PKWARE®

Alternative Uses of Common Access Cards (CAC) to Protect Sensitive Defense Data

TECHNICAL WHITEPAPER

TABLE OF CONTENTS

INTRODUCTION

The Department of Defense (DoD) selected smart card technology as the best means to satisfy the various requirements for identity management years ago. The unique implementation of this smart technology for defense is known as the Common Access Card or CAC. The CAC, a "smart" card about the size of a credit card, is the standard identification for active-duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel.[1]

Since its inception, the DoD has issued more than 24 million smart card-based secure credentials[2] with 3.5 million employees using CACs to electronically sign e-mails, submit time and attendance information securely, gain physical access to controlled sites, and most significantly, log onto to the DoD network. In 2011, the DoD issued more than 10,000 cards a day to its employees.[3]

The architecture is proven for its express purpose of authenticating personnel before granting access to facilities and systems. Several procedures surround issuance of the credential, requiring appropriate background checks before a CAC is issued, and periodic status review to confirm continued eligibility.

This paper explores the additional and alternative data security uses for smart media containing electronic credentials and highlights practical use in daily operations to further enhance overall ROI.

COMMON ACCESS CARD: BACKGROUND

Accurate identification of service personnel can be traced back to the first issuance of dog tags during the Franco-Prussian War of 1870. The more sophisticated "CACs" began taking shape in 1996, when the Army tested a multi-access reader card. "By November 1999, DoD created what became the Common Access Card office and began to create the DoD wide standard for smart cards. In a short amount of time, the DoD saw the huge benefits the card could provide and pushed the issuance across the department. And by 2006, the military issued its ten millionth card." [3]

The objective of the CAC is to enhance security of military personnel, plants, and systems while increasing government efficiency, reducing identity fraud in access to defense benefits such as medical care and post exchange (PX), and protect military personnel and dependents' personal privacy. It also serves as an identification card under the Geneva Conventions. Some may say the CAC paved the way for the PIV credentials carried by federal employees across the country. Others go even further calling it the example for all high-tech, Public Key Infrastructure (PKI)-enabled IDs.[2] (PKI is briefly discussed later in this document.)

The DoD's CAC became the model for the 2004 Homeland Security Presidential Directive-12 (HSPD-12).[3] The Directive mandated Personal Identity Verification (PIV) cards to be issued for civilian executive branch employees and contractors.

A Closer look at HSPD-12 Intent and the CAC

Years after the DoD had established the CAC program and developed a sophisticated infrastructure to support it, the formal HSPD-12 directive came from President George W. Bush. HSPD-12 calls for a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and to the employees of federal contractors.

This directive in conjunction with The Office of Management and Budget Memo 24 of 2005 (OMB M-05-24) requires federal agencies to issue identity credentials that meet the Federal Information Processing Standards

(FIPS) 201 specification. All information systems used by, or on behalf of, a federal agency must comply with FIPS; established by the National Institute of Standards and Technology (NIST). The NIST is a non-regulatory branch of the U.S. Department of Commerce.

Personal Identity Verification --PIV

FIPS 201, specifically defined in support of HSPD-12, is the NIST standard for PIV. The NIST is responsible for developing the standards and guidance for the cryptography used by Federal Government Agencies. OMB Memo 11-11, establishes that all new systems must be PIV enabled effective immediately, that all existing physical and logical access control systems be upgraded to use PIV and all agency processes must accept and electronically verify PIV credentials issued by other federal agencies.[4]

Under the HSPD-12 mandates, and technical specifications of FIPS 201, the DoD CAC program shifted in line with the civilian agency PIV program. The merge is intended to give the US federal government one electronic identification program for all defense and civilian personnel. As of April 2011, the DoD issued more than 80% of the PIV-compliant CACs with cross use of PKI certificates and is reportedly on track to continue.[2] The Defense Department's CAC was brought into conformance with technical specifications for PIV in order to create a single interoperable platform for physical and logical access across government.[5]

ANATOMY OF A CAC SMART CARD

Source: 7DoD Flyer

Electronic identity credentials in use today most often take the form of a smart card. A smart card is a plastic card usually the size and shape of a common credit card. For the purposes of Defense Common Access Cards, there are three major components: hardware, software, and a credential. Each card includes an embedded processing chip used to store the electronic credentials of the authorized card holder; the chip interfaces with card readers used to read and validate the contained credentials.

