

The PKE Quarterly Post

New PKE Tools Roundup



DoD PKE has recently developed and updated several tools to assist organizations, administrators and end users with configuring their systems to use PKI. Here's an overview of the new additions and changes to our tool lineup.

Trust Anchor Constraint Tool (TACT) *New

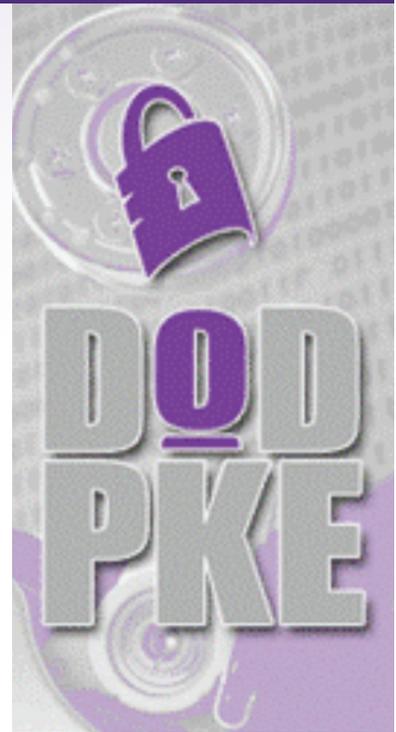
Target Audience: Web Server Administrators

TACT is a set of web server plugins and management applications for Microsoft Internet Information Services (IIS) and Apache HTTPD servers that aim to enable interoperability and enhance security when using mutually authenticated SSL/TLS. TACT enables web servers to accept PKI credentials from DoD-approved external PKIs in accordance with DoD policy (no custom code required) and to manage the cross-certificate chaining issue (described in our fall 2011 newsletter, our *FAQ: DoD Root Certificate Chaining Problems, and the FBCA Cross-Certificate Remover User Guide*) on the server side rather than requiring client workstation configuration changes.

The tool works by allowing the system administrator to define additional constraints, such as those that might typically be contained within a cross-certificate, as part of the local certificate path validation. For example, policy constraints can be configured to ensure that a system only accepts hardware certificates, and key size constraints can be applied to deny certificates with RSA 1024-bit keys. A complete list of the available constraints, as well as configuration instructions, is available in the *TACT User Guide*. TACT comes with a policy mapping database that makes it easy for administrators to identify which partner PKI certificate policies map to DoD-approved Federal Bridge assurance levels (medium hardware or higher) and configure their systems to require that a user credential meet the DoD assurance level requirements.

TACT allows the cross-certificate chaining issue to be addressed server-side by enabling the administrator to install all of the trust anchors to which a user's certificate may chain in the server's standard certificate store, then use TACT to restrict which sub-set of credentials are accepted from

continued on page 2



In This Issue

Wireless Update	4
DoD PKE Website Updates	5
Guest Contributor	5
Working Toward a More Streamlined CAC	6
New DoD-Approved External PKIs	7
Thin Client SIPRNet Token Support	7

In Every Issue

Ask the Expert	2
Notes from DoD PKE	2
In the Pipeline	3
RA/LRA/KRA Corner	4
Upcoming Events	6
Latest Document Releases	7
Latest Tool Releases	7
PKE Puzzle Corner	8
About DoD PKE	8



Ask the Expert

The CA where I usually request my server certificate says it no longer issues server certificates. Where do I request server certificates?

Both DoD CA-21 and CA-22 have reached the end of their issuance periods and are now in maintenance mode. They will continue to issue CRLs for 3 years, throughout the lifespan of all certificates that were issued by the CAs. Going forward, to obtain server certificates users can use DoD CA-27 (<https://ca-27.csd.disa.mil>) and CA-28 (<https://ca-28.csd.disa.mil>). Additional guidance on requesting SSL server certificates can be found on the *For Administrators, Integrators and Developers* page of the DoD PKE web site under *Web Servers*.

How can I update a BlackBerry device's trust store with new CAs without a new InstallRoot package?

