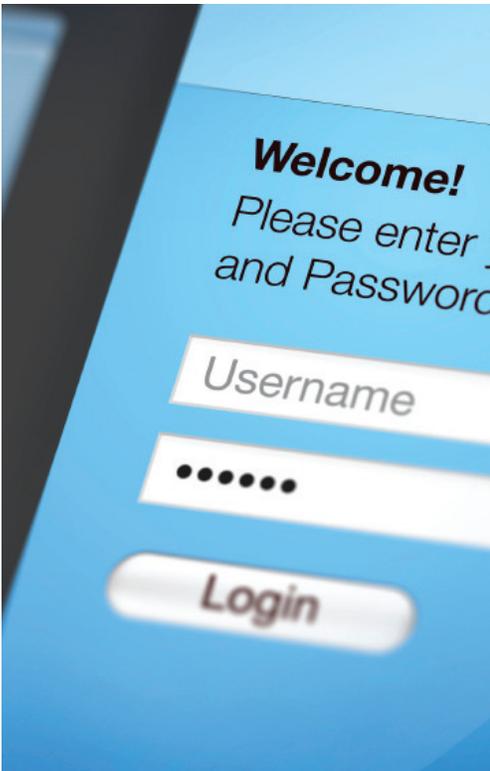


The PKE Quarterly Post

Authentication is having an Identity Crisis

By Kristopher Tracy



No matter what kind of technological or procedural advancements occur, certain principles of computer security will remain important—especially those concerning information security. When working with information security, the basic understanding of these fundamentals is often brushed aside. In this article, we will explore the concepts of identity, authentication, and authorization to help you understand their important distinctions, and to help guard you against the misunderstanding and tendency to assume PKI provides the former two concepts. Let's establish an understanding of these principles and then see where PKI will fit in.

Identity. Because the system doesn't know you yet, you need to make a declaration of who you are. Your answer to the question, "Who are you?" is the first thing you present to a system when you want to use it. Some common examples of identity are user IDs, digital certificates (which include public keys), and ATM cards. A notable characteristic of identity is that it is public, and it has to be this way. Identity is your claim about yourself, and you make that claim using something that's publicly available.

Authentication. This answers the question, "OK, how can you prove it?" When you present your identity to a system, the system wants you to prove that it is indeed you and not someone else.

The system will challenge you, and you must respond in some way. Common authenticators include passwords, private keys, and personal identification numbers (PINs). Whereas identity is public, authentication is private; it's a secret known (presumably) only by you. In some cases, like passwords, the system also knows the secret. In other cases, like PKI, the system doesn't need to possess the secret, but nonetheless can validate its authenticity (this is one of many reasons why PKI is superior). Your possession of this secret is what proves that you are who you claim to be.

In This Issue

PKE Support for External PKIs.....	3
Smartphones Need Smart Security	4
Coalition PKI	5
Mobile Code Signing Certificates? Who Needs 'Em?.....	5
When a Good Card Goes Bad	5
ActivClient and Remote Desktop Protocol (RDP).....	5

In Every Issue

Ask the Expert.....	2
Notes from DOD PKE.....	2
In the Pipeline	3

continued on page 3



Ask the Expert

Question How can I contact my Local Help Desk?

Answer Here is a list of the CC/S/A Helpdesks

Help Desks		
Name	Organization	Contact Information
DOD PKI Help Desk	DISA	disa-esmost@okc.disa.mil 1-800-490-1643 DSN 339-5600
Air Force CAC/PKI Help Desk	PKI SPO	https://afpki.lackland.af.mil AFPki.Helpdesk@LACKLAND.AF.MIL 210-925-2521
Army CAC/PKI Help Desk	NETCOM OM-IA CAC/ PKI	OM-IA CAC PKI Help Desk iacacpki.helpdesk@us.army.mil 703-602-7514 1-866-738-3222 DSN 332-7514
Navy CAC/PKI Help Desk	NMCI	http://www.nmci-isf.com/faq.htm 1-866-843-6624
SPAWAR Integrated Support Center Help Desk	SPAWAR	https://infosec.navy.mil/PKI itac@infosec.navy.mil 1-800-304-4636 DSN 588-4286
USMC RA Operations Help Desk	USMC	raoperations@mcnosc.usmc.mil 703-432-0394
WHS Help Desk	WHS	https://pkisupport.whs.mil IPMSupport@whs.mil
AKO Help Desk	Army	1-866-335-2769 (ARMY)
GDS	DISA	gds@disa.mil
JITC (Test Certificates)		pki@fhu.disa.mil pke@fhu.disa.mil

Question Who should I contact to obtain PKI certificates and certificate approvals?