The front of the CAC contains such information as Organization Seal, Branch of Service, Color Photograph, Personnel Category, Name, Rank and Pay Grade, Issue Date, Expiration Date, Card Type, Card Identification Information, Hologram, PDF417 Bar Code which contains DoD Electronic Data Interchange Person Identifier, and the Integrated Circuit Chip (ICC). The back of the CAC contains a Magnetic stripe, Code 39 bar code, Date of Birth, Geneva Conventions Category, Blood Type, and Organ Donor Status.[6] In June 2011, as a measure to further protect privacy and personal identity information, the Social Security Number (SSN) was replaced with a DoD ID Number on all ID cards.[7]

CAC employs smart card and PKI technology. These devices provide a secure, tamper-proof, and portable means for storing identity information. Compliance with FIPS 201[8] requires that identity device manufacturers adhere to the specification and must pass certification. FIPS 201 defines the architecture and technical requirements for a PIV and now CAC systems. This is the system that provides the means for verifying the identity of an individual seeking physical access to facilities or electronic access to systems. Merger of the Defense and civilian identification schemes is natural, as the FIPS 201 standard is founded on the success of the Department of Defense and its use of CACs since 1999. [2]

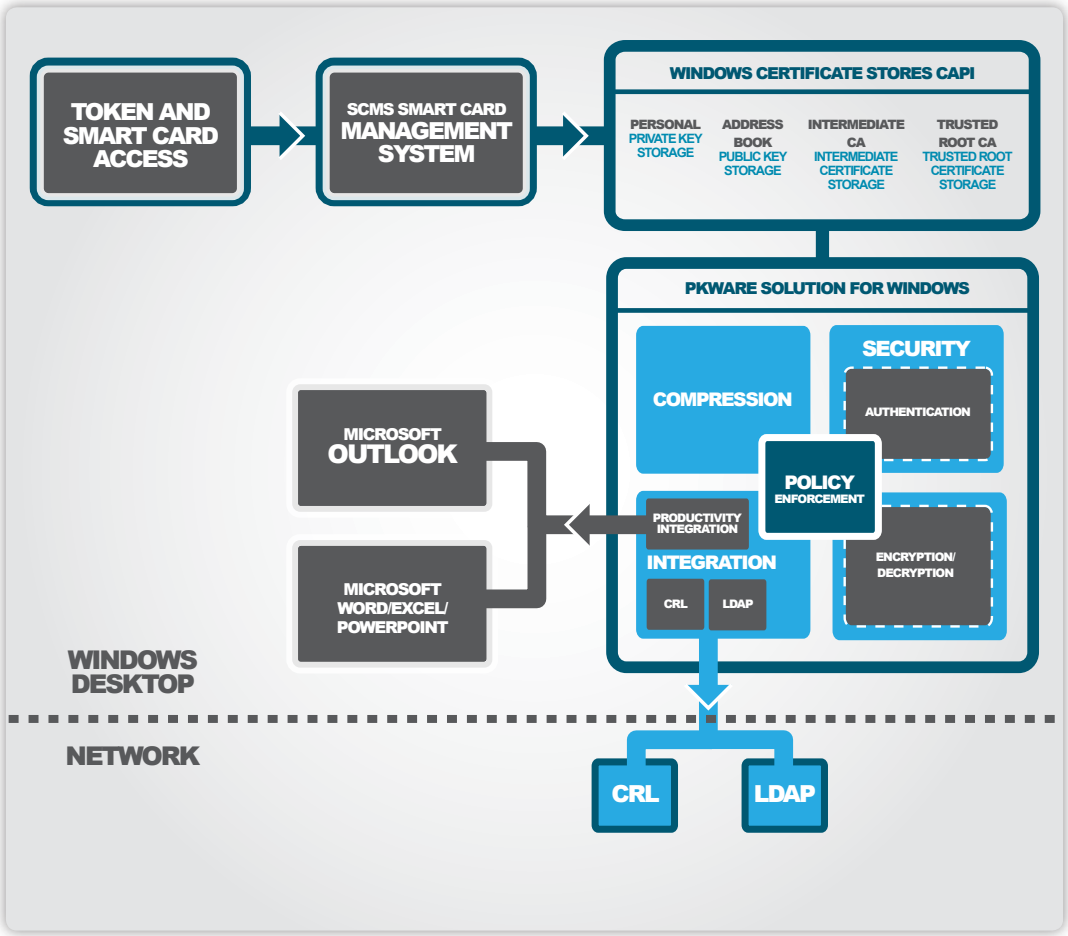
CAC – A SECURE FOUNDATION

Today, CACs, somewhat unlike PIV electronic credentials and smart cards, are for far more than just granting

access to US government facilities and systems. CAC also serves as the primary ID used to gain access to the medical, dental and other services accorded to active duty personnel and their dependents. When the CAC credential is used for facility access, the card owner presents it to a reader integrated into Physical Access Control Systems (PACS).[9] The use of smart cards for access to Department or agencies' technology and networks, controlled by Logical Access Control Systems (LACS) is also growing. In this case, the smart card may be inserted directly into a card reader on the laptop or PC, into a reader on an attached peripheral such as a keyboard, or even a dedicated peripheral smart card reader attached via USB.

When best practices are applied, the user is prompted for a password to grant the smart card reader access to the credential on the smart card. This effectively implements the preferred two-factor authentication, requiring the employee to have something (the smart card) and to know something (the password).

