



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

MAY 08 2012

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM
EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF
DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF
DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Public Key Infrastructure (PKI) Interoperability with FVEY partner nations on the Nonsecure Internet Protocol Router Network (NIPRNet)

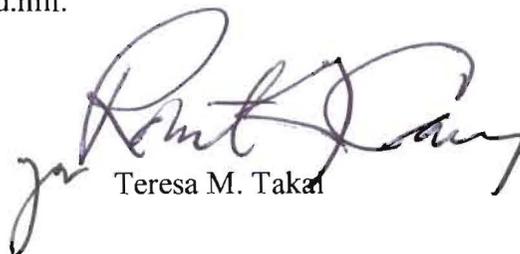
References: (a) DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key Enabling," May 24, 2011
(b) Allied Communications Publication 185, "Public Key Infrastructures (PKI) Cross-Certification Between Combined Communications-Electronics Board (CCEB) Nations," November 2011

In accordance with reference (a), the Department has implemented a DoD-wide PKI on the NIPRNet to enhance the security of DoD information systems.

DoD requires its FVEY partner nations (Australia, New Zealand, Canada, and the United Kingdom) to use PKI for secure communication with DoD personnel on the NIPRNet, and authentication to DoD NIPRNet websites. In February 2006, the FVEY partner nations signed an Annex to the Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding (CJM3IEM), in which DoD agreed to issue software PKI certificates to FVEY partner nations for three years while they developed their own PKI's. The initial agreement has since been extended twice, and expires at the end of May 2012.

To enhance the security of networks, information systems and websites, DoD will cease issuing software PKI certificates to FVEY partner nations after the CJM3IEM Annex expires. After May 31, 2012, FVEY partner nations that interact with DoD on the NIPRNet will be required to purchase Medium Token Assurance PKI certificates from DoD ECA vendors or use their approved PKI IAW reference (b). Software PKI certificates that have already been issued by DoD to FVEY partner nations will be accepted until the end of May 2013. Information on the ECA program can be found in the attached information sheet or at <http://iase.disa.mil/pki/eca/index.html>.

For additional information about this memorandum, my point of contact is Mr. Tim Fong, 703-614-1991, or timothy.fong@osd.mil.



Teresa M. Takai

Attachments:
As stated

ATTACHMENT

The DoD External Certification Authority (ECA) Program

In order to obtain medium token assurance ECA certificates, FVEY partner nations will need to go through one of the three DoD-approved ECA certificate providers:

- Operational Research Consultants (ORC): <http://www.eca.orc.com/>
- VeriSign (Symantec): <http://www.verisign.com/eca>
- IdenTrust: <http://www.identrust.com/certificates/eca/index.html>

While the details and order vary by ECA provider, applicants generally need to perform the following steps to obtain ECA certificates:

- 1) The applicant fills out an application for medium token assurance ECA certificates on the provider's website. ECA providers also sell FIPS 140-2 compliant smart-cards and USB tokens, as well as smart-card readers and middleware.
- 2) The applicant brings a passport, a second official identity credential, and proof of organizational affiliation to a U.S. Consular Officer, a U.S. Judge Advocate General (JAG) Officer, or an authorized DoD employee for in-person identity proofing.
- 3) After approving the application and verifying the identity-proofing, the ECA provider will send an e-mail to the applicant with information on how to retrieve their certificates and download them onto the smart-card or USB token.
- 4) The applicant imports the ECA Root and subordinate CA certificates into their workstation's trust store. For instructions, see http://iase.disa.mil/pki/eca/installation_of_eca_certificates.html.

Estimated Costs per Applicant

- ECA Certificates:
 - 1 year certificate: \$119 - \$149
 - 2 year certificate: \$218 - \$259
 - 3 year certificate: \$279 - \$329
 - Bulk purchases are available as well. See ECA provider websites.
- Additional hardware and software
 - USB Token: \$30
 - Smart-Card: \$20 - \$30
 - Smart-Card Reader: \$25
 - Middleware: \$30
- In order to validate digitally-signed e-mails, applicants will need to purchase certificate validation software separately.

Further Information

- DISA ECA Website: <http://iase.disa.mil/pki/eca/index.html>
- Locations of U.S. consular offices and embassies: http://travel.state.gov/travel/tips/embassies/embassies_1214.html