



# The PKE Quarterly Post

## Why isn't my favorite touch screen device part of a DOD approved unclassified mobile messaging solution?

by Ross N. Schwalm



Steve Jobs has created quite a stir in the personal mobile phone industry. The "there's an app for that" slogan has many government users wondering why they can't use a device that may better suit their needs. Innovation from Android, Palm WebOS, and Symbian S60 device makers means it is only a matter of time before they draw the same demand. DOD PKE Engineering Support wants the DOD community to understand the current requirements for mobile messaging solutions, existing solutions, and the current status of these new devices becoming part of an approved solution.

### Requirements for Mobile Messaging Solutions

The basic requirements for a mobile messaging solution (besides an email infrastructure) are a remote policy management capability, mobile device security (Federal Information Processing Standard (FIPS) 140 validated data-at-rest encryption, device configuration control, approved anti-virus, and firewall), support for a smart card reader (SCR), and Secure/Multipurpose Internet Mail Extensions (S/MIME). Unfortunately, when attempting to meet all these requirements, "there's NOT an app for that." As discussed in the last issue of *"The PKE Quarterly Post,"* S/MIME is a standard that allows users to send and receive encrypted and digitally

signed emails by utilizing an existing Public Key Infrastructure (PKI). A mobile messaging solution usually consists of one or several devices with a specific operating system, a mobile device policy management client/server, and a specific SCR to support the required S/MIME functionality and smart card logon. Additionally, the solution's encryption module (the device's operating system and/or third party overlay) must be validated against the most recent version of FIPS 140, which is currently 140-2. Prior to DOD approval, the National Security Agency (NSA) evaluates the implementation of its security capabilities. If NSA's tests are passed, a Security Technical Implementation Guide (STIG) or security checklist must be written by the DISA Field Security Office and approved/published by the Defense Security Accreditation Working Group to be considered a DOD approved solution. Published security checklists can be found at

*continued on page 2*

### In This Issue

New SECRET Level PKI for the DOD and Our Federal Partners.....	3
The Combined Endeavor Experience.....	4
Coalition PKI .....	5
Use of Approved the DOD External Certification Authority (ECA) Program .....	5
IPM Conference 2010: Extending the Bridge to Our External Partners.....	6
DOD and Microsoft PKI TIM Slides Available.....	6

### In Every Issue

Ask the Expert .....	2
Notes from DOD PKE.....	2
RA/LRA/TA Corner .....	4
In the Pipeline .....	4
Upcoming Events.....	6





## Ask the Expert

### DOD Root CA-2 Cross Certificate (expiration 3/3/2011)

**Question:** I am having trouble accessing DOD web sites. When I click on my certificate it shows the DOD Interoperability CA 1 in the trust path, what should I do?

**Answer:** DOD workstation misconfigurations can cause improper chaining behavior. Please follow the steps listed in the Cross Certificate Issue document on DKO at <https://www.us.army.mil/suite/page/21166734>

### Deployment of New Public Key Infrastructure (PKI) Certification Authorities (CAS)

**Question:** I am unable to logon to Network after receiving new CACs issued from the newly deployed PKI certificate authorities.

**Answer:** Recently we have received reports where system administrators have said they have had to actually reinstall the certificates several times before users with certificates issued from these CAs were able to successfully log in to the network.

The DOD PKI will occasionally add new CAs to issue CACs. When new CAs come online there are 3 steps that need to occur to make sure that users with CACs with certificates issued by the new CAs are able to login to the network and access web servers. DOD is currently using several methods to get the word out to the field regarding new CAs. These include the DOD Tech Leads mailing list and the JTF-GNO INFOSPOT (<https://www.jtfgno.mil>).

1) All of the most current root certificates must be installed on both the servers and workstations. InstallRoot is a utility used to manage DOD authorized PKI credentials (or root certificates) issued by Trusted Root Certification Authorities and Intermediate Certification Authorities on Microsoft servers and workstations.