InstallRoot for BlackBerry is developed by RIM, so in some instances is not released at the same time as other InstallRoot updates. If a version of InstallRoot for BlackBerry containing the latest CAs has not yet been published, you can install the new CAs manually by performing the following steps:

1. Install the latest version of InstallRoot onto your personal computer.
2. Export the desired CAs (e.g. DoD CAs 27-30) from your computer's trust store to an easily accessible location on your computer.
3. Install BlackBerry Desktop Software.
4. Connect your BlackBerry device to your computer and make sure it has synced to the BlackBerry Desktop Software.
5. From BlackBerry Desktop Software, go to Tools > Desktop Options, and check Use Certificate Synchronization.
6. From the BlackBerry Desktop Software home page, select Certificates, go to the Intermediate Certificates tab, and click the Import Certificates button.
7. Once you have successfully imported each of the desired CA certificates, click the Sync button.

Note: The latest version of InstallRoot for BlackBerry (5.0.0.826) is now available from the DoD PKE Tools page on <http://iase.disa.mil/pki-pke>!

Notes from DoD PKE

Welcome to the Winter Edition of the DoD PKE Quarterly Post. We are excited to share with you a special PKE Tools edition that focuses on recently developed and updated tools that organizations can use to help configure their systems to use DoD and DoD-approved PKI.

A recent addition to the PKE tool belt is the Trust Anchor Constraints Tool (TACT). TACT is a web server plugin for Microsoft IIS and Apache servers that aids in enabling interoperability and enhancing security when using mutually authenticated TLS. TACT allows additional trust anchor constraints to be configured so that a system owner can choose to accept, for example, DoD CAC hardware certificates but deny DoD software certificates. Another exciting feature of TACT is that it allows the FBCA cross-certificate chaining issue to be addressed by the server instead of the client. This means that end users visiting your site will no longer have to run the FBCA Cross-Certificate Removal tool on their local systems if your web server has TACT.

CRLAutoCache release 3.0 has been completely revamped and rewritten in C#

to provide better Microsoft CAPI integration capabilities. CRLAutoCache can now run as a Windows service and inject CRLs into the local Microsoft CRL cache as well as publish them to web servers and network file shares in support of local enclave caching and tiered CRL distribution architectures. A Linux version of CRLAutoCache has also been developed that provides support for downloading external non-DoD CRLs in bulk through the use of a configuration file.

We also added Windows 7 support for MailCrypt, updated the FBCA Cross-Certificate Removal tool with some new options, and created 64-bit versions of the various command-line versions of InstallRoot. Please read the newsletter for more details and even more exciting tool updates.

Conference season is also just around the corner. The 2012 Identity Protection and Management Conference is May 15-17 in Anaheim, California. DoD PKE will be hosting our annual PKE track. If you are interested in presenting a topic in the PKE track at the 2012 IPMC, email pke_support@disa.mil.

New PKE Tools Roundup – *continued*

those trust anchors. Since the trust anchor presented by the client exists in the server's standard certificate store, the user won't immediately be denied access due to his trust anchor being unrecognized by the server. Once the server has validated the path, TACT will perform additional validation to ensure that the certificate chains to a trust anchor in the TACT certificate store (which can contain a sub-set of the certificates in the standard server certificate store) as well as meets any additional configured constraints. For example, the server may validate a path from a user certificate to the Common Policy root certificate. Depending on its configuration, TACT may truncate this path and validate a path terminated by the ECA trust anchor, evaluating any constraints associated with the ECA trust anchor or additional certification path validation inputs. In this example, all paths validated to the Common Policy root certificate that do not traverse the ECA certificate may be rejected by TACT. This addresses the cross-certificate chaining problem by allowing the server trust anchor certificate store to provide for interoperability, while the TACT trust anchor store provides for security.

In addition to solving the major interoperability challenges of DoD policy compliance and cross-certificate chaining, TACT can help administrators strengthen the overall security of their web servers, regardless of user community, through the evaluation of factors beyond the standard path validation checks of trust, time validity and revocation status to further assess the strength and goodness of a client's PKI certificate.

CRLAutoCache 3.0 for Windows ****Major Update**

Target Audience: System Administrators

Function: CRLAutoCache 3.0 for Windows provides a flexible solution for CRL caching. The tool performs scheduled downloads of configured CRLs with robust retry and failover capabilities. Once CRLs have been downloaded, the tool can inject them into the local Microsoft CRL cache as well as publish them to web servers and network file shares in support of local enclave caching and tiered CRL distribution architectures.



