CAC and PIV: Government Leading the Way into Mobile Security

CAC and PIV: Government Leading the Way into Mobile Security

The Department of Defense has mandated that its Common Access Card (CAC), issued to military-connected personnel and contractors, be used to secure access to DoD networks and services from mobile devices such as smart phones and tablets. A similar directive could eventually come regarding the Personal Identity Verification (PIV) card issued to federal employees and contractors. This leads to one very big question: what products and technologies are currently available to accomplish that goal? This paper strives to answer that question.

The technologies that are driving mobile device security in the government have been quickly evolving for over a decade. All the while, the need for such technology has remained constant: convenient data assurance and physical security. The US Federal Government and Department of Defense (DoD) has led the way in smart card deployment and is again on the bleeding edge of mobile device security. To best identify the technologies and solutions for mobile device security, we'll examine several areas. First, the history of the Common Access Card and Personal Identity Verification technology and how it has defined the context for mobile security. Second, emerging trends that require new security measures. Third, the current state of smart card technology. Fourth, challenges for technical implementation. Lastly, we'll discuss the most promising technologies that will take mobile security into the future.

Wanted: A Better Security Solution

The DoD has long battled military ID fraud. As printing and reproduction technology improved, so too did the ability for fraudulent card production. A 1997 DoD memo reads in part:

> "The Assistant Secretary of Defense Health Affairs under the Under Secretary of Defense for Personnel and Readiness shall establish overall policy and procedures for providing medical care through the Military Health Services System to authorized beneficiaries and the elimination of fraud, waste, and abuse in the provision of medical benefits."

The Defense Enrollment and Eligibility Reporting System (DEERS) was launched in 1982 to streamline military personnel and medical information. The system was designed to maintain benefits information for active, retired and uniformed service personnel, their families and even some civilian contractors.

Fast-forward to the late 1990's and the DoD implemented the Real-Time Automated Personnel Identification System (RAPIDS) to work alongside of DEERS to facilitate accessing the data stored in DEERS; the two systems work hand in glove. With a system to capture personnel information and a system to securely access that data, DoD access systems took an early shape of what we see today.

In 1999, the Department of Defense launched a smart card initiative to improve physical security, provide network security for data assurance and also to reduce costs by improving workflows and general efficiency.

The goal was one card, the Common Access Card, to provide secure access and authentication into secure networks, while reducing costs and maintaining compliance across departmental, federal and Geneva Convention guidelines.

The DoD succeeded in its challenge and today has issued nearly 25 million smart cards, know as the Common Access Card (CAC).

The CAC works in conjunction with legacy DoD systems. A user must first be registered in the DEERS system and then physically go to a RAPIDS site and prove their identity before obtaining a CAC.

The CAC of 2012 contains all the information necessary to provide physical access security, logical security and even application level security for a wide range of users, from active duty to civilian contractors.