Using a smart card with personal computers requires that software specific to the vendor and architecture of the smart card is installed. This middleware software is called a smart card management system (SCMS) and bridges the proprietary firmware of the smart card integrated chip and the personal computer operating system. This allows applications on the personal computer to locate and recognize the credential. Currently, only the ActiveIdentity ActivClient middleware is approved for Department of Defense use.[11]



For CAC, that credential is a digital certificate and public/private key pair that complies with the X.509 v3 standard. The integrated chip of the smart card contains a certificate unique to the individual identified on the smart card, making the certificate the third element in its anatomy.

Each CAC contains a public and a private key specific to the cardholder. These keys can be used for data and e-mail encryption. Each person to receive a CAC will be issued an identity certificate, an e-mail encryption certificate, and a digital signature certificate to be used by applications that are part of the DoD PKI. Authoritative x.509 credentials are issued using an application and process called a Certificate Authority (CA), described in a following section." The CA is a secure server that signs end-user certificates and publishes Certificate Revocation Lists (CRLs) for certificates that are no longer valid. Directories are secured and trusted repositories of information, usually collected during the registration process.[6]

For a thorough understanding, it is helpful to briefly explore Public Key Infrastructure (PKI), a particularly useful branch of cryptography.

PKI PRIMER

Encryption, the best technology for protecting the privacy and confidentiality of data, uses cryptographic algorithms to convert plain text to unreadable cipher text. The process requires mathematical algorithms and unique encryption keys as additional input to ensure that access is strictly limited while the original plain text remains recoverable. While user created passwords (also known as a symmetric key) may be used for encryption keys – meaning the same password is used for decryption, PKI provides a better alternative.

Public Key Infrastructure (PKI) provides a means to create, manage, distribute, use, store, and revoke digital certificates. Digital certificates bind an identity, including name and associated data such as email address, location, etc., to an electronic public key.[12] Public key cryptography is often referred to as an asymmetric or a two-key system. Each user has a pair of keys – the keys are not the same but match up in a unique way. One key is kept only by the user and is called the private key. The other key is widely distributed and is called the public key. These electronic key pairs provide users with two important capabilities. The first is the ability to digitally sign a document. The second is the ability to encrypt and decrypt messages.[6]

As long as the private key is secure and not shared with others, the public key could be on the most malware-infested server sitting on the most compromised network in the world and the worst anyone could do is encrypt data using that key. Only the holder of the private key could decrypt it. Even the person who encrypted it cannot reverse the process. To decrypt data, the recipient uses the private key that corresponds to the public key. This key never leaves the recipient's possession, residing securely either on a computer or a smart device.

Digital Certificate

The digital certificate verifies the identity of an individual or entity and the key pair is bound to the identity associated with that certificate. For HSPD-12, it proves that the identity of the individual to whom it's assigned has been thoroughly vetted by the processes described for the National Agency Check and Inquiries (NACI).[13] In addition to that testimony, it carries data elements such as the employee's name, an electronic record representing their fingerprint, agency, primary location and the expiration date of the certificate. Digital certificates are issued by a type of software application called a Certificate Authority (CA), supported by the identity verification procedures described by NACI.

Certificate Authority

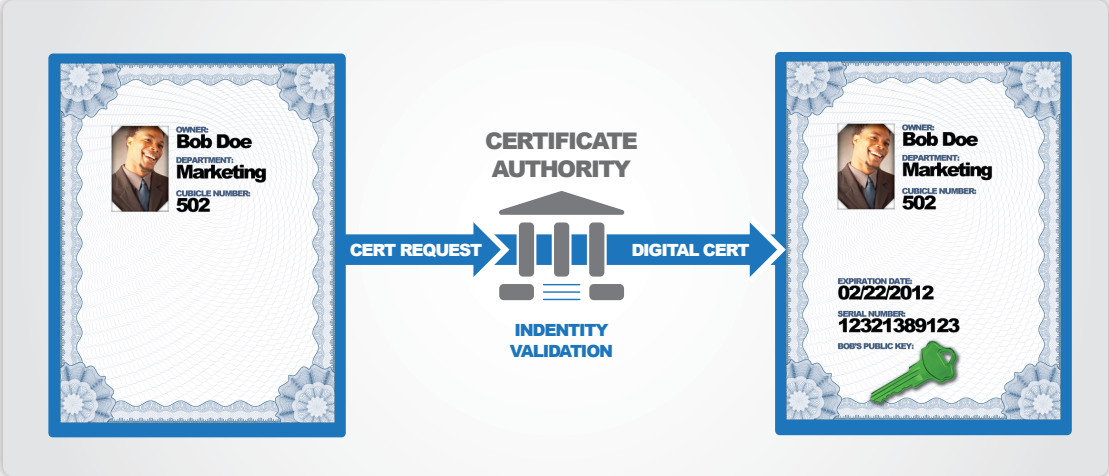
A CA is the application that issues public/private key pairs and binds the identity of an individual (name, email address, and/or other demographic elements) to the public key by means of the certificate. A CA's obligation in such schemes is to verify an applicant's credentials, so that users and relying parties can trust the information in the CA's certificates. CA's use a variety of standards and tests to do so. In essence, the Certificate Authority is responsible for saying "yes, this person is who they say they are, and we, the CA, verify that".