New in this Release: Both NIPRNet and SIPRNet installers are available. The capability to inject CRLs into the local Microsoft CRL cache has been added, and the tool's configuration information is now stored in the registry and updatable via GPO. CRL source download and destination publishing actions may be scheduled individually or in groups. A complete list of configuration options is available in the *CRLAutoCache 3.0 for Windows Administration Guide*. A configuration file containing details for DoD-approved external PKIs is packaged with the NIPRNet installer and can be imported via the administration GUI. The configuration file provides the necessary information for CRLs from the external PKIs to be added to the user or system Microsoft CRL cache (CryptnetUrlCache).

The tool has been rewritten in C# to remove dependence on the Java Virtual Machine (JVM) and provide better Microsoft Cryptography API (CAPI) integration capabilities; it also now runs as a Windows service. Multi-threading with a configurable number of threads has been added for improved performance.

CRLAutoCache 3.0 does not provide support for either retrieval from or publishing to LDAP; however, community need/demand for this feature is currently being assessed and it may be included in a future release.

CRLAutoCache for Linux**Major Update

Target Audience: System Administrators

Function: The CRLAutoCache for Linux utility provides the capability to download DoD and other certificate revocation lists (CRLs) to a local cache on a Linux machine. The tool also has the ability to process downloaded CRLs for use with OpenSSL-based products, such as Apache web server configured with mod_ssl, and Mozilla Network Security Services (NSS). CRLAutoCache for Linux can be scheduled to periodically download CRLs to a local cache automatically.

New in this Release: This tool replaces the downloadCRL tool which was previously used for caching CRLs on Linux operating systems. The tool now provides support for downloading external non-DoD CRLs in bulk (as opposed to one by one) through the use of a configuration file. In addition, a debug feature with network troubleshooting information and enhanced error handling has been added to the tool. Both NIPRNet and SIPRNet versions are available. A configuration file with a list of CRLDPs for all of the DoD-approved external PKIs is distributed with the NIPRNet version.

MailCrypt

Target Audience: End Users

Function: MailCrypt performs bulk decryption and re-encryption of Microsoft Outlook message stores, giving users the ability to decrypt email that was encrypted with an old certificate and optionally re-encrypt it with a current (new) CAC certificate.

New in this Release: MailCrypt has been updated to support Microsoft Cryptography API (CAPI): Next Generation (CNG)-based operating systems, including Windows Vista and 7. Support for installation to a non-default location and 64-bit operating systems has been added, as well as additional performance enhancements to improve the speed of tool execution.

FBCA Cross-Certificate Remover

Target Audience: Desktop Administrators and End Users

Function: The FBCA Cross-Certificate Remover removes and untrusts certificates which cause the cross-certificate chaining issue (described in our fall 2011 newsletter, our *FAQ: DoD Root Certificate Chaining Problems, and the FBCA Cross-Certificate Remover User Guide*) from Microsoft Local Computer or Current User Certificate stores when run as an administrator or non-privileged user, respectively.

New in this Release: Two new tool options have been added: ECA and NODELETE. The ECA option will remove and untrust the SHA-1 Federal Root CA > ECA Root CA 2 cross-certificate in addition to performing the tool's default actions; it should only be used on machines that trust the ECA Root CA 2 and wish to prevent ECA certificates from chaining beyond that root. The NODELETE option will prevent the deletion of any certificates, and only perform the untrusting actions; this option may assist administrators with remote, silent deployment to workstations that may otherwise prompt end users to confirm the deletions. Logic has also been incorporated to address any future cross-certificates issued to DoD Root CA 2

InstallRoot 3.15.2 -A, -E, -J and -S

Target Audience: System and Desktop Administrators

Function: These lettered zip archives contain command-line versions of InstallRoot as well as PKCS7 certificate bundles to support installation of the DoD PKI (-A), ECA PKI (-E), JITC PKI (-J) and NSS and legacy DoD SIPRNet PKI (-S) CA certificates.

New in this Release: 64-bit command-line versions have been added to the Windows sub-directory of the zip archives. User Account Control (UAC) support has been added for Windows 7 and Server 2008. A PKCS7 directory with the standard set of certificate bundles has been added InstallRoot-S, and expired and obsolete certificates have been removed.

For more information and to download DoD PKE tools including those described in this article, visit the Tools page of the DoD PKE website at <http://iase.disa.mil/pki-pke>.