Answer Here is a list of CC/S/A RA Operations Offices.

RA Operations			
Name	Organization	Contact Information	COCOMS Supported
Army	Army CTNOSC Army NETCOM	ctnos.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/iracontacts.asp	USCENTCOM USSOCOM USTRANSCOM USNORTHCOM USSTRATCOM
Navy	Navy PKI Help Desk	https://infosec.navy.mil/PKI/lramain.html	USJFCOM USPACOM
Marine Corp	USMC PKI RA Operations	raoperations@mcnosc.usmc.mil	
DISA	DISA RA Operations	disaraoperations@disa.mil	
Joint Staff	Joint Staff RA Support	isra@is.pentagon.mil	

This list will be posted on the PKI/PKE web site: <http://iase.disa.mil/pki/pke>

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

Notes from the DOD PKE

by Carmella Webster, PKE Team Lead

With the conference season now behind us, it has remained a busy time for the DOD PKE Team. Allison and I wanted to especially thank all of the CC/SAs for your valuable contributions to the very well-received and well-attended Identity & Protection Management Conference, PK-Enabling Sub-Track and Technical Interchange Meeting (TIM). Without you, success would not have been possible!

In other, non-conference news, the DOD PKE Team serves as the Co-Chair (with GSA) of the Federal Identity, Credential, and Access Management (FICAM) Logical Access Working Group (LAWG) in support of continued expansion of DOD's trust of approved external PKIs. We are developing the Roadmap and Implementation Guidance in support of FICAM Initiative 8: Modernized Logical Access Control System (LACS) Infrastructure. The Working Group was formed to develop guidance for leveraging the PIV Authentication PKI certificate for identity and authentication services.

Our team remains heavily engaged with the on-going efforts to accept DOD Approved External Partner PKIs. Some of the early adopters we are supporting include:

- **DKO**—Provide engineering support to enable authentication to DKO using DOD approved external partner PKIs.
- **DoS**—Enable DoS systems to allow DOD employees to access DOD resources while operating in a DoS environment.
- **North Chicago VA PIV acceptance**—Coordination between the Navy and VA to enable the use of each other's credentials in each other's environment.

The DOD PKE team, along with the DOD PKI PMO, worked directly with ASD NII and DMDC to develop a formal response of non-concurrence with the proposed timeline in the NIST SP 800-131, "DRAFT Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes." The DOD CIO delivered this memorandum to the Secretary of Commerce earlier this year.

PKE is also heavily engaged with efforts supporting the migration to stronger cryptographic algorithms. Along with the response to NIST regarding SHA256 the DOD PKI PMO is leading a team to conduct internal testing of the DOD PKI PMO assets to gain better insight into the feasibility of full SHA256 deployment throughout the DOD PKI systems. The PKE team is assisting with this effort in addition to supporting the DMDC lead Cryptographic Migration Testing (CMT) effort to determine if products used by the DOD PKI community will interoperate with SHA256.



Authentication – continued

Authorization. Once you've successfully authenticated yourself to a system, the system controls which resources you're allowed to access. Typically this is through the use of a token or ticket mechanism. The token or ticket constrains your ability to roam freely throughout the system. By "caching" your authenticated identity for subsequent access control decisions, it allows you to access only that which the administrators have determined is necessary, thus enforcing the principle of least privilege.

Now let's examine PKI. Given the definitions and characteristics authentication and authorization, which does PKI provide: authentication or authentication?

Before we answer the question, we will examine the attributes of PKI. PKI provides certificates for a user to utilize to establish identity. When the certificates are issued by the certificate authority (CA), identity is established. Authentication is established through typing in a PIN, revocation checking, etc. but authorization? Problems arise when systems begin using PKI for authorization. Let's consider an example of a computer system which requires a Common Access Card (CAC) and successful validation of a PIN in order to use the system. Because getting a CAC is such a rigorous process, you might think that because an individual carries the CAC, this would be a sufficient method of security, right? Wrong. Because authorization didn't take place, anyone with a CAC will be allowed entry, regardless of whether they should be there or not. Perhaps an individual showed up at the wrong website, used their CAC for entry, and decided to browse through classified documents because the

rationale might be, "Hey, I'm allowed to be here, my CAC allowed me in." It's important then for us to keep in mind that just because a user has authenticated with a certificate does NOT necessarily mean they are authorized to access the data.

Authorization must be distinguished from authentication and used responsibly. Applying access controls are an essential component of establishing trust. If we focus on authentication and ignore authorization, an illusion is created to misrepresent the level of trust.

Traditionally, many people see PKI as encompassing utilization of the CAC only. However, software-based certificates provide another means of utilizing PKI. PK-enablement also encompasses working with these software-based certificates. Within the DOD, external Certificate Authorities (ECA) now also exist. ECAs include DOD-approved external partner PKIs. Therefore, when discussing PK-enablement, these software-based certificates must also provide authentication.

It is crucial to understand this difference between authentication and authorization regardless of the means used to access the PKI. These fundamentals will never lose importance, and this understanding can help you more successfully choose products and develop processes revolving around information security.

PKE Support for External PKIs

by Dan Jeffers

The DOD PKE team has been supporting DOD organizations as they transition systems to accept DOD-approved external PKI certificates for authentication. Some efforts worth mentioning include the Navy and Veteran Affairs (VA) consolidation, which will allow VA personnel to authenticate with VA certificates to certain Navy websites and networks and vice versa. DOD PKE is also supporting DKO/AKO as they plan to accept DOD-approved external PKI certificates in the future.

The DOD PKE team is currently updating our documentation to include guidance for external PKIs. We are developing general guidance such as Frequently Asked Questions (FAQ) documents and updating existing PKE reference guides to include configuration information for DOD-approved external PKIs. Additionally, DOD PKE is compiling information for a partner certificate map, which will detail certificate policy OID and other partner certificate information that should be useful to DOD system administrators.

The DOD PKE team is also working with the DOD External Interoperability Working Group (EIWG) and Joint Information Testing Command (JITC) to facilitate the testing and approval of additional external PKIs to be approved for use within DOD. The next PKI to go through the approval process will be General Services Administration (GSA).

The DOD PKE interoperability application testing is now complete and the final report currently being finalized. The report details the DOD PKI interoperability application testing methodology and how applications actually behave in cross-certificate or direct trust environments. DOD PKE is also recommending some changes to existing cross-certificates to support validation of other agency Personal Identity Verification (PIV) certificates against the DOD Interoperability Root CA 1.

In the Pipeline



Alternative Revocation Checking Solutions

By Ross Schwalm

The DOD PKI PMO recognizes the size of DOD Certificate Revocation Lists (CRLs) is becoming an important issue as more DOD-approved PKIs come online. System administrators now have an alternative option for keeping their local certificate revocation checking solutions up to date. For example, if an organization has a local Online Certificate Status Protocol (OCSP) responder, its local cache can now be maintained (with significantly less bandwidth requirements) by using proprietary CRL reducing technologies available from two newly available Robust Certificate Validation Service (RCVS) load-balanced URLs. Using these solutions requires a proprietary client to recognize the CRLs, but reduces the DOD CRLs from ~175MB to ~4MB:

CompactCRL—A proprietary solution from Axway (who purchased Tumbleweed) that requires an Axway validation infrastructure. RCVS hosts CompactCRLs at sa.disa.mil:6132.

MiniCRL—A proprietary solution from Corestreet that requires a Corestreet validation infrastructure. RCVS hosts MiniCRLs at sa.disa.mil/proofs.

