-----Original Message-----
From: Jones, Martin L CIV DISA PEO-MA
Sent: Thursday, October 13, 2011 9:56 AM
To: dod-pki-technical-lead-list@LISTS.MITRE.ORG; APPL PKI
Cc: Schaen, Samuel I CTR DISA PEO-MA; Scogin, Allison CIV DISA PEO-MA; Scheffler, Philip A CIV DISA PEO-MA; Burkhart, Linderman L CIV DISA PEO-MA; Coulson, Cindy Ms CTR DISA CD21; Sieger, Robert Mr CIV DISA CDK21; CHA-PKI_Chambersburg Processing Element; 'Alex Brown'; Smith, Jason Mr CTR DISA CDK53; 'iacacpki.helpdesk@us.army.mil'; PKE_Support; 'afpki.helpdesk@lackland.af.mil'; 'itac@infosec.navy.mil'; 'raoperations@mcnosc.usmc.mil'; 'IPMSupport@whs.mil'
Subject: PKI PMO deployment of new Public Key Infrastructure (PKI) Certification Authorities (CAs) (UNCLASSIFIED)

Classification: UNCLASSIFIED
Caveats: NONE

ALLCON;

Narr/Ref Public Key Infrastructure (PKI) supports security services including authentication to systems, confidentiality and integrity of data including secure email. New certification authorities (CAs) have been added to the infrastructure and must be configured to be trusted by all DoD public key enabled systems to avoid denial of service to users.

1. Exsum: The purpose of this message is to inform the DoD Combatant Commands, Services, and Agencies (CC/S/A) that the DoD PKI has deployed new CAs. The new CAs includes CA-27, CA-28, CA-29, CA-30, EMAIL CA-27, EMAIL CA-28, EMAIL CA-29, and EMAIL CA-30 and are available in the latest release (3.15) of InstallRoot. This release also includes four new External Certification Authority (ECA) intermediate CAs which should be installed on systems currently trusting the ECA PKI.

2. Current Situation. Public key enabled systems are configured to trust current CAs. However, after the new CAs begin issuing certificates, systems will be unable to authenticate users with certificates issued by the new CAs unless the systems have been configured to trust these new CAs. In addition, users will receive error messages when reading signed email or documents from other users with new certificates until steps are taken to trust the new CAs.

3. Guidance. System and network owners must ensure that all public key enabled systems have the new CA certificates installed in their trust stores before 14 December 2011. Many organizations have procedures (e.g., group policy objects) for pushing new certificates to desktops utilizing InstallRoot, which is available on the Information Assurance Support Environment (IASE) at http://iase.disa.mil/pki-pke/function_pages/tools.html under the Trust Store Management category. New for the 3.15 release of InstallRoot are PKCS#7 PEM and DER-formatted certificate bundles as well as associated files and instructions for validating them in the lettered archives (e.g. InstallRoot 3.15 A, E, J) containing the same certificates installed by the corresponding command-line executables. These certificate bundles provide a mechanism for trusted distribution of the DoD PKI root and intermediate CA certificates in a format consumable by OpenSSL, NSS, Firefox, and other applications and trust stores used by MAC OS, UNIX, and Linux Operating Systems.

4. Task. System and network owners must ensure that all public key enabled systems have the new CA certificates installed in their trust stores before 14 December 2011 to support new Common Access

Cards (CAC) and other certificates issued from these CAs (e.g. web server and domain controller certificates). Installation of the new CA certificates in system trust stores is critical to avoid denial of service issues for users issued CACs with certificates from the new CAs. System and network owners that use Online Certificate Status Protocol (OCSP) for certificate revocation checking must ensure their OCSP client configurations are updated to include the new CAs. If a CRL caching solution is being used ensure it is configured to retrieve the new CRLs associated with the new CAs. Configuration guidance for Administrators, Integrators and Developers can be found on the DoD PKI-PKE website on IASE at http://iase.disa.mil/pki-pke

5. Applicability. This message applies to all DoD Components. This includes, but is not limited to, all combatant commands, services, agencies, field activities, U.S. Coast Guard, and all other entities, military or civilian, that use the DoD PKI.

6. Points of contact:

DoD PKI Help Desk:
DSN 339-5600
COMMERICAL (800) 490-1643
Email okcpeoservicedesk@csd.disa.mil

DoD Public Key Enablement (PKE) Team
Email pke_support@disa.mil
PKE website http://iase.disa.mil/pki-pke

Martin Jones (DISA)
DSN 381-8743
COMMERCIAL (301) 225-8743
NIPR: martin.jones@disa.mil

Martin Jones
IA-4, Identity Management Division
Martin.Jones@disa.mil
301-225-8743
BB: 703-217-1442

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE