

The PKE Quarterly Post

DoD's Migration to SHA-256

By Julia Ott



Background

In March of 2007, the National Institute of Standards and Technology (NIST) published Special Publication (SP) 800-57, *Recommendation for Key Management: Part 1 - General*, which defined cryptographic algorithm strengths and timelines for use within the federal government. One of the milestones in NIST SP 800-57 was that the Secure Hash Algorithm (SHA)-1 should not be used for digital signatures beyond 2010 because it has only 80 bits of security. By comparison, the SHA-256 algorithm is considered to have 128 bits of security for digital signature applications.

In January of 2010, NIST released draft SP 800-131 which provided further details on the migration timelines. In January of 2011, SP 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, was released in final form. Section 9 of SP 800-131A, entitled "Hash Functions," states that all federal agencies should have migrated to SHA-256 for digital signature generation by January 1, 2011. However, it also allows for continued use of SHA-1 through the end of 2013 with an acceptance of risk:

"From January 1, 2011 through December 31, 2013, the use of SHA-1 is deprecated for digital signature generation. The user must accept risk when SHA-1 is used, particularly when approaching the December 31, 2013 upper limit."

continued on page 3

In This Issue

Ensuring Security and Interoperability with DoD Partners: 2048-bit RSA Certificates.....	2
Security Awareness	4
Wireless Update	5
OCSP Trust Models	5

In Every Issue

Ask the Expert.....	2
Notes from DoD PKE.....	2
In the Pipeline	3
RA/LRA/KRA Corner.....	4
Latest Tool Releases	5
Latest Document Releases	5
About DoD PKE.....	6

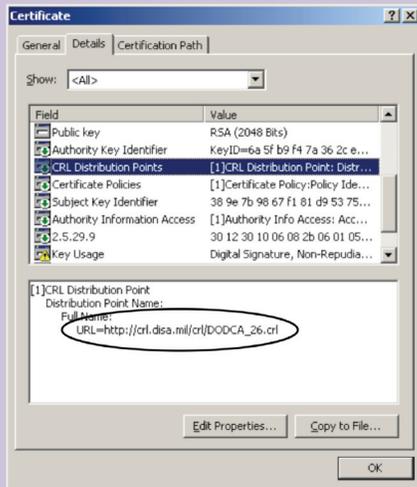


Ask the Expert

Where can I find revocation information for a certificate?

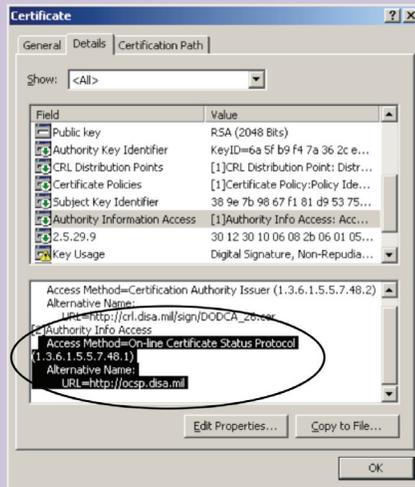
There are two methods commonly provided by PKIs for certificate revocation status checking: Certificate revocation lists (CRL) and online certificate status protocol (OCSP) responders. Most certificates (including those issued by DoD) contain pointers to this information within the certificates themselves.

CRL Distribution Point Extension (for CRL Location)



The CRL Distribution Point (CRLDP or CDP) extension contains a download URL for the CRL governing the certificate.

Authority Information Access Extension (for OCSP Responder Location)



The Authority Information Access (AIA) extension may contain a URL for an OCSP responder that responds on behalf of the certificate. Note that AIA extensions can contain two types of URLs; an OCSP responder URL will be denoted within the AIA information by a designation of Access Method=On-line Certificate Status Protocol.

How do I obtain a production SIPR token? How about a test SIPR token?

