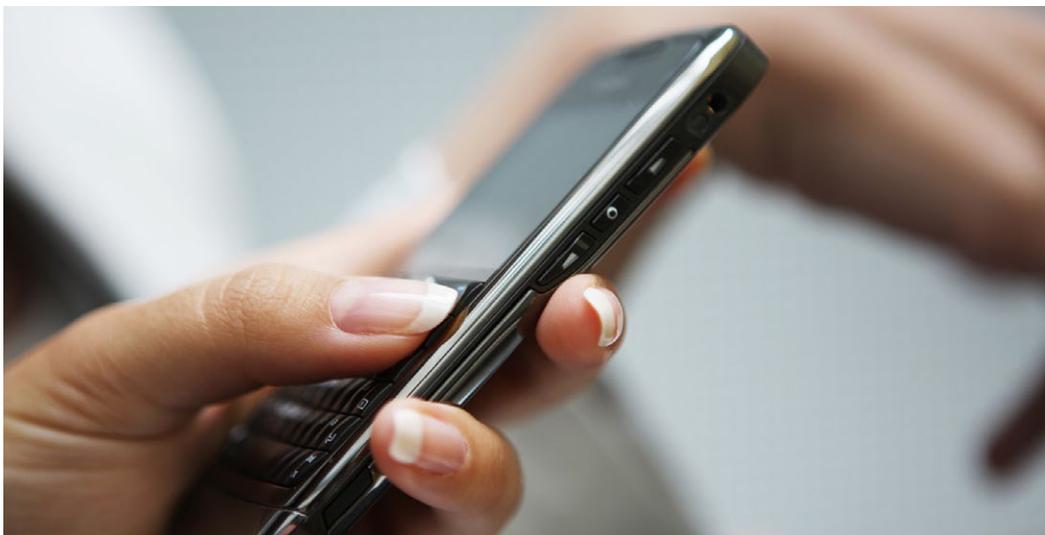


The PKE Quarterly Post

Smart Phones Need Smart Security



Mobile devices like smart phones and tablets are a hot topic for many DoD organizations right now. Understandably, there is high demand to leverage the unique communication and computing capabilities these mobile devices offer on DoD networks.

However, one challenge of a mobile device that's development and design efforts have focused primarily on the user experience is that the security considerations for bringing it into the enterprise have taken a back seat. Furthermore, the technology and deployment scenarios for mobile devices are different enough from PCs that new guidance must be developed to steer our adoption of mobile devices into the enterprise. To that end, the DISA Field Security Office (FSO) has begun to develop Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs) for various mobile technologies; current guides can be found on the DISA Information Assurance Support Environment (IASE) web site at http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html.

These SRGs already require support for the use of DoD PKI. Included in these requirements are common PKI functions such as using S/MIME to secure email with digital signatures and encryption (a function that neither the native Android nor iOS email client supports) and performing PKI-based client authentication to a web site (another function not supported by either Android or iOS's native web browsers today).

continued on page 3

In This Issue

Combined Endeavor	3
Risks of Software Certificates	4
Alternate Revocation Checking Options	5
Which Certificate Profile Should I Choose?.....	6
Digital Signature and Encryption Challenges within Outlook and OWA....	6

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 support a few stand-alone workstations that are not connected to a Microsoft domain. Does DoD PKE have a reference guide for implementing smart card logon (SCL) on stand-alone workstations? Are stand-alone systems required to be PK-enabled?

Microsoft operating systems cannot natively support SCL on stand-alone workstations or servers, as SCL in the Windows environment requires being joined to a Microsoft Active Directory domain.

DoD Instruction 8520.02 *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, dated May 24, 2011 provides guidance regarding the requirements for PK-enabling DoD systems and networks. In Section 2.b of the instruction it states that the directives for PK-enabling do not apply to stand-alone systems that are not connected to the DoD Global Information Grid (GIG). You can find the instruction on the *Policies* page of the DoD PKE website at <http://iase.disa.mil/pki-pke>.