New OCSP URLs

By Curt Spann

As the DOD PKI PMO transitions the Robust Certificate Validation Service (RCVS) to the Delegated Trust Model (DTM) configuration, the existing RCVS URL (ocsp.disa.mil) may contain both the older configured self-signed OCSP responders along with the newly deployed DTM configured OCSP responders. Some systems and applications may encounter issues

continued on page 4



when attempting to operate in the mix-mode. If the system or application is configured for self-signed and hits a DTM configured responder, it may be unable to validate the response. If the system or application is configured for DTM and hits a self-signed configured RCVS node, it also may be unable to validate the response. Since the existing RCVS URL is a DNS round-robin of multiple OCSP nodes in different configurations, the application or system may periodically be unable to validate a presented certificate depending on the configuration and OCSP responder hit based on the DNS round-robin. DOD PKI PMO has supplied two new URLs for clients to be configured either for self-signed or DTM. The self-signed URL is <http://ocsp-legacy.disa.mil>, and the DTM URL is <http://ocsp-dtm.csd.disa.mil>.

Latest Updates from DOD PKE

Latest Document Releases

The following documents have been added or updated to the DOD PKE Knowledgebase—

- Obtaining a DOD Code Signing Certificate
- Obtaining a PKI Cert for a DOD Server
- InstallRoot Users Guide
- Key Store tools and procedures
- Configuring Firefox to utilize the DOD CAC
- Deploying DOD PKI CA Certificates using Group Policy Objects (GPO)
- Tumbleweed Desktop Validation

Smartphones Need Smart Security

By John Hamilton



Wireless mobility has arrived, if you like it or not, and it is changing the way DOD employees and contractors conduct business. Smartphones are being used not only for voice calls, calendaring, and text messaging, but also for tasks normally done on a computer such as web browsing, e-mailing, storing and modifying documents, delivering presentations, and remotely accessing data. However, as the use and functionality of smartphones continues to grow, so do the security risks. As a result, it has become increasingly more important for DOD organizations to mitigate the risks posed by smartphones and to educate users about these risks.

The Risks

Smartphones introduce a range of potential security risks to DOD organizations, but malware, insiders, and lost or stolen smartphones pose the most significant threats.

Malware—Compromising legitimate websites, text messages, Bluetooth transmissions, and e-mail attachments for the purpose of propagating malware on smartphones have become popular and highly effective techniques for attackers. Once a smartphone has been infected, malicious code can interfere with the devices' contents, capture sensitive data, pinpoint a user's whereabouts by querying the device's Global Positioning System (GPS) receiver, or allow an attacker to eavesdrop by turning on the device's microphone. To make matters worse, current malware code often avoids behavioral and signature-based detection, and can disable anti-virus software on a device.

Insiders—Insiders pose a very serious threat because they know how to exploit an organization's weaknesses, security policies, and technologies to

steal data, intellectual property, money, or simply disrupt operations. Insiders not only could be current or former employees, but contractors or other third parties.

Lost or Stolen Smartphones—If a smartphone is lost or stolen, confidential data such as meeting notes, e-mails, customer contacts, and business proposals could be viewed by or sent to a wide variety of unintended recipients such as a competitor, journalist, or identity thief. The loss of control over confidential data could be a serious threat to business operations and, potentially, national security.

Protecting Mobile Devices

Public key technology provides a means to strongly authenticate over networks, ensure the integrity of transmitted data, guarantee confidentiality of information through strong encryption, and achieve non-repudiation for transactions. To protect against the risks posed by smartphones, the DOD primarily uses two Public Key Enabled (PKE) solutions. Currently, the DOD uses Research in Motion's (RIM's) BlackBerry Enterprise Solution more than any other mobile messaging solution to secure BlackBerry devices that connect to their network infrastructure. A BlackBerry device's hardware and software is centrally managed through the BlackBerry Enterprise Server (BES). The BES enforces a personal firewall and FIPS 140-validated data-at-rest encryption. RIM also has its own S/MIME package and an approved Bluetooth smart card reader (SCR).

To secure Windows Mobile smartphones, the DOD uses Good Technology's Good for Government Solution. This approach provides similar personal firewall, device configuration management, and FIPS-140 validated data-at-rest encryption capabilities. However, unlike the BlackBerry, an approved anti-virus application must be installed on the device. In addition, Good provides its own S/MIME package that interoperates with the Biometrics Associates' (BAI) baimobile Bluetooth SCR and Apriva's BT100-C and BT200 Bluetooth SCRs.

