

United States Department of Defense DoD Common Access Card (CAC)

||||| A smart move to next-generation identity credentials



FINANCIAL SERVICES & RETAIL

ENTERPRISE

INTERNET CONTENT PROVIDERS

PUBLIC SECTOR > CASE STUDY

TELECOMMUNICATIONS

TRANSPORT



gemalto^{*}
security to be free

United States DoD Common Access Card (CAC)

IIIIII A smart move to next-generation identity credentials

Identity Management is a critical aspect of the Department of Defense's (DoD) need to control who gains access to specific resources. Historically each resource managed a local access control list and provided employees with credentials for each system. This resulted in employee management and maintenance of multiple credentials for multiple sites. Local access control lists were quickly outdated with constant changes and new assignments for employees, leaving vulnerabilities to the systems.

The DoD conducted a review to move identity management from individual locally maintained systems to a centrally managed approach. As part of this unified system, each employee would be given a single common identity credential. This credential would be used for physical access, to gain access to specific services, provide logical access to information systems including ensuring confidentiality and accountability in email based communications. The result of this review was the introduction of the Common Access Card (CAC). Through the detailed evaluation of potential technologies for the CAC, the DoD selected a Java based card adding a CAC applet to meet their use requirements.

The DoD first issued CAC credentials in October 2001 provided by Gemalto. The CAC program enables secure physical access to DoD facilities as well as secure logical authentication for access to the DoD intranet, systems and related network



> DoD: the nation's largest employer

With 718,000 civilian personnel and more than 1.4 million men and women on active duty, the United States Department of Defense (DoD) is the United States' single largest employer. Established under the National Security Act of 1947, DoD coordinates and supervises all agencies and functions of government relating directly to national security and the military.

Data integrity is of paramount importance given the highly sensitive nature of information handled by DoD employees and contractors on a daily basis. By introducing strong employee authentication measures, DoD has led the way in digital security for the Federal government. Its CAC program has issued over 17 million smart identity badges to date.

resources. The program is the U.S. Federal Government's largest rollout to date.

CAC credentials leverage industry proven Public Key Infrastructure (PKI) cryptographic technology. PKI establishes the foundation and structure for authorized access to DoD systems, while the chip card serves as a hardware token holding several digital keys. Each government identity badge is programmed with a private and a public code.

An end to password and identifier vulnerability

A personal identification number selected by the bearer is used in tandem with the card to access the secure network, forever rendering identity/password combinations obsolete. The smart identity badges

now enable users to access secured applications, digitally sign documents and encrypt and decrypt information from laptops or Blackberry mobile phones.

The CAC's memory and processing capabilities have also enabled a seamless phase-out of unique identifiers. Previously, Social Security Numbers (SSNs) were used widely as a means to identify and authenticate individuals. The upward trend in identity theft witnessed in recent years in the United States led the DoD to formalize a policy on gradual elimination of the use of SSNs, however. Application of the new policy has been swift, thanks in part to CAC card technology.

> Chief technical features of the CAC card

The Gemalto FIPS 140-2 Level 3 certified dual interface smart cards support Java Card Global Platform specifications. It is available in either 64 or 128 kilobytes of EEPROM and supports on-card secure cryptographic functions including key generation, encryption and digital signing. The card is personalized with three PKI certificates and some 30 demographic data elements. To support legacy applications, it also features multiple bar codes and a magnetic stripe. Although the CAC card can store and process data, the DoD uses it mainly as a secure authentication token for accessing data stored on networks.



“One of the greatest vulnerabilities of our networks is posed by weak user names and passwords. Spyware or keystroke tracking software can steal your username and password, and even your personal identification number or PIN. It cannot steal your CAC.”

– Lt. Gen. Steven W. Boutelle, Chief Information Officer/G-6 (CIO/G-6)

■ Simple to deploy, even easier to use

Smart card applications feature an open-system configuration. Despite its tamper-proof design, the CAC card’s open system engineering facilitates interoperability with a wide range of commercial, government and military applications. The basic demographics and unique personnel benefit entitlements stored on the CAC chip enable swift yet highly reliable authentication in any DoD transaction.

Personnel can acquire the card by enrolling in the Defense Enrollment Eligibility Reporting System (DEERS) in accordance with clearance procedure. This procedure requires eligible employees and contractors must meet all Real-Time Automated Personnel Identification System (RAPIDS) requirements to obtain their CAC card from one of over 1,500 RAPIDS central issuance centers.