My command is deploying a networked system that leverages the National Security Systems (NSS) PKI. Since the system will not always have connectivity to the DoD Robust Certificate Validation Service (RCVS), how should I configure revocation checking without resorting to downloading the full set of Certificate Revocation Lists (CRLs)?

Since downloading CRLs can be resource intensive, another option to consider for your environment is employing a keyless Online Certificate Status Protocol (OCSP) responder within your network. In this architecture, the OCSP responder within a local enclave periodically connects to DoD's enterprise OCSP responder infrastructure, the Robust Certificate Validation Service (RCVS), to download OCSP proof sets – databases of pre-computed and pre-signed OCSP responses indicating whether the certificate status is good, revoked, or unknown. Since the local OCSP responder is hosting pre-signed OCSP proof sets obtained from RCVS, the responder does not need to secure an OCSP signing key for signing responses itself – hence the term keyless responder. The local OCSP responder can thereby provide the same signed response as the DoD enterprise RCVS in those situations in which the local clients cannot reach outside of their local network. Note that both DoD PKI (NIPRNet) and NSS PKI (SIPRNet) offer proof sets that can be used by keyless OCSP responders.

If you think this capability might be appropriate for your operational environment, you can find our new reference guide for *Deploying a Keyless OCSP Responder Using Axway (Tumbleweed) Validation Authority on the PKE A-Z* page of the DoD PKE website at <http://iase.disa.mil/pki-pke>.

Notes from DoD PKE

Welcome to the Fall Edition of the DoD PKE Quarterly Post. It's been an exciting season for the PKE team with many new initiatives. Headlining those initiatives is PKI and mobile devices. The PKE team has been actively supporting the DISA Mobility Pilot with PKI support for a mixture of Android and iOS devices. The team is focusing on balancing security with a satisfactory user experience and exploring alternatives to traditional smart card readers and software certificates. To learn more about the PKE team's mobile work, please read this issue's cover story, *Smart Phones Need Smart Security*, on page 1. To learn more about the risks of using software certificates on mobile devices, please read the article *Risks of Software Certificates* on page 4. The DoD PKE team will be hosting the second DoD PKI Mobility TIM on November 28th. It will be an open forum for exchanging information on ongoing pilots, capability gaps and implementation challenges. If you are interested in attending the TIM, please send a request to dodpke@mail.mil.

This September the DoD PKE team traveled to Grafenwöhr, Germany to support the European Command (EUCOM)-sponsored Combined Endeavor 2012 exercise. The team deployed the PKI for the exercise and provided PKE support to NATO and Partnership for Peace member nations' pre-testing and troubleshooting efforts in advance of their formal PKI test execution.

The exercise highlighted one of our common challenges within DoD – the need to provide alternative certificate revocation checking methods for disconnected and low-bandwidth environments. The DoD PKI PMO offers a variety of Tumbleweed and CoreStreet proprietary mechanisms that an organization can leverage. For more information on alternate revocation checking, please read the *Alternate Revocation Checking* article on page 5 and also refer to the DoD PKE slick sheet *Alternate Certificate Revocation Checking Options* available on the DoD PKE website, <http://iase.disa.mil/pki-pke>.

And just as a reminder – we have migrated to Defense Enterprise Email. Our new email address is dodpke@mail.mil. Our old pke_support@disa.mil address has ceased forwarding, so please make sure you have updated your contact record!



Smart Phones Need Smart Security – continued

Other relevant PKE uses cases for mobile devices include digitally signing documents and performing client-authenticated TLS for WPA2-Enterprise secured WiFi or IPsec virtual private networks (VPNs).

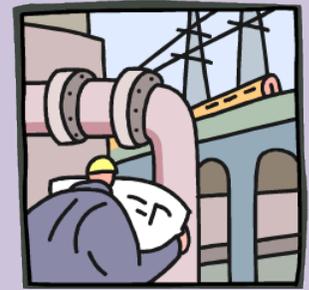
The mobile technology industry is already developing software to meet some of these use cases, and some have software available today. BlackBerry in particular offers reasonably complete support for PKI. However, the PK-enabling technologies available for Android and iOS are somewhat less developed and suffer from severe interoperability shortcomings. While applications on your PC may refer to a middle-ware provider's PKCS11 library to communicate with a security token's driver, the current state of affairs for mobile applications is to include all necessary drivers and middleware into the application itself. This means every PK-enabled application comes with a short list of supported smart card readers. To help address these limitations, DISA is piloting a variety of implementation approaches as well as working with vendors to bridge the gap.