DoD CAs are computer servers that contain and automate the registration process using PKI technology. A certificate is a computer-generated record that ties a user's identification with the user's public key in a trusted bond. This trust is based on a registration process and is automated by the CA. The Secure Sockets Layer (SSL) session encrypts all communications between:

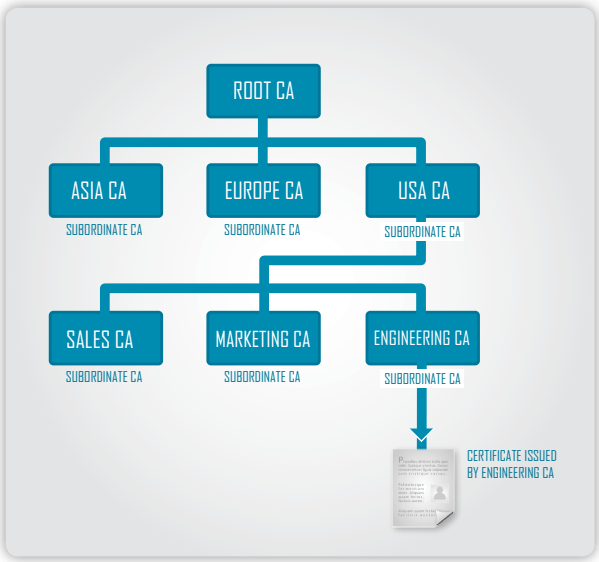
- **Defense Enrollment Eligibility Reporting System (DEERS):** the database that tracks personnel and medical DoD benefits. The DoD operates one of the largest health care systems in the world) and
- **Real-time Automated Personnel Identification System (RAPIDS):** the application software that allows users to communicate with the DEERS database) and the CA.

Public and private keys help ensure that the information transmitted between computers is secure.[6]

If the user trusts the CA and can verify the CA's signature, then he can also verify that a certain public key does indeed belong to whoever is identified in the certificate. CAs may be hosted by an organization internally or third-party organizations may provide CA as a service. These services range from issuing certificates to fully managing the entire PKI infrastructure and identity verification procedures. Providers of CA services include organizations such as VeriSign®, Comodo® and Citigroup® Managed Identity Services.



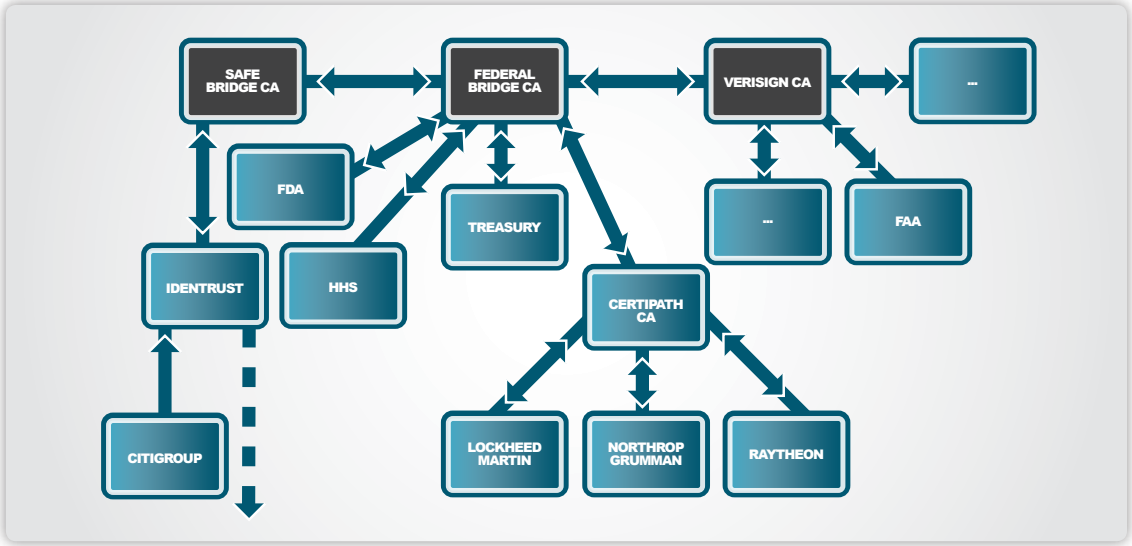
An essential aspect of the digital certificate and CA infrastructure relates to trust. The FIPS 201 standard requires that the digital certificate infrastructure complies with the ITU-T[14] X.509 standard for PKI and digital certificate trust. The trusted CA establishes trust for a certificate. This means that a digital certificate is judged trustworthy based on signatures applied to it by CAs.[15]



Federal Bridge- Cross Certification

Recognizing the diversity of IT infrastructures and needs spanning agencies and departments, the government empowered global root CAs to cross-certify for the purposes of cross-agency identification. This strategy is called Federal Bridge and is managed by the Federal Public Key Infrastructure Policy Authority. The Federal Bridge[16] initiative enables trusted identity authentication across federal agencies and between federal agencies and third parties.