*continued on page 3*

## Notes from DOD PKE

by Carmella Webster, PKE Team Lead

It is conference season for DOD PKI and we are putting our efforts into making it a great one. We value this time of year, as it presents opportunities to interface directly with our customers and encourage collaboration amongst the community. We plan these events with your interests in mind and encourage your suggestions and feedback. We just returned from a fruitful Microsoft Technical Interchange Meeting (MS TIM) and the Information Assurance Symposium (IAS). Still to come are the Identity Protection and Management Conference (IPMC) and the DISA Customer Conference. You can find information about past and upcoming conferences throughout this newsletter. There is still time to provide input into the IPMC so please send your suggestions to [pke\\_support@disa.mil](mailto:pke_support@disa.mil).

In addition to conference preparation, the PKE team spent the majority of last quarter addressing two reoccurring topics 1) certificate validation and 2) External Partner PKIs. Certificate validation concerns and questions are being generated by both large and small implementations: from enterprise solutions with world-wide servers validating thousands of users per minute to a single server whose only validation requirement is for one pre-defined server certificate. While there is information published on the types of certificate validation solutions available, it is often unclear to implementers which solution best fits their environment. There are several factors that feed this decision and the PKE Team is often involved with helping our DOD customers identify these factors and ultimately choose and implement a solution. Recently we have partnered with some large Programs of Record within DISA to help engineer their certificate validation solutions. From this partnership, we will gain hands-on experience

which will allow us to improve on the guidance and documentation we currently have. One outcome will be a best practice guide with definitive factors to consider and thresholds that will guide the decision making process. To compliment the best practice guide we will be publishing configuration guidance specific to use; servers, desktops, domain controllers, etc.

Accepting PKI credentials from partners external to DOD is beginning to be discussed and sometimes encouraged from the top down. PKE is working this issue from the bottom up – looking at the technical feasibility of this capability and what products are available to support with establishing and verifying trust relationships between PKIs. We believe in the concept of leveraging PKI credentials issued by partner PKIs tested and approved for use within the DOD. It makes sense to use these credentials and not expend resources to recreate them. At the same time it is incumbent upon relying parties (in this case DOD) to use these credentials responsibly; to ensure and maintain security within DOD networks. Currently, most applications are immature in supporting cross certification functionality which enables use of the federal bridge while maintaining trust, assurance and verification. In addition to limited product support, information dissemination has also been limited yet needed to various levels within organizations. This change will affect Chief Information Officers, business process owners, developers, operators, testers, certifiers and users. In the upcoming months, the DOD PKE Team will be assisting with clarifying policy, documenting use and overall awareness on this issue. Look for updates on <http://iase.disa.mil/pki/pke>.

### Favorite Touch Screen Device – *continued*

<http://iase.disa.mil/stigs/checklist/index.html>. It is important to note that individual DOD components may perform additional evaluations or require supplemental controls to be applied prior to approving implementation.

### Currently Approved Solutions

Research in Motion's (RIM) BlackBerry Enterprise Solution accounts for approximately 90% of DOD mobile messaging solutions. RIM controls both the hardware and software in their BlackBerry devices, ensuring granular control of the security configuration (e.g. password requirements, required/disallowed applications, etc.) through the BlackBerry Enterprise Server without relying on third party software. BlackBerry devices provide a personal firewall and FIPS 140 validated data-at-rest encryption that can be enforced from the BlackBerry Enterprise Server. Anti-virus software is not required for BlackBerry's. RIM also has an S/MIME package and an approved Bluetooth SCR.

Windows Mobile devices provide an alternative solution. A Windows Mobile device cannot natively meet the requirements of an approved mobile messaging solution, but two vendors have developed overlays to meet those requirements, Trust Digital and Good Technology. Both solutions include a policy enforcement server and a mobile device client for several Windows Mobile 5.0, 6.0, and 6.1 devices. They both provide the necessary personal firewall, device configuration management, and FIPS 140 validated data-at-rest encryption capabilities, but an approved anti-virus application still must be installed on the mobile device. The Biometrics Associates' (BAI) baimobile Bluetooth SCR and Apriva's BT100-C and BT200 Bluetooth SCRs are compatible with both overlays. Trust Digital's solution utilizes the native Windows Mobile S/MIME mail client capability, while Good's solution uses Good S/MIME. For completeness, it should be noted that the Apriva SensaMail System provides another alternative mail client capability, but it still relies on the Trust Digital solution to meet all the requirements.