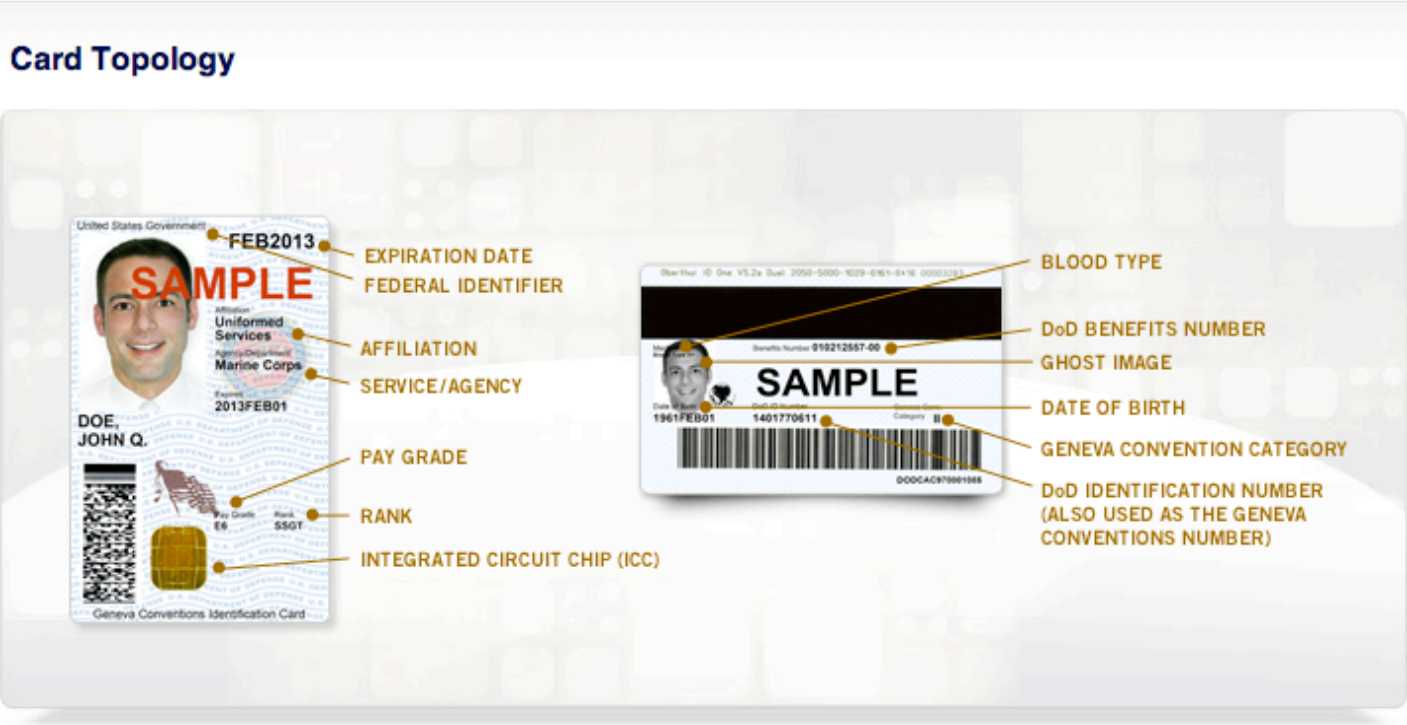
Early iterations of smart cards contained only a magnetic strip containing various access data, from simple identity to banking information. The CAC of today goes far beyond that.

First, the card is designed for multi-factor authentication:

1) What you have (the card)
2) What you know (a PIN)
3) Who you are (fingerprint or other biometric).

Today's card contains an embedded Integrated circuit chip that can perform a variety of functions including storing biometric data like fingerprints, facial mapping and even iris mapping. The IC chip can perform additional access functions to allow or disallow access at the application level. The increasing memory and computing power of the on-board IC chip plays an important role in an emerging era of bring-your-own-device (BYOD).

Here is a diagram of the information contained on today's CAC:



(Source: http://www.cac.mil/common-access-card/)

Similar to the CAC, Federal Information Processing Standard (FIPS) 201, entitled Personal Identity Verification of Federal Employees and Contractors, was developed to satisfy the requirements of HSPD 12, approved by the Secretary of Commerce, and issued on February 25, 2005.

The PIV card is issued to all Federal employees and contractors for physical and logical access using strong authentication credentials and identity proofing. There is a variant of PIV known as the PIV-I as well. In many cases, CAC and PIV are used interchangeably since they share many similar data structures and purposes.

In short, the primary differences between the smart card types is as follows:

Common Access Card - issued by the Department of Defense to active and retired military personnel,.

Personal Identification Verification Card - issued by federal agencies to federal employees and contractors.

PIV-I - for non-federal issuers needing access to government data and physical locations.

It is important to note that the cards have differing standards. For example, a PIV must conform to the standards set forth in the Federal Information Processing

Standard, Publication 201 (FIPS 201). A PIV-I card does not necessarily meet all the standards in FIPS 201.

All of these cards represent similar challenges from a technical, security and practical usage perspective.

Match-On-Card Technology

With increased microprocessing power and speed contained in the Integrated Circuit chips on smart cards, biometric authentication no longer has to be stored in a central database. This is an important consideration, because each mobile device is essentially an untrusted terminal.