Next Steps

It's vital for DOD organizations to defend themselves at all levels of their business. Smartphones must be comprehensively secured by utilizing public key technology to combat against the myriad of threats posed by the criminal underground, lost or stolen devices, and by insiders within the organization. Along with these efforts, it is critical that DOD organizations educate their employees about security awareness in order to safeguard their own online identity and understanding of the risks that go along with their use of technology.



Mobile Code Signing Certificates? Who Needs 'Em?

By Ellen Collins

If you have found yourself having the thought expressed here, we have an answer for you. Information contained in the recently published Reference Guide (RG) "Obtaining a DOD Mobile Code Signing Certificate" should clarify both the processes and reasoning behind this requirement.

Just what is mobile code? DOD Instruction 8552.01 defines mobile code as "software obtained from remote systems outside the enclave boundary, transferred across a network, and then downloaded and executed on a system without explicit installation or execution by the recipient." Depending on the mobile technology used, this code could be considered high risk and may pose a threat to DOD operations. DOD units have been directed to protect systems from the threat of malicious or improper use of ActiveX, Java, and VBA code. In addition, while not a requirement, it is recommended that locally-created software (i.e., installation files) to be used on a DOD network also be signed with a mobile code signing certificate.

Specific processes for obtaining these certificates can be obtained from your supporting Registration Authority (RA) office. Basically, Each Combatant Command/Service/Agency (CC/S/A) currently has or will have a Code Signing Attribute Authority (CSAA) who is the approval authority for organizations to perform code signing functions. The CSAA must approve issuance of any code-signing certificate prior to the RA office processing the request. It is expected that each CC/S/A will have a limited number of authorized code signers.

More detailed information on Mobile Code Categories and Requirements for a Mobile Code Signing Certificate are contained in the RG noted above. This document can be downloaded from the Certificates folder of the Knowledge Base Library on DKO at <https://www.us.army.mil/suite/page/474113>.

When a Good Card Goes Bad

By Nicole Baker

DOD PKE has received sporadic reports from the field concerning Common Access Cards (CACs) that would function normally for several weeks or months and then would no longer be recognized by a user's workstation. The common error message being displayed upon inserting a CAC into the card reader is: "The card supplied was not recognized. Please check that the card is inserted correctly, and fits tightly." This issue was originally reported in Spring 2008.

Analysis of this issue was conducted in Winter 2008/2009 by the Defense Manpower Data Center's (DMDC's) Independent, Verification, and Validation (IV&V) contractor. The analysis showed that some CAC (Personal Identity Verification) PIVs (OCS ID One and Gemalto GCX4) begin to fail in the field over a period of time. The result is that readers are unable to

recognize the card and it appears "damaged" or "mute," when in fact the cards are still functional. Some card readers are able to overcome this abnormal behavior; some cannot. In addition to the analysis of failed returned cards, DMDC conducted tests of different smart card readers, both standalone and integrated PC products. DMDC's tests concluded that readers were operating within the normal parameters and are not the cause of the failures. The analysis identified shorts within the chips of several of the failed returned cards that appear to be the cause of the sporadic failures. This does not appear to be isolated to a single card vendor. The only resolution is to get the CAC re-issued. Issuance facilities that indicate CACs have been re-issued for this reason may be sent to DMDC for additional testing.

ActivClient and Remote Desktop Protocol (RDP)

By Kebba Sallah

The PKE team recently found an issue with the latest version of ActivClient within Remote Desktop sessions. It was noted that ActivClient 6.2 was not recognizing the 128K Oberthur Common Access Cards (CACs) only when logged into a remote machine through Windows Remote Desktop connection. The middleware detected that a card was inserted but did not display certificate information in the ActivClient Agent console nor were certificates populated in the Personal Certificates store of Microsoft CAPI. This issue only arose with the fairly new Oberthur ID One 128k v5.5 Dual PIV Endpoint

CAC; every other CAC worked fine in a Remote Desktop Protocol (RDP) session. This bug affects all CAC functions such as Smart Card Logon and Client Authentication.

Fortunately, it was discovered that the latest ActivClient Hotfix (v78) solves this problem. Applying the Hotfix provides normal function for the middleware in a RDP connection. The actual cause of the problem was not exactly pinpointed but was assumed to be related to a failure in the middleware calls made to the local machine smart card reader.

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