## Favorite Touch Screen Device – *continued*

Future of iPhone, Android, Palm WebOS, and Symbian S60 Approved Government Usage

The good news is both mobile device clients from Trust Digital and Good Technology support all four types of devices today. The bad news is that it is not the same client that is part of the approved mobile messaging solutions described above.

Many capabilities including configuration management and personal firewall are available, but FIPS 140 validated data-at-rest encryption, S/MIME and SCR support are important missing capabilities. These are not small pieces, but there seems to be a big enough demand that one of these vendors, or possibly a new vendor, will want to position itself to control the market.

## New SECRET level PKI for the DOD and our Federal Partners

by Sam Fuson

### Background

A major goal of the Department of Defense Public Key Infrastructure (DOD PKI) Program's Increment 2 is to develop a PKI for the SIPRNet that is distinct from the NIPRNet while still offering many of the same products and services available to current unclassified users (e.g. Hardware Tokens). To accomplish this goal, the DOD has been working closely with our Federal Partners to institute a PKI for all federal departments and agencies at the Secret level. The Committee on National Security Systems (CNSS) Policy Number 25 now establishes the hierarchical NSS-PKI to support this initiative. This enhancement consists of implementing a National Security Systems (NSS) Root Certificate Authority (CA) and new SIPRNet Subordinate CAs in addition to centralizing the Token Management Services (TMS) to support certificate and token management on the SIPRNet. Similarly other departments and agencies will develop and deploy Subordinate CAs that will also be signed by the NSS Root.

### Major Activities to Date and Next Steps

The NSS PKI Member Governing Body was established with the responsibility for maintaining the NSS CP and for reviewing Certificate Practice Statements (CPS) of Agency CAs for compliance with the NSS CP. The DOD PKI Program Management Office (DOD PKI PMO) is a co-Chair of the NSS PKI Member Governing Body that drafted both CNSSP No. 25 and the NSS Certificate Policy (CP), which were approved in March 2009.

The SIPRNet PKI Hardware Token Pilot is currently underway. At the conclusion of the pilot the results will be reviewed and final preparations made for the initial fielding of a fully interoperable Secret level PKI capability. In the near-term all current SIPRNet products and services will remain intact until such time that graceful retirement occurs.

### Key Differences

There are several key differences from our Unclassified PKIs—

- Private keys associated with certificates issued by the NSS PKI are considered Secret, Certificates issued by the NSS PKI are considered unclassified.
- Due to hardware tokens being considered Secret once a private key has been generated on the token, the National Security Agency (NSA) is working with token vendors to develop and approve one or more tokens that contain sufficient protection for the token to be considered unclassified when the private key is not in an active status.
- This enhancement consists of implementing a NSS Root CA and new SIPRNet CAs in addition to centralizing the TMS to support certificate and token management on the SIPRNet. SIPRNet certificates will be issued by the NSS Root CA not the DOD Root CA.
- An Authoritative Data Source will be implemented to assign a unique identifier to each SIPRNet user. The unique identifier for any user will be the same as the NIPRNet unique identifier for that individual, if it exists.
- Web-server certificates will not be available upon initial release. It is anticipated that these certificates will be available approximately six months after fielding.
- As specified in the NSS CP, the NSS PKI requires that all of the following be verified prior to issuing certificates to named individuals.
  - **Identity**—applicants must appear in person and present either a valid PIV card or two forms of identity source documents in original form from the list of acceptable documents included in OMB Form I-9. At least one of these documents shall be a valid State or federal government-issued picture identification.

## Ask the Expert - *continued*

There are five command line versions of the InstallRoot application available. We suggest installing version A. The current version is 3.13.

InstallRoot is available on the DOD PKE website in the Downloads section—<https://www.us.army.mil/suite/page/474113>

2) The new CA certificates need to be loaded into the Trust Store.

Running the latest version of InstallRoot will install the new CA certificates into the Local Machine Trust Store. In the scenario where IIS is joined to a domain, please use the following instructions—

In order for the domain controller allow logon by accepting a user certificate that has been issued by a new CA, any new email CA's certificate must be loaded into the ENTERPRISE NTAAuth Store. Note that once these are added there will be a replication delay (normally 24 hours) before the information is available throughout the forest. The new CA certificate should also be loaded into the Trusted Root Store. For users who do not have DKO accounts there is a secondary site available to obtain the InstallRoot utility. <https://www.dodpke.com/installroot>.