Users should contact their organization's RA team to find out the organization's plan for distributing production SIPRNET tokens. As for test tokens (that work with the JITC unclassified test environment), these are very scarce right now as we prepare for Interim Operational Test and Evaluation using production tokens. Requests for test tokens should be sent to the PKI PMO.

How should I protect my SIPR token when not in use?

There is a three-page memorandum that describes how to protect the token and how to handle various mishaps. In general, the token is to be protected as a high-value UNCLASSIFIED item when not in a card reader. Contact pke_support@disa.mil for more information on how to protect your SIPR token.

What happens if I insert my SIPR token into an unclassified computer?

Mistakes happen, but users should try to avoid this. In general, if the PIN is entered, it is a security violation and the token must be revoked. If the PIN is not entered, there is no security violation.

Notes from DoD PKE

By Allison Scogin

It seems all of our Notes from DoD PKE can be started the same way: "It is a busy time to be in PKE." We just returned from the Information Assurance Symposium (IAS) in Nashville, Tennessee, where we met a lot of new faces that we look forward to working with in the future!

Some of the big questions we received at the IAS were about the new SIPR hardware token and the SHA-256 migration. This newsletter addresses some of those questions. In addition, the team will produce new slick sheets to address the questions in greater detail. The slick sheets will be available the week of April 18th from our website and from the DoD PKI Booth at the 2011 Identity Protection and Management Conference in Orlando, Florida.

On the topic of the website, we have officially moved away from our AKO website and are now full time on the Information Assurance Support Environment (IASE) website. We are continuing to transition content from AKO to our new home on the IASE. If there is software or a reference guide that you cannot find on IASE, please make sure to let us know by emailing pke_support@disa.mil.

In closing, the team has several exciting projects on the horizon. We will be supporting the DoD PKI PMO in the rollout and use of the SIPR hardware token and the NSS PKI. In the near future you should expect to see a revised PKE website on SIPR IASE. The team is standing by to answer your questions about the upcoming SIPR DTM RCVS migration and is continuing to support the DoD CIO as the technical point of contact for the SHA-256 migration.

Ensuring Security and Interoperability with DoD Partners: 2048-bit RSA Certificates

By Allison Scogin

Many DoD partners do business with DoD web applications via HTTPS. In many cases these non-DoD partners have not installed DoD's Certificate Authorities into their certificate trust stores and are operating client browsers with default settings. After the re-issuance of the cross certificate from the Federal Bridge Certificate Authority to the DoD Interoperability Root CA (IRCA) 1 in December 2010, these partners reported that they were presented with a certificate warning page which was followed by a more generic connection error from their web browser which could not be bypassed.

continued on page 3



Ensuring Security – *continued*

This occurred because the certificate policy OID corresponding to the DoD RSA 1024 bit certificate was no longer mapped in the cross certificate issued from the FBCA to the DoD IRCA 1. This was a purposeful design choice made in service of the FBCA Certificate Policy which acquires its cryptographic requirements from several NIST Special Publications: SP 800-57, SP 800-78 and SP 800-131. The

DoD Certificate Policy also mandates that all RSA keys issued after 31 December 2010 shall be 2048 bits.

DoD Registration Authorities (RA) should no longer approve RSA 1024-bit keys. Furthermore, RSA 1024-bit certificates on servers should be replaced as soon as practicable with RSA 2048-bit certificates. Priority should be given to those servers that are used to do business with non-DoD partners who do not explicitly trust the DoD PKI.

Migration to SHA-256 – *continued*

Current State

The DoD is still using SHA-1 under the acceptance-of-risk condition allowed by NIST SP 800-131A; however, the use of SHA-1 after 2013 is completely disallowed. To support the requirement to transition to SHA-256 by 2014, in the fall of 2010 the DoD CIO's office directed that each DoD component conduct an assessment of their deployed systems to establish the level of impact that the SHA-256 migration would have on the Department. In collaboration with the DoD services and agencies, the DoD CIO's office is developing a plan for migrating to the use of SHA-256 in DoD systems performing digital signature operations. The resulting SHA-256 Migration Roadmap will identify migration milestones that all Combatant Commands, Services and Agencies (CC/S/A) will need to meet in order for the DoD to collectively complete migration by the December 31, 2013 deadline. At the time of writing, the first version of the roadmap is anticipated to be released in early April, with Plans of Action & Milestones (POAM) for complying with the roadmap's milestones due from each CC/S/A to the DoD Deputy CIO near the end of April.