In the Pipeline

90meter SCM Release 22

90m Smart Card Manager (SCM) 1.2.22 is currently being tested by JITC for release to the DoD community. SCM 1.2.22 contains code that offers better support to thin client environments. An unforeseen boundary condition between the middleware and SIPRNet token caused an occasional error to occur during smart card logon (SCL). SCM 1.2.22 addresses the boundary condition to allow for successful SCL. Organizations experiencing issues with SCM 1.2.21 and thin client environments are encouraged to contact pke_support@disa.mil for assistance.

Web Server Auditing Tool (WSAT) Development

The DoD PKE team is working with USCYBERCOM, MARFORCYBER and the USMC to identify requirements and target functionality for the Web Server Auditing Tool (WSAT). WSAT, which was developed as a prototype by USMC in 2006, is a tool which remotely assesses a web server's implementation of PKI-related functionality. For example, the tool can determine whether a server is performing certificate revocation checking or using FIPS-compliant algorithms for connection negotiation. USCYBERCOM has funded the USMC to perform additional development to expand the tool into a robust enterprise capability. Once development is complete, DISA will offer the tool as an enterprise service and provide ongoing operations and maintenance support.

continued on page 5



RA/LRA/KRA Corner



Certification Authority Updates

The DoD PKI PMO has released eight new NIPRNet Certification Authorities (CAs). RAs and LRAs are encouraged to utilize the following NIPRNet CAs, which are operational and now available for certificate issuance:

Certification Authority	Issuance Type
CA-27 & Email CA-27	Software
CA-28 & Email CA-28	Software
CA-29 & Email CA-29	CAC
CA-30 & Email CA-30	CAC

The following CAs have entered maintenance mode and are no longer issuing certificates. RAs and LRAs can still manage certificates issued from these systems.

Certification Authority	Maintenance Mode
CA-21 & Email CA-21	January 26, 2012
CA-22 & Email CA-22	January 26, 2012
CA-23 & Email CA-23	January 26, 2012
CA-24 & Email CA-24	January 26, 2012

Finally, several older CAs that were previously operating in maintenance mode have been decommissioned and are no longer accessible online. Operations related to managing certificates issued from these systems will be affected. Additional older CAs are expected to be decommissioned in the near future. The following NIPRNet CAs have been or will be placed offline, per the decommission dates listed below:

Certification Authority	Decommission Date
CA-11 & Email CA-11	January 1, 2012
CA-12 & Email CA-12	January 8, 2012
CA-13 & Email CA-13	January 22, 2012
CA-14 & Email CA-14	January 8, 2012
CA-15 & Email CA-15	June 13, 2012
CA-16 & Email CA-16	June 14, 2012
CA-17 & Email CA-17	June 14, 2012
CA-18 & Email CA-18	June 14, 2012

Wireless Update

The Department of Defense Chief Information Officer (DoD CIO), Ms. Teresa Takai, signed a memorandum on January 17th, 2012 entitled DoD Commercial Mobile Device (CMD) Interim Policy. The memorandum focuses on three distinct areas related to CMDs:

1. Defining a process for configuring optional security settings in the BlackBerry Security Technical Implementation Guide (STIG) to improve user acceptance and functionality
2. Establishing requirements for the use of non-enterprise activated CMDs
3. Outlining interim steps to support CMD applications in the DoD

The DoD has made a significant investment in BlackBerry devices and infrastructure, and the DoD CIO memorandum emphasizes the fact that DoD Components should consider using their BlackBerry devices to meet mission requirements prior to investing in a new CMD management infrastructure. Many DoD users have the impression that their BlackBerry devices are significantly less capable than their iOS or Android counterparts. While this may be true for older BlackBerry devices, the perception is also influenced by the fact that the DoD locks down many of the features users expect with a CMD, such as the camera, GPS, and social networking. Other CMDs, such as iOS and Android-based devices, would be subject to similar restrictions if deployed in DoD environments.

The memorandum also defines the policy for altering optional security settings in the BlackBerry STIG. Component CIOs must make a risk-based determination when modifying optional settings for BlackBerry devices. Certain values for optional setting in the BlackBerry STIG may still introduce new threats to information stored on user devices or potentially even DoD networks, and thus should be carefully evaluated prior to implementation.

The last two areas are of particular interest for the DoD community, as there is a strong desire to use iOS and Android devices within the DoD. This desire is underscored by the DoD's efforts to develop security configuration guidance for these platforms. The Wireless Update in the Fall 2011 PKE Quarterly Post discussed the iOS 4 Interim Security Configuration Guide (ISCG) and the Dell Android 2.2 STIG, which are both available at http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html.