See the following article on Microsoft's website—<http://support.microsoft.com/kb/295663>

3) Ensure your CRL caching solutions or OCSP clients are configured to retrieve the new CRLs. If you are using third-party tools that require individual entries per CA/CRL, please add new entries for the new CRLs.

*continued on page 4*





## RA Corner

### DOD Medium Assurance PKI RA/LRA Reference CPS Update

The final discussion on the draft Combined DOD Medium Assurance PKI Registration Authority/Local Registration Authority (RA/LRA) Reference Certificate Practice Statement (CPS) took place 9 Dec 2009 at the Certificate Policy Management Working Group (CPMVG) meeting. The draft was approved and is now available on the IASE website at <http://iase.disa.mil/cpmwg/doclibrary/doclibrary.htm>



## In the Pipeline

The PKE team recently found an issue within the Robust Certificate Validation Service (RCVS) which prevents the OCSP client inherent to newer Microsoft operating systems from being able to check certificate revocation status. This MS client is built into Windows Vista and Windows 7 and helps eliminate the need to download large CRLs or utilize additional software to perform this function. DOD PKE has been working with the RCVS team to develop a solution to this problem and hope to have a fix implemented within the first quarter of 2010.

## SIPRNet – continued

- **Clearance**—the applicant must possess a minimum of a current SECRET clearance.
- **Citizenship**—citizenship of the applicant must be determined through an authoritative source, such as the I-9 or Security Clearance.
- **Account**—the applicant must possess an account on an accredited U.S. SECRET level information system or network.

## Impact to the Community

- **Secret Level Users**—As detailed, this capability will enable the rollout of hardware tokens for SIPRNet. However, subscribers will be required to maintain multiple tokens. At a minimum, subscribers with SIPRNet accounts will have both their CAC and their SIPRNet hardware token.
- **CN\SA Policy**—The CNSS PKI Working Group will now be responsible for the review and approval of the DOD's CA CPS. The Certificate Policy Management Working Group (CPMVG) will retain responsibilities for the review and

approval of DOD Services' and Agency's Registration Authority (RA) Practice Statements (RPS) detailing RA operational procedures should they choose not to accept the common language detailed within the NSS DOD Reference RPS.

- **Trusted Roles**—All personnel assigned to a trusted role under an RA (RA Officer, Information Assurance Officer (IAO), System Administrator (SA), Trusted Agent (TA)) are provided with training on the stipulations of [CNSSI 1300], any appropriate local guidance, and the PKI duties they are expected to perform. RA Ops personnel are also instructed on RA operational and security principles, mechanism, and procedures to include disaster recovery and business continuity, and any PKI specific details of the software/hardware that is used for RA operations.

## References

*CNSS Policy #25, authorizes the NSS PKI,*  
<http://www.cnss.gov/Assets/pdf/CNSSP-25.pdf>.

*CNSS Instruction #1300, is the NSS CP,*  
[http://www.cnss.gov/Assets/pdf/CNSSI\\_1300.pdf](http://www.cnss.gov/Assets/pdf/CNSSI_1300.pdf)

## The Combined Endeavor Experience



Combined Endeavor is a U.S. European Command sponsored communications and information systems interoperability testing exercise between NATO and Partnership for Peace (PfP) Nations. It is the largest international Command, Control,

Communications & Computers (C4) exercise in the world. This year more than 1000 military and civilian personnel from 40 nations took part in the 2 week exercise (September 4 – 17, 2009) in one of three locations: Bosnia and Herzegovina, the Netherlands and Denmark. Among those participants were members of the DOD PKE Team, the PKI PMO, and the AF PKI SPO.

Combined Endeavor is a communications and information systems interoperability testing exercise. The results of these tests are compiled and added to the integrated interoperability guide that has been maintained since the establishment of Combined Endeavor 14 years ago. The testing done at Combined Endeavor simulates the conditions of a multinational C4 deployment and helps to eliminate "discovery learning" upon actual deployment for military and humanitarian operations. But the purpose of Combined Endeavor is

more than just successfully establishing technical interoperability between NATO and PfP communications systems; human interoperability is an equal goal as well. To establish the technical goals of CE, there must be strong human interaction. Without this collaboration, the technical goals could not be achieved.

