



DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer/G-6

SAIS-CB

13 JUN 2013

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Updated Alternative Smart Card Logon (ASCL) Token Policy Guidance

1. References:

- a. Memorandum, Army Chief Information Officer/G-6, 17 Aug 11, subject: Alternative Smart Card Logon (ASCL) Token for Two-Factor Authentication.
- b. Memorandum, Department of Defense Chief Information Officer, 14 Aug 06, subject: Approval of the Alternate Logon Token 06.
- c. Department of Defense Instruction 8520.02, subject: Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 11.
- d. Army Regulation 25-2, subject: Information Management – Information Assurance, Rapid Action Revision, 23 Mar 09.
- e. Memorandum, Under Secretary of Defense for Personnel and Readiness, 31 Mar 11, subject: Directive-Type Memorandum (DTM) 08-003, Next Generation Common Access Card Implementation Guidance, Incorporating Change 2.
- f. Memorandum, Deputy Chief of Staff, G-2, 5 Oct 10, subject: Interim Policy Guidance for Common Access Card (CAC) Background Vetting for Foreign Nationals.

2. This memorandum supersedes the Army CIO/G-6 ASCL token guidance for two-factor authentication (reference 1a), and provides additional policy guidance for implementation of the ASCL token, approved by the Department of Defense Chief Information Officer (reference 1b) and DoD Instruction 8520.02 (reference 1c).

3. All Army activities shall accept the ASCL token as an alternative PKI credential to the CAC for logical two-factor authentication to the Non-Secure Internet Protocol Router Network (NIPRNet). Although medium-assurance software certificates are primarily intended for use on servers and other non-person entities (NPEs), they are approved for use on the ASCL token to identify people on the NIPRNet. Without CIO/G-6 approval, use of software certificates beyond NPEs and the ASCL is prohibited.

SAIS-CB

SUBJECT: Updated Alternative Smart Card Logon (ASCL) Token Policy Guidance

4. The CAC is the primary hardware token for NIPRNet logon by eligible DoD uniformed, civilian and contractor personnel, authorized foreign officials, and properly vetted and adjudicated foreign nationals (reference 1d). Army network users who are otherwise eligible to receive a CAC, but are constrained by technical limitations of the network or host-nation agreements, are eligible to receive an ASCL token. To receive an ASCL token, Army users must meet the vetting and adjudication standards required to receive a CAC (references 1e and 1f).

5. Several user groups are approved to receive ASCL tokens. To extend the user groups, Army organizations must submit a request to the CIO/G-6 for consideration. CIO/G-6 authorizes ASCL token issuance to the following user groups or personnel.

- a. Network system administrators.
- b. General Officers and civilian equivalents, and their staff aides.
- c. Paid American Red Cross employees supporting U.S. military installations in the continental United States.
- d. Army Junior Reserve Officer Training Corps instructors.
- e. Vetted and approved foreign nationals, foreign exchange personnel, foreign officers or foreign liaison officers eligible to receive a CAC whose host-nation agreements prohibit their use or possession of a CAC.
- f. Retired physicians or medical staff who require access to the Medical Protection System application.

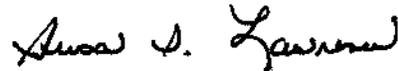
6. ASCL tokens issued to the staff of General Officers (GO) and their civilian equivalents (i.e., Senior Executive Service (SES)) for the purpose of authenticating to the network and reading encrypted email on behalf of the GO/SES will contain a DoD PKI identity certificate linked to the GO's/SES's Electronic Data Interface Personal Identifier and a copy of the GO's/SES's recovered private encryption key. The ASCL token will not contain a DoD PKI signature certificate; thus, GO/SES staff will not have the capability to sign emails or sign forms as or on behalf of the GO/SES.

7. System owners, application owners and program managers shall coordinate with Network Enterprise Technology Command G-5 if a technical solution is required in order to authenticate ASCL tokens to Army information systems.

SAIS-CB

SUBJECT: Updated Alternative Smart Card Logon (ASCL) Token Policy Guidance

8. The point of contact for this action, and for consideration of new ASCL use cases, is Mr. Jude Roeger: (703) 545-1749 (DSN 865) or jude.roeger2@mail.mil.


SUSAN S. LAWRENCE
Lieutenant General, GS
Chief Information Officer/G-6

DISTRIBUTION:

Principal Officials of Headquarters, Department of the Army
Commander

- U.S. Army Forces Command
- U.S. Army Training and Doctrine Command
- U.S. Army Materiel Command
- U.S. Army Pacific
- U.S. Army Europe
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Africa
- U.S. Army Cyber Command
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Forces Strategic Command
- U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Criminal Investigation Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Installation Management Command
- Superintendent, United States Military Academy
- Director, U.S. Army Acquisition Support Center

CF:

- Director, Army National Guard
- Director of Business Transformation