Several public and private sector authorities have "cross-certified" and as a result: an agency that uses their own Certificate Authority with its implicit chain-of-trust is authorized and can easily accept and trust a digital certificate issued by a different Certificate Authority with a different chain-of-trust to grant federal employees and contractors access to facilities and systems. While some Defense contractors have cross-certified, Defense cross-certification remains under review as of the time of this writing.



EXPANDING THE USE AND BENEFITS OF CAC SMART CARDS

The baseline functionality of the CAC is to (1) provide for logical access to computer systems, (2) provide personnel identification, (3) enable physical access to buildings, and (4) PKI for signing, encryption, and non-repudiation. Furthermore, the CAC is intended as a multi-application smart card. It serves as a token for PKI identity, email, and encryption certificates utilizing a linear barcode, two-dimensional barcode, magnetic stripe, color digital photograph, and printed text.[10]

Beyond the government's primary goal of enhanced identification methods and management for secure access to facilities and systems, the credentials on CAC smart cards can be applied to other Department needs. The digital certificates and key pairs that compose the credential can be used for agency data protection and data authentication processing. The CAC program is expected to evolve and work seamlessly with PIV civilian initiatives, making the benefits of a single, government-wide identification program a reality:

- **Provide interoperability across multiple jurisdictions** - Reduce redundant credentialing efforts and expenditures, allow one ID to be issued (rather than multiple IDs), and increase policy effectiveness
- **Provide trust across multiple jurisdictions** - implement a standardized identity proofing process and standardized issuance procedures.
- **Provide strong proof of cardholder identity** - maintain and protect data from accidental or deliberate loss, alteration, or destruction. Data accuracy is enhanced through processes that prevent, detect, and correct errors.
- **Provide the ability to authenticate identity and attributes electronically** - Electronic authentication enhances data security, physical security, and personal privacy while allowing for secure physical and logical access. It also protects against identity theft and reduces the incidence of fraudulent benefit, entitlement, or service payments to individuals who misrepresent themselves.
- **Improve ROI for identity credentialing programs** - The ability to leverage a common identity infrastructure and technology across multiple credentialing programs can improve return on investment. In addition, the GSA co-op purchasing program is available to state and local governments so that they can acquire products through a GSA purchasing vehicle.[17]

Anticipated activities will likely proliferate as Defense also seeks to reduce costs through IT infrastructure virtualization, including utilization of private and public clouds. Although real benefits of cost control are relevant, the scenarios inherently increase the risk to taxpayer, military personnel and Defense sensitive data—therefore requiring additional data protection and data authentication procedures to ensure privacy. With proper attention and safeguards, data security is possible across platforms, across the extended enterprise and into virtual and cloud environments.

Improving Data Privacy Protection using Smart Card Credentials

Protecting the privacy of Defense personnel personally identifiable information (PII) is a priority across the Department. Defense manages volumes of sensitive information related to uniformed personnel and their dependents, and protection of this information is paramount both for the protection of the individuals and for the well being of the armed forces as a whole. Clearly, sensitive information detailing the health of ranking officers or the family status of combatants in the field must be held closely and protected from view by unauthorized individuals. The scope of this challenge only increases as data centers are consolidated and more workloads migrated into virtualized environments.

Pete Lindstrom, former senior analyst at Burton Group, once posted that there are Five Immutable Laws of Virtualization Security,[18] one of which states that "A VM has higher risk than its counterpart physical system that is running the exact same OS and applications and is configured identically." In other words, explains Lindstrom, "The risk is additive even though its footprint is typically small. Of course, even that footprint is changing as more and more functionality is introduced into the hypervisor that manages the VMs."

According to Gartner research, as more workloads are virtualized, as workloads of different trust levels are combined and as virtualized workloads become more mobile, the security issues associated with virtualization become more critical to address. Above all, Gartner advises, organizations should not rely on host-based security controls to detect a compromise or protect anything running below it.[19]

When management of virtualization is transferred to an external provider of cloud computing, the agency yields direct control of the infrastructure and the ability to protect data within in it. For legacy, contemporary, and emerging infrastructures, encryption remains one of the best means to protect data privacy.