DISA is currently conducting a mobility pilot with a mixture of Android and iOS devices. This pilot effort is currently using the baiMobile 3000MP Bluetooth Smart Card Reader and the Good for Enterprise email client to provide S/MIME security for DoD Enterprise Email. Future spirals of the DISA mobility pilot will feature client-authenticated web browsing on iOS devices using the Thursby PKard Reader App and two additional smart card readers: The Thursby

PKard Reader and the Precise Biometrics Tactivo. The latter smart card readers attach directly to iOS devices and eliminate the Bluetooth pairing process that many users find cumbersome with their Bluetooth smart card readers.

DISA is also considering a BlackBerry pilot that seeks to eliminate smart card readers altogether. Instead of using a CAC to store user credentials, this pilot is exploring the use of a similar hardware security module (HSM) to what exists on the CAC, but packaged in a microSD form factor. DISA will be using the microSD HSM to store user credentials, and present the credentials to the BlackBerry handheld using mobile middle-ware. This solution allows both S/MIME secured email and client-authenticated web browsing. From a usability standpoint, this solution will appear very similar to software certificates, but will protect the user's private key inside a FIPS 140-2 level 3 validated hardware token.

PKE lessons learned from these pilots will be shared at PKI Mobility Technical Interchange Meetings (TIMs) hosted by DoD PKE. The first TIM was hosted in June of 2012 and included representation from CC/S/A PKI offices as well as mobility offices and pilots across DoD. In November of 2012, DoD PKE will host a second TIM which will be open to observers from federal agencies in addition to DoD stakeholders. If you represent a PKI office or mobile device pilot effort within DoD or elsewhere across the federal government and are interested in attending, please email dodpke@mail.mil for additional information.



In the Pipeline

New Intermediate CAs Planned for Winter 2013

New DoD PKI intermediate identity and email Certification Authorities (CAs) 31 and 32 are scheduled to be deployed this winter. Once the CAs are deployed, DoD PKE will publish a new version of InstallRoot to help the DoD community with installing these new certificates before CAC issuance begins. Stay tuned for more information in our next newsletter.

Upcoming Events

PKI Mobility Technical Interchange Meeting (TIM)

November 28, 2012

1 PM – 3 PM EST

Arlington, VA

Dial-in and DCO session available for remote attendees. Please email dodpke@mail.mil for additional details if you would like to attend.

Combined Endeavor

For three weeks this September, PEO-MA deployed a team of engineers to support the EUCOM-sponsored Combined Endeavor exercise, a communications and information systems interoperability testing exercise between the North Atlantic Treaty Organization (NATO) and Partnership for Peace (PfP) nations. Combined Endeavor is the largest international Command, Control, Communications & Computers (C4) exercise in the world. The exercise took place September 6-20 at the Joint Military Training Command on U.S. Army Garrison Grafenwöhr, Germany and included participants from 39 countries and two multinational organizations.

Combined Endeavor testing simulates the conditions of a multinational C4 deployment and helps to eliminate "discovery learning" down range. More than a thousand interoperability tests were conducted this year, including PKI testing which verified products performed

certificate validation correctly for valid, revoked and untrusted certificates. Test results are collected, compiled and ultimately added to the integrated interoperability guide that has been maintained by the Joint Interoperability Test Command (JITC) since the establishment of the exercise 18 years ago.



continued on page 4





RA/LRA/KRA Corner

Documentation for DoD Registration Authority Officials

The DoD PKI is continually updating and expanding its capabilities to provide additional security services to the DoD CC/S/As. With the infrastructure constantly evolving, the DoD PKE team understands the need for a centralized location where RA Officials can obtain the latest documentation relevant to their responsibilities. To meet this need, the DoD PKE team hosts and regularly updates the *For RAs, LRAs, KRAs & TAs* section on the IASE website at <http://iase.disa.mil/pki-pke/>. At the time of writing, the site contains:

- LRA, RA and KRA training decks updated with the latest available information
- Training schedule for LRA, RA and KRA classes offered by the DoD PKI PMO
- Classroom registration procedures outlining the steps necessary to nominate and register students for LRA, RA and KRA training classes
- Nomination templates required to be completed for students obtaining production credentials
- 90meter Certificate Issuance Workstation (CIW) software for SIPRNet RA workstations
- Troubleshooting guides addressing common LRA, RA and KRA problems

All the documentation on this site is PKI-protected and only accessible with a DoD PKI certificate. If you do not currently possess a DoD PKI certificate and require access to information included on the site, please contact the DoD PKE team at dodpke@mail.mil.

RA/LRA/KRA Contact Information

RA Operations			
Name	Organization	Contact Information	COCOMS Support
Army	Army CTNOSC Army NET-COM	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	disa.meade.CIO.mbx.disa-ra-operations@mail.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

Combined Endeavor – continued

PKI secure email tests required nations to exchange digitally signed and encrypted email. Web services testing required each nation to establish a mutually authenticated SSL connection to another nation's website using each type of client certificate. Throughout the testing, data collectors independently observed and recorded the results of each test and other relevant information to develop lessons learned for the final interoperability guide.

The PKI team was part of the Services Technical Working Group (TWG) within the Coalition Joint Task Force (CJTF). The Services TWG included members from Denmark, Finland, Estonia, Slovenia, and the United States. The PKI team was responsible for deploying the Combined Endeavor PKI on the core testing network, including building the Coalition Root Certification Authority (CA), a Coalition Subordinate CA, a router CA to support IPSEC certificate issuance for backbone routers, an OSCP responder, and an Untrusted CA. The team also deployed a PKI information web site that included certificate enrollment links, CA certificate and Certificate Revocation List (CRL) distribution information, and a client authentication test page to support member nations' pre-testing and troubleshooting efforts in advance of their formal PKI test execution. Once the infrastructure was deployed, the team provided PKE technical support to participating nations throughout the exercise.

Nations participating in PKI testing for Combined Endeavor 2012 included Albania, Armenia, Belgium, Estonia, Finland, France, Hungary, Italy, Ireland, Kazakhstan, Kyrgyzstan, Macedonia, Moldova, Montenegro, Portugal, Romania, Serbia, Slovakia, Slovenia and Ukraine.

Risks of Software Certificates

Recently, there has been a lot of discussion and controversy around the use of private keys certified by DoD PKI and stored in software. Commonly these types of private keys, along with their corresponding certificates, are called software certificates. The certificates contain an identifier that distinguishes them from certificates that correspond to private keys stored in hardware cryptographic modules. The request for software certificates is driven by a renewed interest in mobile device use in DoD combined with dislike of the current CAC reader solutions available for those mobile devices.

continued on page 5



Risks of Software Certificates – *continued*

DoD PKI has offered software certificates on the NIPRNet and SIPRNet for many years. The most common types of software certificates assert the identities for web servers, Microsoft Active Directory Domain Controllers, and other network appliances, and are designed for specific authentication capabilities such as TLS, IPSEC, and Microsoft's PKINIT protocol. DoD PKI has also offered (on a very limited basis on the NIPRNet and now via a legacy capability on SIPRNet) software certificates asserting the identities of human DoD PKI subscribers. These software certificates provide a PKI subscriber many of the same capabilities as the certificates found on the CAC – email decryption, email signing, and authentication to DoD web sites.

It is the software certificate for human subscribers that draws the most interest when trying to integrate DoD PKI with mobile devices. PKI subscribers do not want to use CAC sleds with their BlackBerry, Android or iOS devices; they are just too clunky and clumsy! Software certificates offer easy integration and use on a mobile device.

