the email. To encrypt an email, select the **Encrypt** option in the **Encoding** field. Note that when sending signed messages or decrypting email encrypted to you, you may be prompted to enter your CAC PIN.

Additional resources for using your BlackBerry with your CAC can be found in the *BlackBerry* section of *Mobile* page on the DoD PKE website at <http://iase.disa.mil/pki-pke>.



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 IASE—
<http://iase.disa.mil/pki-pke>

Send your questions and feedback to—
dodpke@mail.mil



PKE Puzzle Corner

Welcome to the PKE Puzzle Corner. This is your chance to try your hand at cryptanalysis. The first person to respond to dodpke@mail.mil with the correct answer will be announced in the next PKE Quarterly Post. Solutions will be posted to the Newsletters section of our web site at <http://iase.disa.mil/pki-pke> and published in the next edition of the Post.

Hint:

Q: What do you think of the Summer 2012 Newsletter?

A: It's "a fine" issue!

Decrypt the encrypted text below to solve:

RHLYY WMG QYYF M OYSLYR, KB RAC CB RHYW MLY VYMV. - PYZNMWKZ BLMZQTKZ

Winter Quarterly Post Puzzle Solution

Congratulations to Cynthia J. with the Army who was the first person to correctly solve the fall puzzle!

Cipher: Rail fence, 3 rows

Mind your p's and q's with a FIPS 140-2 validated random number generator

MYPNS HPOAA ROMGR RIDOR 'AD'W TAIS4 -VLDT D ADMU BREEA ONUSQ IF12I ENNEN T

M Y P N S H P O A A R O M G R R
I D O R ' A D ' W T A I S 4 - V L D T D A D M U B R E A O
N U S Q I F 1 2 I E N N E N T