DoD PKE Website Updates

The DoD PKE team is continually working to improve our website and provide content to meet the needs of the DoD community. Some recent focus areas include:

SIPRNet PKI: You'll notice a new *SIPRNet PKI* tab in our new navigation menu. This page contains all SIPRNet-specific content, including policies, general SIPRNet PKI information, and specific implementation guidance. You'll see the content on this page expand over the coming months as we work to incorporate SIPRNet instructions into our existing product reference guides.

Getting Started: We've identified a need to provide instructions for DoD users, such as reservists, who may require access to DoD PKI-protected web sites from non-GFE or machines not pre-configured by their organizations for use with a CAC. The new *Getting Started* page instructs users on how to configure their machines to read the CAC and use its certificates to access DoD PKI-protected web sites with common browsers such as Internet Explorer, Firefox and Chrome.

Mobile Devices: We've consolidated all things mobile on a single page for easy access. The new mobile page includes BlackBerry, Android, iOS and Windows Mobile sub-pages with information specific to each of the mobile operating systems.

Interoperability: Our *Interoperability* page has been updated with information for new DoD-approved external PKIs such as ActivIdentity Inc. Non-Federal Issuer (NFI), Citi Managed Identity Services NFI, Entrust Managed Services NFI, VeriSign NFI, and Verizon Business NFI. In addition, new information on the policy driving the Federal Bridge and a new graphic reflecting the updated Federal Bridge architecture (as described in our summer 2011 Federal Bridge 2.0 article) have been added to the page.

We've also added a lot of new content to the site since our last Quarterly Post release. See the Recent Tools (or cover story) and Recent Documents sections of the newsletter for a listing of new items available from our site. Looking for something that's not currently available? Email pke_support@disa.mil with suggestions for new content.

Guest Contributor: US Army North

By D. Knight (Security Engineer with FRC) at U.S. Army North, Fort Sam Houston, Texas

Evaluating Copier/Printer/Multi-Function Device PKI Capabilities

Ever heard "All you need is Lightweight Data Access Protocol (LDAP)" from a printer or copier vendor? A recent acquisition order of copiers afforded our Information Assurance office the opportunity to provide security implementation guidance before real dollars were committed. We received a test copier and asked the vendor representative to begin by self-reporting the DISA STIG compliance capabilities of the device and the certificate path validation mechanism. The response said a lot for the vendor's awareness of DISA STIGs, but little for their appreciation of the PKI benefits. When asked to configure the device for Online Certificate Status Protocol (OCSP), the representative explained that no one ever configures that. All you need is to point to an LDAP source and do a user look-up was the response. We asked if the product could do OCSP and were assured it could, but the representative would need to ask his office how to do it.

In our mission, we often support multiple Federal and governmental agencies during emergency preparations and execution. We may have DoD users with us for just a few hours or days in various locations throughout the CONUS AO. In Garrison, LDAP is part of the solution, but LDAP does not provide the flexibility or an authoritative validation check that might avert an opportunistic OPSEC or other attack in the field. If your vendor tells you the device can be DoD PKI compliant, ask them to show the settings and prove it.

*Interested in contributing a guest article to the PKE Quarterly Post?
Email pke_support@disa.mil.*

Thin Client SIPRNet Token Support

The DoD PKE team is currently testing thin clients in use throughout the DoD for their functionality with the new DoD SIPRNet hardware tokens. The PKE team has been working closely with the services and vendor community to test various thin client hardware appliances and software solutions

including Oracle Sun Ray, Wyse, General Dynamics (GD) Tadpole, ClearCube and Hewlett Packard (HP) units. Use cases being evaluated include smart card logon, secure web authentication, digital document signing and encrypting/decrypting email using the SIPRNet token. Thin clients are being

continued on page 7

In the Pipeline - *continued*

HBSS PKI Auditing Plug-In

The DoD PKE team has developed a PKI auditing plug-in proof-of-concept for HBSS designed to assess the PKI configuration of the asset on which HBSS is running. The proof-of-concept is able to examine machine certificate trust stores and evaluated contents against white lists and black lists of certificates. Next steps for the plug-in will be to pilot the capability and incorporate additional configuration checks, with the ultimate goal of integrating PKI configuration auditing into the standard enterprise suite.