Cryptographic algorithms, as previously mentioned, convert plain text to cipher text, requiring keys as additional input to ensure that access is strictly limited while the original plain text remains recoverable. Strong encryption, compliant with NIST's FIPS 140-2 standard, protects data privacy to a degree that prevents lawbreakers from accessing data as long as the key used to encrypt the data is sufficiently long and complex.

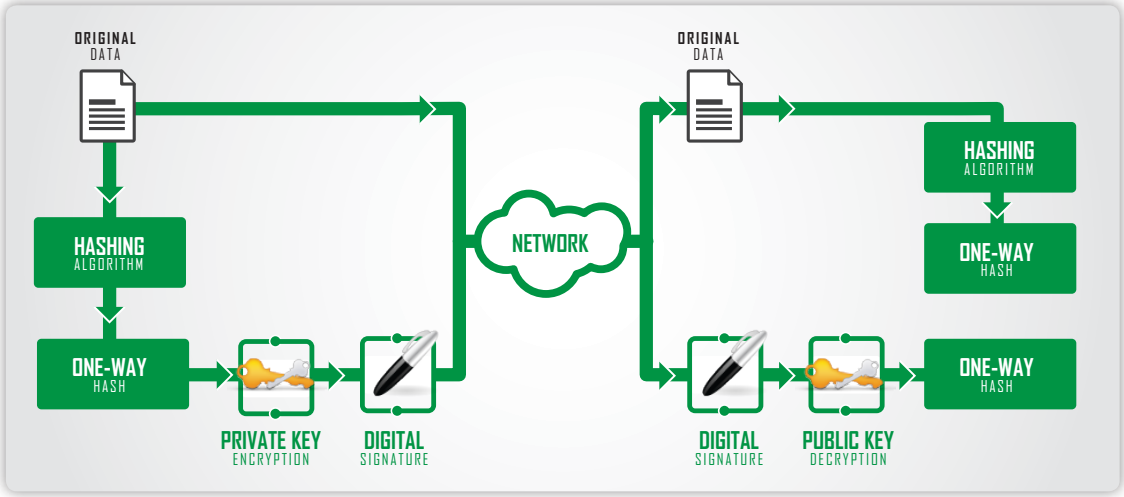
The public keys included with CAC credentials fit that definition of "long and complex", and are perfectly suited to that purpose. If the public key used is paired with a private key held on an HSPD-12 smart card, a user (i.e., Alice) would need to make the smart card and credential available to the computer before she could decrypt and read the clear text.

In Practice

For federal agencies, this has particular elegance in that employee and contractor public keys can be added to their network directory entries and automatically located via Lightweight Directory Access Protocol (LDAP) integration. These directories are hosted by the CA service providers, such as VeriSign, where any public keys issued are hosted and made easily available for others to use. It is a superior level of data protection because it implements two-factor authentication requiring the person decrypting data to present something they have (the smart card) and something they know (the password) before allowing access to the credential on the smart card.

Validating Integrity of Stored Data Using Smart Card Credentials

CAC credentials can also be used to ensure the integrity of transmitted, transported, and stored data using a different cryptographic operation. The importance of authenticating the integrity of data has increased exponentially with the increased connectivity within and between organizations. For example, each time an email is sent across the Internet, it is subject to man-in-the-middle attack, wherein it is intercepted and a fraudulent modification or replacement is substituted in its place. Similar risks apply when data is stored outside an agency's direct and constant control, such as in cloud storage, or when data is written to media and transported by third parties.



In Practice

Digitally signing the data, before sending or storing, mitigates the risk of man-in-the-middle attacks. Mechanically, digital signing takes the variable length document or data file as input, and then processes it with a one-way hashing algorithm[20] to create a fixed length output, sometimes called the input's digest.[21] The digest is then encrypted with a user's private key, creating a digital signature unique to the input and the user. That digital signature is then attached to the original clear text file. The data can then be sent or stored with confidence that any substitution or tampering with the data can be immediately identified. For example, the input document is again hashed using the same hashing algorithm to create a second digest. If the two digests do not match, the source data should be treated as suspect and potentially fraudulent.

DATA PROTECTION

Although many agencies have one or more data protection technologies in place, constant vigilance and multiple approaches are required to effectively protect PII across constituents. Understanding that the pressure is on to avoid duplication or unnecessary expenses, this section explores the advantages of file-based encryption in context of other popular encryption procedures.

Disk Encryption

Disk encryption focuses on the need to protect data on personal computers, laptops, tablets and handheld devices that are lost or stolen. Equally, it may be used to protect data on drives that are fraudulently removed from servers. Disk encryption ensures that the privacy of all data contained within the perimeter of the inactive device is strongly protected. However,

- Disk encryption does not address protection when the system is turned on and the user is logged in (it only protects data when the user is logged out of the operating system or the system is turned off), Therefore if an agency employee logs into their laptop in a public space and leaves the computer, a criminal might gain access to the sensitive data contained.
- Disk encryption does not extend any protection to data that moves beyond its perimeter. It does not protect documents attached to emails, files that are moved or copied to network servers, or otherwise transmitted.