The DoD CIO's office is also working with the Office of the Under Secretary of Defense for Acquisition, Technology & Logistics (OUSD(AT&L)) and the General Services Administration (GSA) to ensure that major product vendors are aware of the migration requirements and to identify the vendors' support plans for their products.

Migration Challenges and Impacts

The primary challenge facing the SHA-256 migration is that many widely deployed products do not support use of the SHA-256 algorithm. In order to ensure continuity of operations, all systems that perform digital signature validation operations need to support the use of SHA-256 before the DoD PKI begins issuing SHA-256 signed objects including certificates, certificate

revocation lists (CRL), and online certificate status protocol (OCSP) responses. This includes any system that uses the certificates on the DoD Common Access Card (CAC), DoD software certificates, or DoD approval external PKI certificates. Any system which does not currently support SHA-256 must be patched, upgraded, or if no support is available within the current product line, migrated to a different platform which does provide support.

This pre-requisite has far-reaching implications for the DoD's resources, both human and financial. For example, Microsoft Windows XP Service Pack 3 provides only limited SHA-256 support, and earlier service packs provide none; Tumbleweed Desktop Validator did not introduce SHA-256 support until version 4.10. In both of these instances, wide-scale system upgrades will be necessary to ensure that the systems are fully capable of processing SHA-256 signed objects.

Until the DoD migrates its own PKI to start signing objects with SHA-256, the major operational impact that DoD users will see is in DoD systems with users from other federal agencies who have already begun issuing SHA-256 signed PIV certificates. In that scenario, if the DoD system does not support SHA-256, the external users may experience denial of service or other usage challenges. Once the DoD PKI begins issuing SHA-256 signed certificates, CRLs and OCSP responses, DoD users will experience those same challenges with any system that does not support the stronger algorithm.

For more information on the migration process as well as where and how SHA is used within systems, visit our site at <http://iase.disa.mil/pki-pke/sha256/index.html>. Interested parties may also contact the OSD POCs for SHA-256 migration information and guidance at sha256transition@osd.mil.

In the Pipeline



New Intermediate CAs Planned for Summer 2011

New intermediate Certification Authorities (CAs) are planned to be set up this summer. When this happens we will publish a new version of InstallRoot so you will have plenty of time to install these new certificates before CAC issuance begins. Stay tuned for more information in our next newsletter.

SIPRNET RCVS DTM Migration

The DoD PKI PMO will transition the SIPRNET Robust Certificate Validation Service (RCVS) nodes to the Delegated Trust Model (DTM) beginning in summer 2011. The PKI PMO is currently finalizing a transition schedule. Community notification will use the DoD PKI Technical Lead Mailing List and a United States Cyber Command DoD GIG Operation Tasking Message (DGTm). The DoD PKI PMO will allow ample time for relying parties to migrate their information systems to support DTM. The DoD PKI PMO encourages SIPRNET information system owners to immediately begin an evaluation of their systems' ability to support DTM. Please direct any questions or concerns about the SIPRNET DTM RCVS migration to pke_support@disa.mil.





RA/LRA/KRA Corner

New Combined RA/LRA/KRA Training for NIPRNET and SIPRNET

By Chris Clements, RA/LRA/KRA Trainer

The DoD PKI PMO has recently expanded the DoD PKI RA/LRA/KRA Training to include National Security Systems (NSS) PKI Training. Training is still held at the training facility in Virginia and continues to cover a different role each day including Local Registration Authority (LRA), Registration Authority (RA), and Key Recovery Agent (KRA). These roles are now trained from both an NSS PKI perspective and a DoD PKI perspective.