At any one time, the CAC card is being used by 4.5 million personnel:

- Active-duty armed forces
- National Guard, Reserves
- DoD civil servants
- Select contractor workforce

Through secure CAC-enabled access to the Army Knowledge Online (AKO) portal, eligible employees and contractors can access and update their personnel records in the click of a mouse. AKO’s primary function is e-mail, which enables information to pass through the chain of command quickly and efficiently. AKO is also the central point for management of all career development and financial, education and medical benefits, among others.

Beyond their online authentication function, CAC cards enable highly secure access to DoD facilities including controlled-access bases, buildings, mess halls and gyms. They also manage a number of military privileges, such as access to commissaries, military exchange

stores and Morale, Welfare and Recreation (MWR) centers.

■ Essential to every aspect of life at DoD

Since its implementation, the CAC card has significantly expedited administrative processing. The card provides all necessary information in a single use, preventing countless hours of busywork, such as filling out forms by hand. Flight manifest tracking, weapons issuance and deployment processing can be completed in minutes rather than hours, meaning that employees and contractors spend less time waiting in line.

But the CAC card is not just a timesaver. With over 1.5 million CAC transactions logged daily, this fully scalable solution has quickly become a vital part of everything DoD employees and contractors do throughout their workday. More importantly, it has streamlined many business practices and processes, making DoD operations more efficient and secure than ever. In addition to ensuring fail-safe physical and logical security, the CAC card:

- Enables exact headcounts through computerized building access files
- Improves accountability for food service and recruit functions
- Provides reliable authentication for healthcare and benefits processing
- Has served in lieu of a visa for deployment to Iraq
- Is recognized as an identification card under the Geneva Conventions

■ Federal identity badges enter the digital age

As part of the sweeping reforms to United States national security introduced in the wake of the September 11 attacks, the need for secure, reliable identity credentials issued by Federal agencies to their employees and contractors was outlined in Homeland Security Presidential Directive (HSPD-12).

Signed in 2004, the presidential directive introduced a mandatory, government-wide standard for interoperable, smart card-based identification to be deployed across the entire federal government. The new standard aimed to eliminate broad variations in the quality and security of identification used to gain access to federal facilities. This standard was built from the extensive



“When I go to the gym, the only identification I take is my Common Access Card”
– Spc. Joshua Simanteris, of Syracuse, N.Y., first cook

experience of the DoD CAC program to form a common interoperable credential for all federal employees.

■ Personal Identity Verification

The new government identity badges would come to be known as the Personal Identity Verification (PIV). Specifications set forth stringent criteria for rapid electronic authentication, as well as resistance to identity fraud, tampering, counterfeiting and terrorist exploitation. The standard also calls for issuance only by accredited providers, based on sound criteria for verifying an individual employee’s identity.

The DoD migrated their CAC program to embrace the PIV standards and are now the leading agency in the deployment and use of secure electronic smart card based credentials under HSPD-12.

KEY DATES

October 10, 2000 – Personnel at the Pentagon and Marine Corps Base in Quantico, Virginia, are the first to receive the new card in a pilot.

September 11, 2001 – Gemalto is designated an accredited provider for the DoD's implementation of the CAC card program and is first to achieve a FIPS140-1 Level 2 cryptographic certification of a Java Card for the CAC program.

August 27, 2004 – The White House issues Homeland Security Presidential Directive 12 (HSPD-12), setting forth policy for a common identification standard for Federal employees and contractors.

October 1, 2006 – Pursuant to the Presidential mandate, DoD begins enabling logic access using CAC. No usernames and passwords are allowed for logical access from this date. Over 50% reduction in cyber attacks result overnight.

March 28, 2008 – Directive-Type Memorandum 07-015-USD(P&R) establishes DoD policy on the elimination of unnecessary use of SSNs.

October 27, 2009 – Gemalto's Personal Identity Verification (PIV) card is listed on the Federal government's General Services Administration (GSA) approved product list. This included a range of 144Kb and 72Kb dual and tri-interface PIV products.

A longstanding partnership with trusted partner Gemalto

As an accredited provider of smart cards to the DoD, Gemalto has shipped over 25 million smart identity credentials to the Federal government to date. Government identity credentials used to secure the identities of Federal government employees and military personnel account for roughly half that figure. Secure travel documents (ePassports) account for the other half.

The Federal government projects future expansion of its programs to issue highly secure, smart card-based identity credentials within other government agencies. Its overall goal is to deploy a common identity credential for both physical and logical access control across all Federal Executive Branch agencies.

All Gemalto products delivered to the Federal government are manufactured at its state-of-the-art production facility and service center in Montgomeryville, Pennsylvania. The center recently earned Security Assurance Certification from the North American Security Products Organization (NASPO). This voluntary certification underscores Gemalto's commitment to providing a stable, reliable US-based supply chain for identity products.

||||| The world leader in digital security

www.gemalto.com

gemalto
security to be free