Participants of the DOD PKE Team, the PKI PMO, and the AF PKI SPO deployed 2 separate PKIs (one PKI for the test network and another PKI for the core network) to support the technical interoperability testing. The teams provided technical guidance and training throughout the exercise to the participants.

The successes of Combined Endeavor are measured in both technical and human terms. While there were many technical PKI challenges faced and overcome throughout the exercise, a valuable achievement would be the collaborative environment that developed between the NATO and PfP nations. The PKI team worked with the NATO and PfP nations to stand up an operational PKI, worked with the nations to solve PKI problems and the nations that participated were able to learn and practice setup and maintenance on their unique national computer systems. This experience solving PKI related problems between nations would be invaluable in a multinational deployment.



# Coalition PKI

by Jackie Huff

Coalition PKI (CPKI) is a DOD operational capability that allows secure information sharing with Coalition partners that do not reside on the GIG. CPKI provides the same cryptographic capabilities as the DOD PKI; enhancing security by supporting digitally signed/encrypted email and secure authentication to DOD Coalition specific applications and resources. Coalition environments produce unique challenges for interoperability with the DOD, e.g. distant partners not collocated with DOD resources, identification of partners, and appropriate information sharing. The CPKI is intended to secure established business processes between the DOD and Coalition partner communities using Coalition partner networks and equipment, e.g. exchanging sensitive information via encrypted email versus resource intensive secure courier or without protection. The CPKI is a lower assurance PKI than the DOD PKI and is not intended to be trusted and deployed Department wide, but rather on an as needed basis. CPKI is currently not intended to allow Coalition partners into existing DOD restricted applications until the enterprise has deployed an access control solution that will ensure information is only shared with the intended individuals or communities of interest.

A few ways CPKI capabilities are different than the DOD—

**Remote Issuance Capability**—Standard assurance certificate tokens allow issuance of credentials to users that may not have the ability to conduct face to face vetting with a US DOD CPKI Registration

Authority. These allow the DOD to provide tokens to known organizations through an established chain of trust comprised of DOD and Coalition trusted personnel.

**Role Based Hardware Token Certificates**—In addition to Medium Assurance Individual PKI certificates (e.g. certificate represents John Doe) the Coalition PKI support Role based Hardware Certificate Token Certificates. Role based certificates increase the usability and life of the tokens themselves as they support a role within a Coalition organization rather than an individual user. Multiple certificate assurance levels allows the DOD to credential based on partner DOD and partner requirements while allowing a mechanism to make access control decisions based on type of credential. A Coalition partner may have access to more information when presenting a Medium Assurance rather than a Role Based token.

**Remote Renewal of End User Certificate**—CPKI Standard Assurance certificates may use the same key pair for up to six years with renewal at 2 year intervals. This capability increases the lifetime of a user token. For intermediate certificates, the individual will require additional vetting every two years as part of their renewal.

More information is available at [https://www.intelink.gov/wiki/Coalition\\_PKI](https://www.intelink.gov/wiki/Coalition_PKI).



## Research in Motion

The DOD PKE Engineering Team recently requested information concerning issues, concerns, enhancements, and suggestions for BlackBerry Enterprise Servers and/or BlackBerry devices in the DOD. We would like to thank everyone who provided us with information. We have sat down with Research In Motion and voiced your issues, concerns, enhancements, and suggestions. Research In Motion are going to try and improve their products in future releases based on the information you provided. If you have more issues, concerns, enhancements, and suggestions for BlackBerry Enterprise Servers and/or BlackBerry devices please send them to our email Address at [pke\\_support@disa.mil](mailto:pke_support@disa.mil).

## Use of Approved the DOD External Certification Authority (ECA) Program

by Sharron Keggler

The External Certification Authority (ECA) program was established in 2004 to support the issuance of DOD-approved certificates to industry partners and other external entities and organizations.