However, software certificates used on end user devices can drastically reduce the assurance of a DoD PKI subscriber's identity (and pose risks to DoD systems relying on these identities) if not adequately protected. Software certificates can

be copied, are not guaranteed to be encrypted when stored, and do not have lock-out protections against guessing the unlock passphrase used to access the private key. Software certificates also provide a management challenge to the PKI subscriber and system administrator. Subscribers that frequently change devices will need to ensure their software certificates change with them or risk losing access to websites and email. During the transfer, a copy of the original private key will be made with no guarantee the original private key will be deleted after the transfer, leading to the unanswerable question "How many copies of this private key exist?" Additionally, not all applications support the use of software certificates; some require hardware certificates when authenticating people.

The protection of software certificates to satisfy identity assurance requirements depends on the proper behavior of the PKI subscriber, the system administrator and properly functioning platform protections such as anti-virus, file access permissions, and patch management. These requirements are difficult to enforce and audit when the operating environment consists of a large number of devices in a geographically disperse enterprise subject to a wide range of threats.

Alternate Revocation Checking Options

A critical component of Public Key Infrastructure (PKI) is the requirement to check if a certificate has been revoked. It is the responsibility of the relying party to check revocation status and make a decision to accept or reject the certificate. It is especially important to ensure certificate validation is performed efficiently to minimize impact to users, networks, and the DoD PKI. Certificate revocation checking in the DoD presents a unique challenge due to the size of the revocation data and the wide variety of clients and networks within the DoD. To this end, the DoD PKI PMO provides a variety of certificate revocation checking services that can be leveraged to alleviate the challenges associated with revocation checking in the DoD.

The primary resources for revocation checking are Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP). Although the primary resources have proven to be successful and reliable for the majority of infrastructures in the DoD, larger sizes of revocation data and increased implementation of PKI in tactical environments has led to a growing need for more compact and efficient forms of revocation checking resources.

The DoD PKI PMO offers a variety of alternative ways to do certificate revocation checking using Tumbleweed (TW) and CoreStreet (CS) proprietary mechanisms such as OCSP proofs, compact CRLs, delta CRLs and miniCRLs.

Tumbleweed supports OCSP proofs, compact CRLs, and delta CRLs. CoreStreet supports OCSP proofs and miniCRLs. OCSP proofs are pre-computed, pre-signed OCSP responses which enable in-house Tumbleweed or CoreStreet responders/repeaters to issue DoD OCSP responses without having to constantly reach back to RCVS. Compact CRLs and miniCRLs are compressed forms of the full CRLs, while delta CRLs are CRLs that only reflect changes that have occurred in a full CRL since a previous update. Alternative revocation checking resources can be leveraged in a variety of ways to improve and facilitate an organization's revocation checking capabilities.

For more information, please refer to the slick sheet *Alternate Certificate Revocation Checking Options* available from the DoD PKE website at <http://iase.disa.mil/pki-pke>.

Latest Document Releases

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

New

Axway Validation Authority: Deploying a Keyless OCSP Responder – This guide provides instructions for deploying a keyless OCSP responder using Axway (previously Tumbleweed) Validation Authority and DoD OCSP proof sets.

iPad 3: Pairing with a baiMobile 3000MP Smart Card Reader (SCR) – This guide provides step-by-step instructions for pairing a baiMobile 3000MP SCR with an iPad 3 to enable the smart card digital signature and encryption functionality of the Good for Enterprise email client.

iPhone 4S: Pairing with a baiMobile 3000MP Smart Card Reader (SCR) – This guide provides step-by-step instructions for pairing a baiMobile 3000MP SCR with an iPhone 4S to enable the smart card digital signature and encryption functionality of the Good for Enterprise email client.

Motorola Droid Razr: Pairing with a baiMobile 3000MP Smart Card Reader (SCR) – This guide provides step-by-step instructions for pairing a baiMobile 3000MP SCR with a Motorola Droid Razr to enable the smart card digital signature and encryption functionality of the Good for Enterprise email client.

iPhone 4S: CAC-Enabled Web Browsing Using the Thursby PKard Reader Smart Card Reader (SCR) and the Thursby PKard Reader Application – This guide provides step-by-step instructions for initial setup and basic CAC-enabled web browsing on an iOS device using the Thursby PKard Reader Smart Card Reader (SCR) and the Thursby PKard Reader Application (App).