With today's smart card, biometric data is not only stored on the card itself, but the access decision point is also processed directly on the card. This creates a desirable scenario, where the mobile computing device becomes a secure access point.

Moreover, concerns about the central storage and management of biometric data points are very real. Resistance to implementation has often centered around the en masse capture and storage of sensitive biometric data. When the bio-mapping is contained on the card itself, this issue is largely eliminated.

Enrollment and administration still need to be properly handled as an essential part of the secure ecosystem. DoD has done this through integration with the existing DEERS and RAPIDS systems described above.

Though match-on-card technology secures physical and logical access, there is still a security gap with the mobile devices being widely used.

The Innovation That Changed Everything

After the release of the iPhone and Android, a flurry of technology innovations ensued. New smart phones, the iPad, and other tablets of all stripes rapidly hit the marketplace. Along with all the hardware, new apps flooded the scene.

By 2012, mobile devices have swept into the mainstream. According to a 2012 comScore report 42% of all US mobile subscribers and 44% of mobile users across the EU5 are using smart phones.

App usage mirrors the growth in mobile device usage. In 2011, there were just as many people using apps to access mobile media as those who used browsers.

The implications for DoD could not be overlooked. In-theater operations could now be directed like never before. Information sharing and collaboration accelerated. Deploying assets to field offices and general geographic distribution became more agile as information could be so readily accessed and shared.

For all the benefits, there was a shadow following close behind. While the benefits of mobile computing were extreme, the door was opened for a great number of potential security gaps.

With millions of DoD personnel walking around with powerful computers in their front pockets, there became an immediate need for new security protocol. That protocol would include directives for physical and logical security.

Practical Uses of Mobile Devices and Match-On-Card

While match-on-card technology greatly enhanced physical and logical security protocols, using it with a mobile device was seen as cumbersome and inefficient. Smart card readers work fine in a desktop environment, since the reader can be hard-wired and left in place on the desk surface for regular access. But with a mobile device, usability becomes a critical issue.

The first versions of mobile card readers still used an external and separate device required for the authentication. An iPhone user, for example, would have to connect the device via the main accessory port to an external card reader via cable or bluetooth that performed the authentication and allowed access.

The need for a second piece of hardware that required the mobile device to be docked into or hard wired is so cumbersome that adoption was resisted.

Precise Biometrics examined this problem and developed Tactivo™, to overcome the issues of inconvenient access.

Tactivo is smart card and biometric reader that integrates seamlessly with an iPhone or iPad. Tactivo could be described as an iPhone or iPad case with a built-in reader, or as a smart card reader disguised as a case.

This technology creates a usable and adoptable platform so that government agencies can fully leverage the power of the latest CAC and PIV technologies, while ensuring that users enthusiastically adopt their use.

This smart card reader supports CAC as well as PIV, PIV-I, and Transportation Worker Identification Credential (TWIC) cards, so it can operate in a variety of environments. And with a built-in biometric reader, it is the mobile device security technology gold standard by enabling multi-factor authentication on these mobile devices.

Security Threats Still Abound

While data and physical security has been dramatically improved with the introduction of advanced biometrics and solutions like Tactivo, there are still security risks that can only be mitigated by a well-informed user community.

In early 2012 reports circulated about a China-based attack on CAC users at the DoD. The attack used documents disguised as official, but contained an executable file that logged keystrokes, thereby capturing the personal identification number used by CAC holders.

While such a breech can only be effective when the compromised user is connected to the network, it underscores the need for training all users on the risks associated with opening files of unknown origin or type.

Still, by implementing multi-layered security protocols including biometrics, match-on-card and deploying these technologies in an easy-to-use format like Tactivo, the

road has been paved for widespread deployment of secure mobile devices across government agencies.

Conclusions

Mobile security will continue to be the hot topic among not only government agencies but also in the corporate enterprise. Although the implementation and usage has been hastened by modern security threats, technology has evolved at a pace that allows government agencies to embrace mobile computing and leverage the portability it brings to both active military and civilian agencies.

By integrating multi-factor authentication into devices that are user friendly, and which accommodate the most recent mobile technologies, the government will be able to successfully deploy access methods to both physical and logical infrastructure and do so with a high degree of security.