BlackBerry Application to Manage Expired OCSP DTM Certificates

DoD BlackBerry users currently experience problems validating digital signatures on emails when they have expired OCSP signing certificates in their devices' certificate trust stores. Because it uses the Delegated Trust Model (DTM) for OCSP signing, the DoD PKI issues new OCSP signing certificates approximately every 45 days; however, the BlackBerry devices are not able to properly recognize and update their trust stores with the new certificates when corresponding expired ones are present. This results in signature validation failing because the device sees the OCSP signing certificate as expired. To alleviate this problem in the short term, the DoD PKE team is working to develop a BlackBerry application to identify and remove expired DoD PKI OCSP signing certificates from a device's certificate trust store. The team is also working with Research in Motion (RIM) to incorporate a fix directly into the device operating system for a long-term fix.



RA/LRA/KRA Contact Information

RA Operations			
Name	Organization	Contact Information	COCOMs Supported
Army	Army CTNOSC Army NETCOM	ctnosc.pki@us.army.mil (Equipment Certificates) army.ra@us.army.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	cgrra@uscg.mil	Not an Executive Agent
Joint Staff	Joint Staff RA Support Help Desk	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	DLA 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

Upcoming Events

DISA Mission Partner Conference 2012

May 7-10, 2012
Tampa Convention Center
333 South Franklin Street
Tampa, FL 33602
Formerly the DISA Customer Conference

2012 Identity Protection and Management Conference (IPMC)

May 15-17, 2012
(Early Bird Session May 14)
The Anaheim Marriott
700 West Convention Way
Anaheim, CA 92802
Register at <https://www.iad.gov/events>
Interested in presenting a topic in the PKE track at IPMC?
Email pke_support@disa.mil.

Working Toward a More Streamlined CAC



The DoD Identity Protection and Management Senior Coordinating Group (IPMSCG) Test and Evaluation Working Group (TEWG) is spearheading the DoD Common Access Card (CAC) certificate reduction effort. The CAC currently contains four certificates, some of which include redundant support for functions such as smart card logon, client authentication, form and email signing. The TEWG is focused on streamlining the certificate capabilities while providing certificates on the CAC that meet the requirements of the DoD CC/S/As.

The DoD PKE team suggested 10 different CAC configuration options for testing. These options featured both modifications to the existing certificate profiles as well as removal of certain certificates. All of the certificate reduction options included removing the Identity certificate and retaining the Encryption certificate. The variations involved modifications to ECU and SAN values on the Email Signature and/or the PIV-Auth certificates. The TEWG has selected a priority subset of the PKE suggested certificate options to be tested by participating CC/S/As. The CC/S/As will have the ability to request other certificate configuration options for additional testing.

The JITC PKI team has provided test certificates matching the proposed test profiles that are issued from the JITC CAs, enabling organizations conducting testing to utilize all of the existing test infrastructure services (including CRL distribution points and OSCP responders) offered by the JITC PKI which mirror DoD's NIPRNet production PKI. The JITC-issued certificates will be loaded onto test CACs by DMDC and sent to CC/S/A TEWG representatives for evaluation. The TEWG has coordinated "quick look" test goals for these CAC configurations and requested volunteers to test different focus areas. Once the test cycle is complete, TEWG members will make a recommendation regarding the preferred future certificate configuration for the CAC based on the test results and CC/S/A requirements.





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 pke_support@disa.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: You might want to throw this one over the fence

Decrypt the encrypted text below to solve:

**MYPNS HP0AA ROMGR RIDOR 'AD'W TAIS4 -VLDT DADMU
BREEA ONUSQ IF12I ENNEN T**

Note: *The PKE Puzzle Corner puzzles are designed to be fun and stimulating mental exercises, solved (and solvable) using your brain and some paper and pencil or perhaps an Excel spreadsheet. Yes, you could have a web site solve them for you, but just because you can doesn't mean you should!*



**DoD
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—
PKE_Support@disa.mil

Fall Quarterly Post Puzzle Solution

Congratulations to MSgt Benjamin R. from DTRA who was the first person to correctly solve the fall puzzle!

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
j	g	r	h	t	i	s	m	a	k	q	y	b	l	f	e	c	p	w	z	d	x	v	n	o	u

Vigenère Cipher Key:
BUILDINGSECURITYIN

Amateurs hack systems professionals hack people ~Bruce Schneier
BGIEHCEY ZEEE JGLRMZT JZZIMFYASPUCA AYKX QYWAOM ~HJYEYJKALMVFL