Major Updates

Adobe Acrobat and Reader 9 and 10: Leveraging Microsoft CAPI for Certificate Validation – This guide documents the steps to configure Adobe to leverage MS CAPI for verifying certificate trust and revocation when performing digital signature validation. This release adds instructions for configuring version 10 of the products.



Which Certificate Profile Should I Choose?

There are currently six different certificate profile types that can be requested from the certificate enrollment page for the DoD PKI, and it's not always easy to tell which one you should use for your particular configuration. The following tables describe the six profile options and discuss when to use each:

Certificate Type	Certificate Use
Manual PKCS10 Domain Controller 2048-bit Certificate	The domain controller profile is configured to support domain controllers <u>only</u> and should not be used for any other server type.
2048-bit Alternate Login Certificate	The Alternate Login profile is typically used for administrator accounts that require a separate credential from an administrator's regular user account, for those who are not eligible for a CAC, and other users who require Alternate Logon Tokens (ALTs); see the <i>Alternate Logon Token</i> slick sheet on the <i>PKE A-Z</i> page of the DoD PKE website at http://iase.disa.mil/pki-pke for a more detailed discussion of ALT use cases and user communities. This profile allows for smart card logon but does not contain an extended key usage (EKU) for an email address.
DoD Mobile Code 2048-bit Certificate	The DoD Mobile Code profile is used to generate certificates that will sign DoD code and uniquely identify the organization that signed the code.

The previous three profiles are fairly straightforward and easy to understand; however, the SSL and Multi-SAN certificate types can be more confusing.

Certificate Type	Certificate Use
Regular 2048-bit SSL Server Certificate	The Regular 2048-bit SSL Server Certificate profile is a legacy profile that only provides the option to specify a Common Name (CN) value. The New 2048-bit SSL Server Certificate profile provides additional options, making it a more versatile profile type.
2048-bit Multi-SAN Server Certificate	The 2048-bit Multi-SAN server profile was created to allow the use of multiple Subject Alternative Names (SAN) for use in implementations such as web servers with multiple IP addresses or URLs, load balanced servers and storage servers. This capability is also included in the New 2048-bit SSL server profile type.
New 2048-bit SSL Server Certificate	The New 2048-bit SSL server profile provides the CN value and multi-SAN option, as well as other usages such as Server Authentication, Client Authentication, IP security IKE intermediate, and Any EKU. This certificate profile is the most flexible and should be used in most cases.

Digital Signature and Encryption Challenges within Outlook and OWA

When you encrypt an email to a recipient, your system uses the recipient's public key to encrypt the email. Once encrypted, the email can only be decrypted using the private key corresponding to the public key used to encrypt it, thus ensuring that only your intended recipient can decrypt the message using their own private key. However, this means that in order to send an encrypted email to a recipient, your system must have access to the recipient's public key.

Microsoft email applications will first check the Global Address List (GAL) for a recipient's encryption certificate (which contains their public key) based on the recipient's email address. This means that if Jane Smith has an entry with an associated public certificate, but her email is listed as jane.smith@agencyx.mil in the entry and you

are trying to send to jane.smith@servicey.mil, the application will not be able to find Jane Smith's certificate. If no matching certificate is found in the GAL, Outlook will also check the Local Contact records; however, Outlook Web App (OWA) will not. If a certificate cannot be found in the GAL (for Outlook and OWA) or the Local Contact records (for Outlook only), encryption to the recipient will fail.

So what if your GAL record or Local Contact contains jane.smith@agencyx.mil and you want to encrypt email to jane.smith@servicey.mil? Or what if jane.smith@servicey.mil exists in your GAL or Local Contacts, but her certificate's RFC822 name is jane.smith@agencyx.mil?

continued on page 7



Digital Signature and Encryption Challenges within Outlook and OWA- *continued*

The name mismatch issue can be addressed on a workstation running Outlook by (1) creating a Local Contact record that contains all of the contact's email addresses and (2) setting the **SupressNameChecks** registry key to true (which tells the machine to ignore whether the RFC822 name in the certificate matches the email address being used). This will allow you to encrypt email to the contact at any of their addresses regardless of the RFC822 name contained in the certificate for the contact. More details on how to set the **SupressNameChecks** registry key can be found in DoD PKE's *Microsoft Outlook XP, 2003, 2007 and 2010: Suppress Name Checking* guide available from <http://iase.disa.mil/pki-pke> under *PKE A – Z > Guides*. In order for Jane to decrypt email that she receives at an address other than the one listed in her certificate or send digitally signed email from such an address, she will also need to have **SupressNameChecks** set on her workstation.

