U.S. Department of Defense Common Access Card

One of the most advanced smart ID card programs in the United States is the Department of Defense (DoD) Common Access Card (CAC), a smart card that serves as the DoD standard identification for active duty military personnel, selected reserve personnel, civilian employees, and eligible contractor personnel. The CAC is the principal card used for logical access to DoD computer networks and systems, and it will be the principal card used to enable physical access as systems are installed for authentication and access at DoD facilities in the future. As of July 2004, DoD has issued over 5.4 million smart cards. (This number includes reissues to accommodate changes in name, rank, or status and to replace lost or stolen cards.) As of the same date, approximately 3 million unterminated or active CACs are in circulation. DoD has deployed an issuance infrastructure at over 930 sites in more than 25 countries around the world and is rolling out more than 1 million card readers and associated middleware. A key goal of the CAC program is to meet DoD's mandate to sign all electronic mail and other electronic documents digitally.

Future plans include using the CAC to sign and encrypt e-mail, expanding the number of portals capable of doing Web-based e-business using PKI authentication tools, adding a biometric to the card to provide three-factor authentication, and expanding the use of the cards to include physical access by adding a contactless chip using ISO/IEC 14443 Parts 1-4 with a FIPS-approved algorithm.

DoD's personnel identity protection addresses threats to the privacy of its members, employees, and beneficiaries, establishes a secure and authoritative process for the issuance and use of identity credentials in DoD, and ensures that DoD benefits and access to DoD physical and logical assets are granted based on authenticated and secure identity information. DoD personnel identity protection systems include, but are not limited to the CAC, The Defense Biometrics Identification System (DBIDS), the Defense National Visitors Center (DNVC), and the Defense Cross-Credentialing Identification System (DCCIS).

The DBIDS is a readily deployable system for capturing, storing, and comparing biometric data to use for authentication. The system also provides a means of registering all personnel requiring access, incorporating complex rules of sponsorship and access, linking access to sponsor, and limiting access by location, building, and force protection level. In addition, DBIDS allows installation security personnel to control access and authenticate identity for population elements not already provided for by DNVC and DCCIS, including maintenance personnel, janitorial staff, and contractor personnel from non-DoD organizations.

DNVC is a system that enables participating DoD facilities to perform physical authentication procedures on DoD personnel presenting the CAC for entrance into DoD facilities. The DNVC is part of the DoD identity management strategy, designed to issue tamper-free smart cards to verified individuals and to authenticate both the credential and the credential holder whenever the card is presented. DNVC is designed to accommodate different readable formats supported by the CAC and uses biometric data as the primary method of authentication. The DNVC is Web-based and provides a means for strengthening security across participating DoD organizations.

DCCIS is an extension of DNVC. DCCIS is an initial proof-of-concept system that proposes to resolve cross-credentialing interoperability difficulties between DoD and certain of its commercial partners. DNVC can be DCCIS-enabled, in which case a participating DNVC facility connects with the DCCIS member organization database to authenticate visiting personnel from those organizations.

As initial issuance of the CAC nears completion, DoD's focus has expanded to include post-issuance CAC support and ensure interoperability with other smart card initiatives throughout the Federal Government. As the government becomes more aware of the importance of identity authentication and assurance, the need to define common policies, interoperability requirements, and technical standards becomes more apparent.

DoD is also in the early stages of planning to serve other large communities that are closely tied to DoD, including military dependents, DoD recipients of health care services from the TRICARE medical system, and veterans.

This profile was developed by the Smart Card Alliance Secure Personal ID Task Force as part of the report, "Logical Access Security: The Role of Smart Cards in Strong Authentication," available at http://www.smartcardalliance.org/alliance_activities/secure_physical_access_report.cfm. Additional information about the DoD CAC program and other U.S. government smart card initiatives can be found at http://www.smart.gov. For more information about how smart cards are used for secure identification applications, visit the Alliance web site at http://www.smartcardalliance.org.