Students nominated for DoD PKI production certificates can still obtain their credentials in the classroom. Students nominated as NSS RAs have two options for obtaining production certificates at the conclusion of training:

- **Option 1:** Students who have an existing NSS RA at their local office can work with their local command to obtain production certificates. For these students class is complete on the Thursday of the training week.
- **Option 2:** Students who do not have an existing NSS RA at their local office can obtain production certificates as the final part of the training class. For these students the following must occur:
 - On the Friday of the training week, the students will meet with a DISA NSS RA at a DISA site within the National Capital Region (NCR). Information on the specific location will be provided once students have registered for the class.
 - The DISA NSS RA will register the students for production certificates and assist with enrollment.

Students who wish to take advantage of Option 2 will need to coordinate additional logistics and are encouraged to register for the class in advance. The current training schedule can be found on the PKE site home page at <http://iase.disa.mil/pki-pke>.

Students who are new to PKI are encouraged to complete the PKI Overview computer based training found at <http://iase.disa.mil/eta/pki-training.html>. Additionally, the classroom presentation can be found at https://powhatan.iiee.disa.mil/pki-pke/landing_pages/rfts.html.

DoD PKI Key Recovery Update

By Rich Klein, RA Advocate

There are two methods by which users can recover historical encryption certificates: Using the Automated Key Recovery Agent (ARA) online, or requesting that the certificate(s) be manually recovered by a Key Recovery Agent (KRA). After the p12 file has either been downloaded from the ARA or sent to the user by the KRA, the certificate must be loaded into the Microsoft Cryptography API (CAPI) certificate store. However, password length and complexity requirements for the wizard used to load the certificates differ by organization and operating system (Windows XP, Windows Vista and Windows 7). Each Service and Agency defines password length and complexity requirements using NIST SP 800-118, Guide to Enterprise Password Management. Prior to instructing the typical user on what password to use, KRAs should verify the password length and complexity requirements with the user's System Administrator.

continued on page 6

Security Awareness

By Sam Fuson

From time to time, personnel within the U.S. Government are targeted by various adversaries using telephonic and electronic mail (email) phishing and social engineering techniques. It is important that you note the DoD PKE Engineering Support team stringently follows information assurance processes to ensure your safety.

- All email originating from the support team (PKE_Support@DISA.mil) will be digitally signed. This especially includes messages that contain attachments or links. Please ensure you verify the certification path chains up to the DoD PKI Root Certification Authority (CA) for all electronic transactions.
- We will not ask you for any sensitive personal information (e.g. SSN, CAC PIN, credit card number) and adhere to U.S. Office of Management and Budget (OMB) guidance for handling of any Personally Identifiable Information (PII) you provide.
- All DoD PKE tools will be digitally signed. Before proceeding with the installation of any PKE tools, verify that the installer package you are about to run has been digitally signed with the DoD PKE code signing certificate. The certification path should have DoD Root CA 2 as its trust anchor, and the DoD Root CA 2 thumbprint should be verified to match an authoritative source of the certificate.
- If you have any questions or concerns, please contact us directly at PKE_Support@DISA.mil.

As presented in annual security awareness training, your actions are essential to protect your own privacy and the resources of the U.S. Government. Please note:

- Do not click on any attachments or links in any suspicious emails or e-cards.
- Do not respond to unexpected invitations to connect on social networking sites such as LinkedIn, Facebook, or Twitter.
- Do not communicate with strangers, on the phone or via the computer.
- Forward any suspicious emails as an attachment to your local Security Office.
- After sending the suspect email as an attachment, delete it from your Outlook account.
- If you believe that your computer has already been infected, contact your local Security Office immediately.