On the Exchange server, the name mismatch issue can be alleviated by entering additional email addresses as alternate SMTP addresses within the user's account, which (when the **UseSecondaryProxiesWhenFindingCertificates** registry key in Exchange is set to its default of true) will enable the system to find the appropriate user record for all listed addresses. However, if the alternate SMTP addresses are not owned by the Exchange system

to which they are being added – for example, if Jane Smith has a separate email account with Service Y, and the Agency X Exchange administrators add `jane.smith@servicey.mil` as an alternate SMTP address – the Agency X system will hijack all mail sent from Agency X users to `jane.smith@servicey.mil` and redirect it to her `jane.smith@agencyx.mil` address. She will never receive the email from Agency X senders at her `jane.smith@servicey.mil` address, which may not be desired behavior for either Jane or Service Y.

On OWA, for recipients who don't exist in the GAL (or whose alternate addresses aren't entered as alternate SMTP addresses in their Exchange account), there is no way to encrypt email. To enable users with name mismatches (and no alternate SMTP addresses) to digitally sign email from OWA, Exchange administrators can set the **AllowUserChoiceOfSigningCertificateExchange** registry entry as described in <http://support.microsoft.com/kb/2497165>.

The table below summarizes necessary settings to enable encryption in various scenarios; for all cases, it assumes that Jane Smith has an Agency X Exchange account and GAL record with a primary SMTP address of `jane.smith@agencyx.mil`.

Recipient Address	Certificate RFC822 Name	Email Client	Special Settings to Successfully Encrypt Email from Agency X to Recipient
jane.smith@agencyx.mil	jane.smith@agencyx.mil	Outlook	None
		OWA	None
jane.smith@agencyx.mil	jane.smith@servicey.mil	Outlook	Set SupressNameChecks registry key to true on sender's workstation
		OWA	*Add <code>jane.smith@servicey.mil</code> as alternate SMTP address within Jane's Agency X Exchange account
jane.smith@servicey.mil	jane.smith@servicey.mil	Outlook	Create Local Contact record that includes <code>jane.smith@servicey.mil</code> in sender's Outlook address book
		OWA	*Add <code>jane.smith@servicey.mil</code> as alternate SMTP address within Jane's Agency X Exchange account
jane.smith@servicey.mil	jane.smith@agencyx.mil	Outlook	Create Local Contact record that includes <code>jane.smith@servicey.mil</code> in sender's Outlook address book AND Set SupressNameChecks registry key to true on sender's workstation
		OWA	*Add <code>jane.smith@servicey.mil</code> as alternate SMTP address within Jane's Agency X Exchange account

***WARNING:** This will cause all email sent from Agency X users to `jane.smith@servicey.mil` to be redirected to her `jane.smith@agencyx.mil` account.





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:

You should **automatical-key** think of Girolamo Cardano when contemplating this enciphered haiku. The American Cryptogram Association would get its start with a tabula recta and this 1920s weekly publication.

Decrypt the encrypted text below to solve:

VSYXYTZZ TQIVYWFZK QMTJGV

TZP'S FNGJUGP YEZGMCC

KG RWJLP, SARFXE

Spring/Summer Quarterly Post Puzzle Solution

Congratulations to Ms. Cynthia J. of the US Army Cyber Leader College, who was the first person to correctly solve the spring/summer puzzle!

Cipher: Affine, a=3, b=12

Three may keep a secret, if two of them are dead. – Benjamin Franklin

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

T E K A R I O H R A B A F K
H E M Y E P S C E , F W O T E A E E D - E J M N R N L N
R A E E T T F M D . N I A I