File-based Encryption Advantage

In contrast, file-based encryption remains with the data at all times, protecting it even when the user is logged into the system and even when the file is sent, copied or otherwise transmitted. This data-centric protection remains in place until the holder of the appropriate key decrypts the data. File-based encryption is a useful complement to disk encryption.

Communication Transport Protocol Encryption

Communication line encryption protects data from the perimeter of the sending organization to the perimeter of the receiving organization. It also provides some protection against man-in-the-middle attacks, especially those that only seek to read or copy transmitted data rather than alter. It protects transmitted data, but only within the perimeter of the transmission connection.

File Based Encryption Advantage

In contrast, file-based encryption protects data before it is transmitted, during transmission, and after receipt. Data is not subject to risk if a receiving transmission server is compromised or an unauthorized transmission administrator seeks access. Without increased risk, data can be transmitted using the lowest-cost

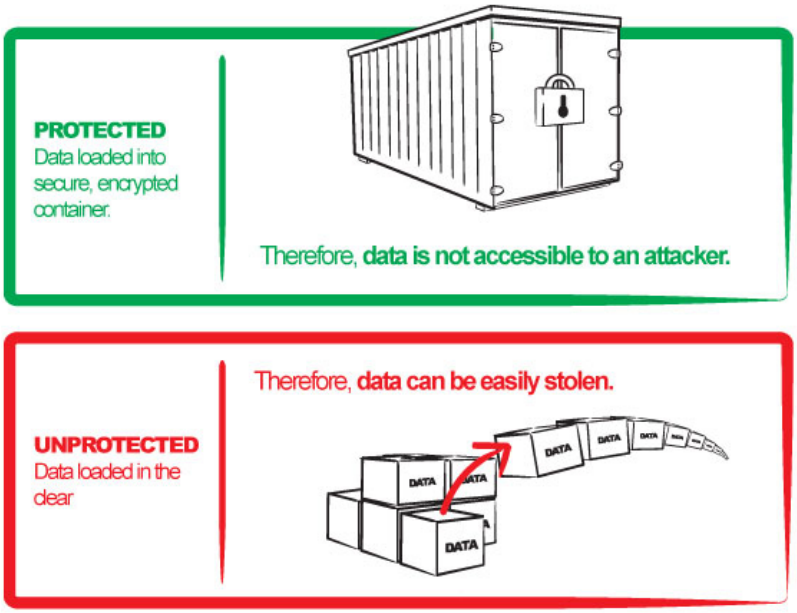
communication link (such as the Internet) instead of more expensive dedicated lines or encrypting managed file transfer (MFT) applications. File-based encryption can complement or become a complete substitute for communication transport protocol encryption.

Database Encryption

Database encryption applies protection to specific columns in specific tables of relational databases, adding a layer of protection to data-in-use. This is useful for high volume transaction databases that include discretely identifiable PII such as SSNs, credit card or debit card numbers, health status, and other protected information. It allows for the majority of the data included in records to remain unencrypted for processing, while protecting the fields deemed sensitive. However, it only protects data that remains within the database and is not practically transferrable once the data is extracted. For example, a federal agency that manages large databases of taxpayer health status information might be required to extract subsets of that data to help research hospitals and universities improve the nation's healthcare. While PHI elements might be protected by database column encryption within the database, it must be removed before transmitting the data for that data to be usable by the recipient.

File Based Encryption Advantage

In contrast, file-based encryption specifically protects extracts and backups from relational databases, with techniques that allow easy exchange with others outside the perimeter of the database. File-based encryption can be applied to extracts from that database, using the encryption key appropriate for the intended recipient. That encryption protects the data outside the perimeter of the database, while it is being sent to the intended recipient, and can be easily decrypted by the recipient using technologies appropriate for the computing platform they use.



Data-Centric Protection

Data-centric protection through encryption renders the data unusable to anyone that does not have the key to decrypt it. No matter whether the data is in motion or at rest, it remains protected. The owner of the decryption keys maintains the security of that data and can decide who and what to allow access to the data. Encryption procedures can be integrated into the existing workflow for cloud services. For example, an admin could encrypt all backup data before sending into the storage cloud.

Source: How Data-Centric Protection Increases Security in Cloud Computing and Virtualization-- Diana Kelley, SecurityCurve

CONCLUSION

The Department of Defense CAC program is a necessary and mandated program with which the armed forces and their supporting agencies and contractors must comply. The PACS and LACS, when implemented, materially mitigate the risks of terrorist attack on Defense facilities and systems, increasing the protection for all uniformed

personnel and US citizens. Moreover, it reduces the barriers for inter-agency cooperation and contributes to accelerated response to emergencies when they occur.