Wireless Update

By Ross Schwalm



BlackBerry security vulnerability exposed at this year's CanSecWest Pwn2Own hacking contest

Hackers wirelessly exfiltrated data, specifically contact list information and image files, from a BlackBerry Torch 9800 using their newly uncovered web browser exploit and tricking a user into browsing to a website with the malicious code. The attack was performed at the 12th annual CanSecWest security conference in a hacking contest known as Pwn2Own. This contest started in 2007 and has become an annual event where contestants are given cash prizes for discovering new vulnerabilities.

Numerous web browser security vulnerabilities have been discovered and subsequently patched on the Android and iOS mobile platforms, but security vulnerabilities on BlackBerry devices are not something you read about every day. There was a new unrelated web browser exploit exposed for iOS 4.2.1 as well (allegedly it is still unpatched in iOS 4.3, the latest version), but that has not received nearly as much media coverage simply due to all the marketing surrounding the security of BlackBerry devices.

The vulnerability targets the BlackBerry implementation of the browser rendering engine, known as Webkit, which coincidentally is the same engine used for the Android browser, iOS browser (mobile Safari), and WebOS browser. To put it simply, Webkit understands web formatting information and displays it correctly on your screen. Webkit has only recently become the rendering engine for

the BlackBerry web browser, so only devices running BlackBerry Device Software version 6.0 or later are affected, which includes the Bold 9650, 9700 and 9780, Curve 9300, Pearl 9100, Style 9670, and Torch 9800 (the highly marketed device exploited in the hacking contest). The hacker community has a lot of experience attacking Webkit implementations on other platforms, which means more exploits probably will be discovered in the future, potentially with more malicious results. Until Research in Motion (RIM), the maker of BlackBerry devices, releases a patch, users can refer to documentation on RIM's website about how to disable JavaScript support and BlackBerry administrators can enable the "Disable JavaScript in Browser" IT policy to protect their entire enterprise. This will have a drastic impact on the browsing experience and many websites probably will no longer display correctly.

This serves as an important reminder of the importance of verifying the digital signature of any email that includes a link. DoD policy requires all emails that include links to be digitally signed for this specific reason. On BlackBerry devices you will see a green bar on the left side of the screen when viewing emails, if the digital signature of the sender is verified. If the bar is yellow or red, you should think twice about clicking on the link. In order for validation to work, you must have the latest DoD intermediate certificate authorities installed in your key store. NOTE: The BlackBerry Root CA Install package has been updated to include CAs 25 and 26 and is posted in the Resources section of the PKE IASE website.

OCSP Trust Models

By Julia Ott

The DoD uses the Online Certificate Status Protocol (OCSP) as a method for providing revocation status for certificates. OCSP, as defined by [RFC 2560], uses a request-response paradigm in which an OCSP client submits a certificate status request to an OCSP responder, and the responder, in turn, returns an OCSP response indicating whether the certificate status is good, revoked or unknown.

Prior to relying upon the status provided by the responder, the OCSP client must validate the OCSP response as described in [RFC 2560]. As part of the validation process, the OCSP client is required to determine that the signer of the response is authorized to have signed the response; in other words, that the responder is authorized to provide certificate status for the certificate in question. There are three main

continued on page 6

Latest Tool Releases

These tools are available on the DoD PKE site at <http://iase.disa.mil/pki-pke>.

CRLAutoCache 2.01 BETA

This beta release of CRLAutoCache includes patches to support the Apache Directory Server (ApacheDS) and allow the publishing of CRLs to any LDAP location.

FBCA Cross-Certificate Removal Tool 1.06

This release of the FBCA Cross-Certificate Removal Tool includes new capabilities to automatically trim the longer certificate path in Microsoft Operating Systems to the Federal Bridge and maintain the shorter path to DoD Root CA 2. This version also removes the new Interoperability Root to DoD Root CA 2 cross-certificate issued in September 2010.

InstallRoot for BlackBerry

This release includes CA certificates issued since the last release (CAs 25 and 26), and is available at <https://www.dodpke.com/blackberry/> in addition to the DoD PKE IASE site.

Latest Document Releases

These documents are available on the DoD PKE site at <http://iase.disa.mil/pki-pke>.

Tumbleweed Desktop Validator 4.9

This updated version of the guide includes instructions for configuring Tumbleweed Desktop Validator 4.9 to support the OCSP Delegated Trust Model (DTM).

Tumbleweed Desktop Validator 4.10

This guide provides recommended configuration steps for Tumbleweed Desktop Validation 4.10 according to DoD best practices.

SHA-256 Slick Sheet

This slick sheet provides an overview of the SHA-256 hashing algorithm and how migration to its usage will impact the DoD.

OCSP Slick Sheet

This slick sheet describes different OCSP client configuration options and trust models, including how they are used within the DoD.

SIPR Token Slick Sheet

This slick sheet provides an overview of the new SIPR token and addresses frequently asked questions about its distribution and use.

continued on page 6



Anatomy of a Certificate Slick Sheet

This slick sheet describes the structure of a certificate, and the information that is contained within each extension.

BlackBerry: Certificate Fetching Troubleshooting

This guide assists BlackBerry Administrators in troubleshooting issues with BlackBerry devices being unable to automatically fetch certificates from DoD411.

BlackBerry: Deleting Expired OCSP Certificates

This guide provides instructions for manually removing expired OCSP certificates whose presence will prevent revocation checking from completing successfully.

BlackBerry: Associating a Secondary Email Address to a Certificate

This guide provides instructions for sending an encrypted email to a recipient at an email address that does not match the email address in their public certificate.

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

OCSP Trust Models – *continued*

methods, or trust models, by which an OCSP responder can be given that authority: Explicit Trust, Certification Authority (CA)-Signed Trust, and Delegated Trust.

In the **Explicit Trust Model** (sometimes colloquially referred to as the self-signed model, due to the fact that the DoD has historically used self-signed OCSP responder certificates), an OCSP client is explicitly configured to look for a specific certificate to have signed the OCSP response. To work with this model, OCSP clients typically must have the OCSP responder’s signing certificate installed in their local trust store, and additionally must configure properties to allow the client to uniquely identify the responder’s certificate in order to match the certificate signing a particular response with the responder’s certificate installed in the local trust store. This is the trust model that the DoD’s Robust Certificate Validation Service (RCVS) on NIPRNET used to employ, and which is still used on SIPRNET (see In the Pipeline for information on changes coming soon).

In the **CA-Signed Trust Model**, the CA that issued the certificate whose status is being determined directly signs the OCSP response. This model is not currently used by the DoD.

In the **Delegated Trust Model (DTM)**, each CA issues a certificate to the OCSP responder specifically to be used for signing OCSP responses (denoted by the inclusion of id-ad-ocspSigning in the extended key usage extension of the certificate). The OCSP signing certificate issued by the CA that issued the certificate whose status is being determined is then used to sign the OCSP response. OCSP clients typically support this model out of the box, and no special configuration (such as installation and configuration of the signing certificate, as with the Explicit Trust Model) is necessary. However, if an OCSP client has been previously configured for the Explicit Trust Model, the configuration may need to be updated to remove the explicit configuration settings in order for DTM to be supported. The DoD RCVS on NIPRNET completed migration from the Explicit Trust Model to DTM in the fall of 2010.

RA/LRA/KRA/TA Corner – *continued*

RA/LRA/KRA Contact Information

RA Operations			
Name	Organization	Contact Information	COCOMS Support
Army	Army CTNOSC Army NETCOM	ctnosc.pki@us.army.mil (Equipment Certificates) 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
DISA	DISA RA Operations	disaraoperations@disa.mil	Not an Executive Agent
Joint Staff	Joint Staff RA Support	jsra@js.pentagon.mil	Not an Executive Agent