All ECA certificates are DOD approved to authenticate to DOD web servers and other systems, and to support digital signature and encryption of email. The ECA PKI consists of a Root CA operated by the DOD and three vendors who issued Subordinate CA certificates by the Root CA. The three approved ECA Vendors are—

- Operational Research Consultants, Inc. (ORC)
- VeriSign, Inc.
- IdenTrust, Inc.

ECA vendors issue multiple types of certificates to support the needs of DOD external partners inside and outside the U.S. ECA vendors are able to issue both identity and encryption software or hardware

certificates. ECA identity certificates are used for both authentication and digital signature. In addition, ECA offers SSL web server certificates and code signing certificates.

ECA defines three levels of assurance, medium, medium token, and medium hardware. Medium assurance certificates are comparable to DOD medium assurance (DOD software). Medium hardware assurance is comparable to DOD medium hardware assurance (DOD Common Access Card). Medium token assurance is a hybrid assurance level that combines hardware certificates (smart card or USB token) with identity proofing using a notary or other authorized official.

ECA vendors are authorized to provide hardware credentials to DOD partners requiring access to DOD applications. Both medium token and medium hardware certificates are cross certified with the Federal Bridge at medium hardware, and are fully comparable with the DOD Partner interoperability effort.



## About DOD PKE



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

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

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

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

Visit us on DKO—  
<http://iase.disa.mil/pki/pke>

Send your questions and feedback to—  
[PKE\\_Support@disa.mil](mailto:PKE_Support@disa.mil)

## Upcoming Events

### 2010 Identity Protection and Management Conference

April 12 – 15, 2010

Minneapolis, MN

[www.iad.gov/events](http://www.iad.gov/events)

### DISA Customer Partnership Conference 2010

May 3 – 7, 2010

Nashville, TN

<http://www.disa.mil/conferences/2010>

## ECA Program – *continued*

The DOD PKE InstallRoot utility contains the ECA Root and all current ECA vendor CA certificates and can be used to add these certificates as trusted CAs. ECA Certificate Revocation Lists (CRL) can be accessed from the DOD Global Directory Service (GDS) at <https://crl.gds.disa.mil/>. Alternatively, all ECA vendors provide an Online Certificate Status Authority (OCSP) capability. When trusting ECA certificates, it is important to map ECA certificates to access privileges.

For more information on the ECA program visit <http://iase.disa.mil/pki/eca>

## IPM Conference 2010: Extending the Bridge to Our External Partners

On April 12 – 15, 2010, the DOD Public Key Infrastructure Program Management Office (DOD PKI PMO), the Defense Manpower Data Center (DMDC), and the Biometrics Task Force (BTF) will host the 6th Annual Identity Protection and Management (IPM) Conference at the Minneapolis Hilton in Minneapolis, MN.

The goal of the IPMC is to serve as a platform for sharing identity and privilege management experiences, challenges, and lessons learned within the DOD and with DOD's partners in the Federal, Commercial, and Global communities. An exciting topic that will be introduced throughout the tracks this year will be Authorization Services: "How to Provide Dynamic Access Control in an Operational Environment."

## DOD and Microsoft PKI TIM Slides Available

The annual PKI Technical Interchange Meeting (TIM) between DOD and Microsoft was held at the Microsoft Campus in Redmond, Washington January 12 – 13. In attendance were PKI representatives from across the Services and Agencies. All participants collaborated with Microsoft on authentication and identification policy and practices; the future direction of the DOD Identity Management programs and projects, and Microsoft's roadmap for operating systems, applications, technical support, and data and communications security. Progress and future plans were made in the areas of technical support,

## Did You Know...

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

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

(Note—CAC/PKI certificates are required to access this Web site).

The agenda will consist of four tracks that span across all areas of identity and privilege management. These tracks include—

- Evolution & Emerging Technologies
- Extending the Bridge to our External Partners
- Implementation, Enablement and Usage
- Working through the Issues

# Microsoft®

code development roadmaps, and organizational strategies. Slides from the TIM are now posted to the PKE site <http://iase.disa.mil/pki/pke>.

To submit comments or suggestions for improvement for the next Microsoft TIM, send an email to [pke\\_support@disa.mil](mailto:pke_support@disa.mil) with the subject line, "January PKE TIM with Microsoft."