Defense branches and their supporting agencies will gain more out of their investments in the technology CAC by applying it to other data protection needs. The PKI foundation of the CAC credentials offers public/private keys and digital certificates that can be applied to both file encryption and file integrity authentication. The importance of data-centric, file-based, encryption becomes more critical and compelling as new virtualization and cloud computing technologies are considered.

PKWARE guarantees protection with persistent file-level security independent of system, application or data format, and at rest or in motion. The PKWARE Solution renders data unusable to anyone that does not have the key to decrypt it and ensures data integrity even when lost or stolen.

Notes

1 http://www.cac.mil/common-access-card/
Defense Human Resource Activity (DHRA) is a DoD Field Activity established under the authority, direction, and control of the Under Secretary of Defense (Personnel and Readiness) (USD (P&R)). The DHRA mission is to enhance the operational effectiveness and efficiency of diverse programs supporting the Department of Defense.

2 Common Access Card continues to pave the way By Zack Martin, Editor, AVISIAN Publications http://www.envoydata.com/content/common-access-card-continues-pave-way

3 Source: The Defense Department's Defense Manpower Data Center and Federal News Radio
(Copyright 2011 by FederalNewsRadio.com. All Rights Reserved.)

4 M-11-11 February 3, 2011: MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES FROM: Jacob J. Lew Director SUBJECT: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors

5 Government Computer News, Why government is still waiting for 'PKI-at-the-door', By William Jackson, Feb 29, 2012 http://gcn.com/articles/2012/02/29/rsa-9-physical-logical-access-pki-at-door.aspx?sc_lang=en

6 Common Access Card/Public Key Infrastructure Training guide, http://www.idmanagement.gov/iab/documents/CACpkiTrainingGuide.pdf

7 DoD Flyer http://milret.daveylee.net/DoD_Flyer_v4.pdf

8 National Institutes of Standards and Technology (NIST) specification smart card technology applied to civilian agency personnel identification credentials: http://csrc.nist.gov/publications/drafts/fips201-2/Draft_NIST-FIPS-201-2.pdf. See foot note 6 for the specific Defense directive

9 Note: in some cases, facility access readers may be contactless, requiring that the federal employee or contractor only pass the smart card in front of the reader

10 DoD Implementation Guide for CAC Next Generation (NG) Version 2.6; November 2006 http://www.idmanagement.gov/iab/documents/CACngImplementationGuide.pdf

11. http://en.wikipedia.org/wiki/Common_Access_Card

12 The unique relationship of public/private key pairs is based on a thoroughly researched branch of mathematics focused on prime numbers. In simple terms, it is very easy to derive the product of two prime numbers, but it is difficult beyond the capabilities of even contemporary supercomputers or massively parallel processing systems to derive the two prime numbers only from their multiplied product. Please see http://www.livinginternet.com/i/is_crypt_pkc_ work.htm for an excellent, more detailed discussion.

13 'A National Agency Check and Inquiries (NACI) is the minimum level of investigation required of Federal employees as a condition to employment with the Federal government and now for contract employees as a condition to access to Federal facilities and information systems. It is essentially a check of law enforcement records, and written inquiries to schools, police departments, and other references to verify your status. … HSPD-12 and FIPS 201 expanded the persons and positions that require such investigations.', downloaded from http://hspd12.nasa.gov/faqs/index.html on April 5, 2011

14 International Telecommunication Union Telecommunication Standardization Sector

15 Chain-of-trust is a typical best practice for PKI implementations and required to conform to the FIPS 201 standard. However, other situations, particularly in the commercial sector, may be better served by a closed system, sometimes referred to as a "self-signed" PKI. For more information on this approach, please contact your PKWARE representative.

16 http://www.idmanagement.gov/fpkipa/

17 Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers: Trusted Identities for Citizens across States, Counties, Cities and Businesses. A Smart Card Alliance Physical Access Council and Identity Council White Paper http://www.securitysales.com/files/PIV-I-White-Paper-012811.pdf

18 Burton Group SRMS Blog, January 08, 2008, "Five Immutable Laws of Virtualization Security," by Pete Lindstrom, http://srmsblog.burtongroup.com/2008/01/five-immutable.html

19 Gartner.com Press Release: Gartner Says 60 Percent of Virtualized Servers Will Be Less Secure Than the Physical Servers They Replace Through 2012 http://www.gartner.com/it/page.jsp?id=1322414

20 Sometimes also known as a 'cryptographic hash function,' this is a mathematical procedure that converts an input of any length into an output of a fixed, shorter length (hash value), doing so such that any change, accidental or intentional, to the original source data results in a different calculated hash value outcome. Currently, SHA-1 hash functions are allowed, with the stipulation that SHA-2, the more sophisticated successor function, be adopted by the end of 2013.

21 The one-way nature of the hashing algorithm guarantees that there is no means to reverse engineer the original variable length clear text data of the input from the fixed length output digest, an additional layer of protection.