-----Original Message-----
From: DODHRA MC-ALEX DMDC Mailbox IPMSCG
Sent: Friday, June 03, 2016 12:41 PM
To: DODHRA MC-ALEX DMDC Mailbox IPMSCG; DODHRA BEAU-ALEX DMDC Mailbox DOD Identity Council
Subject: ANNOUNCEMENT-DoD IdC TEWG Approves Release of SHA256 Versions of the CAC

DoD IPMSCG/IdC Representatives,

We are pleased to announce the approval of the SHA256 versions of the CAC. It has been tested by the participants of the DoD Identity Council's Test and Evaluation Work Group (TEWG) and authorized to be moved into DMDC's operational card inventory. Details about the card platform are as follows:

Product name:
- G&D Sm@rtCafe Expert v3.2
- Gemalto TOP DL GX4 144K
- Oberthur ID-One Cosmo 128 v5.5 for DoD CAC

Name printed on back of CAC:
- G&D FIPS 201 SCE 3.2
- Gemalto TOP DL GX4 144K
- Oberthur ID One 128 v5.5 Dual

Applets:
- CAC 2.6.2.b applet structure

Certificates:
- End entity (EE) DoD PIV Authentication certificate at RSA 2048 with SHA 256 (CRL/OCSP at SHA256)
- EE DoD Identity Certificate at RSA 2048 with SHA256 (CRL/OCSP at SHA256)
- EE DoD E-mail Signature Certificate at RSA 2048 with SHA256 (CRL/OCSP at SHA256)
- EE DoD E-mail encryption certificates at RSA 2048 with SHA256 (CRL/OCSP at SHA256)

PIV objects (facial image/fingerprint template/CHUID):
- Signed with SHA256.

DMDC expects to begin issuing CACs around the world with this configuration between June 11, 2016 and June 30, 2016. If there are any questions, feel free to contact Ms. Felicia Sexton (DMDC/DoD IdC TEWG Chair, 571.372.1083, felicia.f.sexton.civ@mail.mil).

Respectfully,
Mike Butler
DMDC
DoD IPMSCG Executive Secretary/DoD IdC Chair