-----Original Message-----
From: RSS DMDC IPMSCG
Sent: Monday, May 12, 2008 1:50 PM
To: [IPMSCG Action Officers]
Subject: TECHNICAL NOTIFICATION--Stand-up of new CAs (19 and 20)

Earlier this week, key pairs were generated for four new CAs: CA-19, Email CA-19, CA-20, and Email CA-20.

Although the CAs have been keyed, as is customary, Services and agencies will be given 60 days to push the new certificates to desktops and other applications. A new InstallRoot executable is available from the DOD PKE web site (https://www.us.army.mil/suite/page/474113) at the "Tools" link.
Administrators need to ensure that all desktops and servers have the most up to date certificate trust stores before 1 July 2008.

As part of continuing efforts to increase security, these new CAs will have certificates signed with 2048-bit keys (like the root) rather than 1024 as has been the practice until now for CAs. Also, new Personal Identity Verification (PIV) certificates will be supported (and retrofitted to existing active CAs). Finally, new policy Object Identifiers (OIDs) will be included in the certificates produced by these CAs to help distinguish the 2048-bit certificates from 1024-bit certificates. It is expected that most users will not be affected by the information in this paragraph and it is for information only.

Send on behalf of Sam Schaen, DISA PKI