

SOFTWARE ENCRYPTION IN THE DOD

Al Kondi
PMO RCAS
8510 Cinder Bed Road, Suite 1000
Newington, VA 22122-8510

Russ Davis
Boeing IS
MS CV-84
Vienna, VA 22182-3999

Preface

This paper represents the views of the authors and not necessarily those of their employers. Risk analysis is the preferred method used in identifying cost effective security controls. Factors in the analysis include threat assessments and cost. Other risk analysis findings follow. For example, in his 1997 budget, President Clinton called for a 3.4% decrease in Defense spending [1]. At the same time, the Director, National Security Agency (NSA) warned of a fundamental new danger from cyber attacks [2]. Additionally, computer power, available for cracking encryption, is doubling every few years. One can for example purchase a computer capable of one trillion calculations per second [3].

Department of Defense (DoD) Environment

Within the DoD community there exists a myriad of heterogeneous encryption systems. These are predominately based on hardware devices. For the classified environment, NSA type 1 approved devices are used for encryption. For strictly unclassified information, either the Data Encryption Standard (DES) or the NSA type 2 devices (including the Fortezza card) are used for confidentiality protection. Approval to use the SKIPJACK algorithm for sensitive but unclassified (SBU) information is provided by the Escrow Encryption Standard (EES). The SKIPJACK algorithm is implemented in a PC Card device known as Fortezza and is expected to allow software and smart card implementations. Additionally, it is anticipated that the Advanced Encryption Standard (AES) will eventually replace the SKIPJACK algorithm and will be used to encrypt classified information.

The Data Encryption Standard

When Federal Standard 1027 was still applicable, hardware encryption devices were mandatory for DES implementations. The Federal Standard has been replaced by the Federal Information Processing Standard (FIPS) Publication 140-1 [4] and software encryption is now allowed for Government use. The DES has been the algorithm of choice for unclassified sensitive data, especially for data confidentiality protection of network traffic. The banking community currently uses DES Message Authentication Codes (MAC) for ensuring the integrity

of wire transfers. On any given day, billions of dollars worth of wire transfers are protected with MAC authentication.

The current DES standard [5] allows the algorithm to be implemented in software. The DES algorithm uses a 56 bit key resulting in slightly more than 70 quadrillion, or 70 thousand million million (2^{56}) possible keys. While this is an impressive number, commercial-off-the-shelf (COTS) workstations are increasing in performance at an exponential rate. For example, the desktop machines today are approximately 100 times more powerful than those of 10 years ago. Typical machines today operate in excess of 100 million instructions per second (MIPS).

Advanced Encryption Standard

With the evolving risk to 56-bit keys, the National Institute of Standards and Technology (NIST) has embarked on the DES replacement (the AES). On 2 January 1997, the NIST announced in the Federal Register, the development of a FIPS for Advanced Encryption Standard. There are several requirements including that the algorithm be implementable in hardware and software. For sensitive but unclassified systems, the AES will be the standard algorithm used. Based on the first AES workshop held at the NIST, the AES will not interoperate with the DES, thereby making the existing systems isolated. Moreover, the AES will use at least 128 bit keys, which will make the SKIPJACK algorithm obsolete. The AES will be the standard algorithm that replaces the DES within the Federal Government. Additionally, the National Security Agency (NSA) has indicated that the AES will eventually replace the SKIPJACK algorithm for both classified and unclassified encryption.

The length of the encryption keys results in exponential key space. That is, the number of different keys is 2^n , where n is the number of bits in the key. By increasing the key length by one bit, the possible number of different keys doubles. Therefore, it is important to select a sufficiently long key to protect investments over the years to come.

Another way to look at the risk from advanced computers is that every time processing power doubles, one bit is effectively removed from the key length. Thus, 24 doubling periods will reduce the 80-bit SKIPJACK key, used in Fortezza PC cards, to that of today's 56-bit DES. For example, if the doubling period for computer processing is 3 years, this becomes 72 years before SKIPJACK is no better than today's DES.

It is not enough to examine only the processing power but also the number of computers available to the attacker. If the attacker has 1024 machines from a corporation during off hours, then 10-bits are effectively removed from the overall key length. Software encryption provides a cost effect method for replacing encryption algorithms as they become vulnerable to exhaustive search attacks.

The Defense Message System (DMS)

Recently, the NSA has championed a Personal Computer Memory Card International Association (PCMCIA) compliant encryption device, called the Fortezza PC Card. These devices are inserted into a PCMCIA reader located on the computer workstation and were

originally designed for use in the DMS. When used with a trusted operating system, these provide excellent security. However, the Fortezza is also being used on untrusted operating system environments including DOS and Windows for Workgroups machines. The risk in using untrusted operating systems has long been known. For example, The US Air Force's Electronic Systems Division documented the following in 1973 [6]: *"If an error in an operating system program allows a penetration program to work, that program will work every time it is executed – typically retrieving without detection any information accessible to the computer."*

Another example of hardware under the operating system's control is evident from the National Computer Security Center (NCSC) evaluation of Sentinel [7]: *"The security mechanisms can be maintained only if both the operating system in which Sentinel runs, and Sentinel's operational files are protected from unauthorized modification. Since Sentinel's protection mechanisms are implemented in single-state machine hardware, it becomes essential that user/system separation be maintained. In systems with this type of architecture, non-privileged users operate in the same memory space as the security-related system functions; hence it would be possible for an experienced user to modify the operating system and circumvent the security mechanisms without the likelihood of detection."*

The Fortezza card is a hardware crypto implementation running on software. What this boils down to is that Fortezza is only as good as the software it runs on. If you must trust the software to properly operate the hardware device, why then would it not be trusted to perform encryption for unclassified but sensitive applications? Representative from the NSA have indicated that the X509 version 3 certificates will be used for key distribution. The certificate will contain information differentiating hardware from software generated certificates. Given the software trust argument presented above, it is unclear why the level of trust of the operating system used will not be identified in their certificates.

The DMS Fortezza cards implement the Digital Signature Algorithm (DSA), the Secure Hash Algorithm (SHA), the SKIPJACK encryption algorithm [8], a random number generator, and a keys exchange function. These devices are also being used in conjunction with Fortezza enabled Netscape Web products to enable an encrypted session. The session uses the Secure Sockets Layer (SSL), a protocol that provides key exchange and packet encryption. The routing information is left in the clear with the packet contents encrypted. It is anticipated that the Fortezza technology will interoperate with the proposed software solution discussed in this section by using common encryption protocols.

The Fortezza PC card is part of the multilevel information system security initiative (MISSI). Many of the legacy systems do not have PCMCIA compliant readers which are required to use Fortezza. Many of the legacy systems either cannot support encryption or there is a lack of funds to buy the encryptors. For these systems, encryption is normally waived. Software encryption provides an attractive alternative to the normal practice of waiving the requirement for encryption.

Hardware Encryption

Hardware obtains its strength from being rigid and hard to change. Some have argued that hardware is faster and easy to install [9]. However, this argument does not address affordability. Additionally, today's workstations can encrypt faster than a 10 megabit per second

Ethernet can ingest. When dealing with encryption devices, it is questionable how this would be easier to install, use and maintain software. Some large systems, are designed to use hardware DES encryption devices for encrypting wide area traffic. However, the DES will be replaced by the AES. All existing DES hardware will eventually be replaced with devices using the new AES algorithm.

Typically, hardware encryptors are separate devices that contain a cryptographic engine, possibly consisting of a microprocessor. However, a separate device does not imply a secure solution. Although DES devices made by the same company work with their product line, many do not properly communicate with other vendor's products. Given the same key, mode of operation, and initialization vector, all DES products should work across vendor products. Unfortunately, when one purchases a DES hardware device, he or she is stuck with the single vendor product line from then on. If a flawed hardware implementation of DES is discovered, the correction costs are excessively high when compared to software.

Software Alternatives

Some have argued that for system security, communications security (COMSEC) and computer security (COMPUSEC) must be combined [10]. By performing the COMSEC functions in software, for sensitive but unclassified (SBU) communications, the system security goal is satisfied. If software encryption is utilized, it is important to have assurances that the software environment can be trusted. As Thompson [11] points out, you can't trust untrusted software.

For example, a large system might include Microsoft Exchange, as its current mail solution. Starting with Exchange version 5.0, X.500 directory functionality is included. Any client application that is lightweight directory access protocol (LDAP) compliant can access the directory. The directory is a logical storage location for X.509 version 3 certificates.

The NIST standard for crypto modules [12] should be used by the DoD when selecting encryption products for unclassified information. This standard allows encryption to be performed in software. A C2 NT Operating System could be used to achieve Level 2 Security as defined in FIPS 140-1.

Digital Signatures

Digital signatures are created using a public-key signature algorithm such as the RSA public-key cipher or the digital signature algorithm. A public-key algorithm uses two different keys (a public key and a private key). The private key is available only to its owner, while the public key is made available to all. In digital signatures, the private key is used to generate the signature, and the public key is used to validate the signature.

For example, the RSA digital signature is a one-way hash of a document, file, or object that is encrypted using the private key of the sender. The encrypted hash is decrypted using the public key and is compared with the calculated hash of the object. Equal hash values indicate a legitimate object.

Public Key Infrastructure (PKI)

The challenge is how to distribute the user's public keys. Work has been done on how certificates are generated, stored, and retrieved. There are vendor products which perform the Certificate Authority (CA) functionality. That is, to generate a certificates based on requests. Once generated, X.509 version 3 certificates must be placed in a repository. LDAP compliant clients can then retrieve certificates as they are needed.

On 31 December 1996, Assistant Secretary of Defense, Emmett Paige, Jr. released a memorandum describing signature implementation for the Defense Travel System (DTS). The memorandum addresses public key infrastructure devices, including software. The following is taken from the memorandum: *Applications that support software based digital signature keys must be interoperable with other Public Key Infrastructure (PKI) devices (hardware and software), such as the Components being fielded by the Defense Messaging System.*

From a Federal Government point of view, the PKI needs to support interoperability between Federal agencies. It appears the direction at the Federal level supports a COTS implementation. To raise a flag here, it appears that DMS, as currently designed, is moving in a direction that will partition it from the Federal PKI.

DoD Standards

Both the Joint Technical Architecture (JTA) and the Army Technical Architecture (ATA) describe Internet Protocol (IP) version 6 (IPv6). IP Security (IPSec) is mandatory for IPv6 implementations. Given that IPv6 will be dominated by commercial off the shelf (COTS) software products, many in the DoD community will have a software encryption capability at their disposal. The military messaging networks make up only about 1% of the world's cryptography [13]. It is clear that private industry will have a significant impact on the direction in which cryptographic is implemented.

A Large System Example

Figure 1 illustrates the large site environment. Note there are hardware encryptors located at the Frame Relay and dial-up locations. These devices operate only with the same vendor's products. That is, the system users are dependent on the vendor in that there will be no interoperability with different vendor products. In the absence of some hardware standard, launching a hardware solution for encryption leads to isolation.

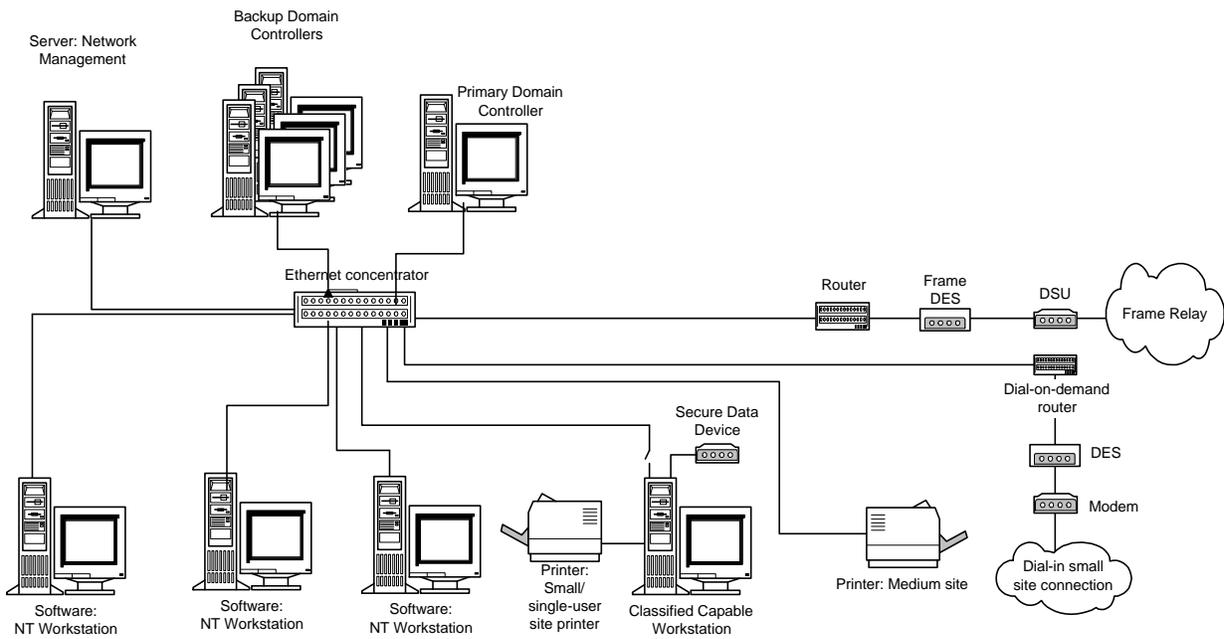


Figure 1 Large Site

The above design provides DES hardware encryption for all wide area network (WAN) communications. Figure 2 illustrates two local area network (LAN) segments securely communicating over a WAN. The traffic on either side of the gateway is not encrypted. In this figure, protection is network facing, leaving internal communications in the clear.

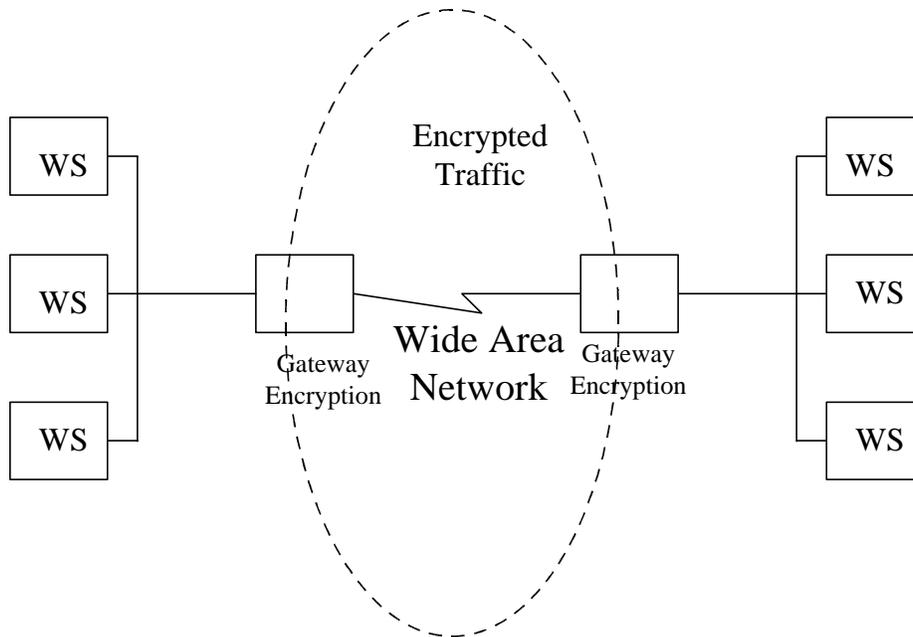


Figure 2 Wide Area Network Encryption

The above is a simplified drawing of Figure 1. What is apparent is that the security occurs at the gateways leaving the LANs vulnerable to sniffers.

Within the system example, workstations and servers use the NT operating system. The Windows NT operating system was evaluated by the NCSC who determined that in a standalone mode, Windows NT satisfied the C2 level of trust. The final evaluation report dated 1 March 1995, also indicated that Windows NT satisfied the requirements for a B2 trusted path. What that means is the user is authenticated to the operating system. This is critical when using tokens such as Fortezza.

Starting with NT version 4.0, the operating system includes a Cryptographic Application Programming Interface (CAPI). It appears that Microsoft will not initially include all the cryptographic module(s) used by the Government as they expect third party vendors to fill this gap. Encryption (and decryption) would be performed at the operating system level. Currently, Microsoft is providing network encryption but not IPsec. In the future, Microsoft will likely provide a complete solution.

Windows NT

The above system example consists of Microsoft Windows NT version 4.0 workstations and servers. It will include newer versions of software and more powerful hardware as they become available. The Windows NT products contain features used to ingest X.509 version 3 certificates and cache them locally. The certificate cache reduces the telecommunications required when compared with implementations that require a certificate to be retrieved each time it is needed. The certificate server provides an automated method for certificate issuance. Starting with Windows NT version 5.0, many of the directory services found only in Microsoft Exchange will be included within the NT operating system.

Microsoft Exchange

Within the system example, Microsoft Exchange version 5.0 is used as the mail solution. The latest Microsoft Exchange Server includes an X.500 directory. It supports any LDAP client and provides SSL for Network News Transport Protocol (NNTP), Post Office Protocol (POP) mail, Web, and LDAP. The SSL protocol is an application to application protocol that includes a compression option (version 3 of the SSL protocol). Turning on the existing feature, a digital signature can be affixed to each email message. The LDAP protocol is specified in the draft NIST Minimum Interoperability Specification for PKI Components (MISPC).

Microsoft Exchange version 5.0 is not completely compatible with the DMS. The capability must be purchased separately off the DMS contract. It is expected that the next version of the Microsoft Exchange, when used with the Fortezza Cryptographic Service Provider (CSP), will provide all requisite DMS functionality and include the Directory Access Protocol (DAP). By using the Fortezza CSP, the Fortezza cards can be used for a multitude of non-DMS uses. The NSA has indicated that the Certification Authority Workstation (CAW) will support LDAP.

A single server in the Microsoft Exchange enterprise when designated as the key management server and holds the public and private key information for the users. Encryption of the message is selected at the client station, and privilege is authenticated by the designated server. A user of Microsoft Exchange may encrypt only, sign only, and encrypt/sign a message.

Virtual Private Networks

A virtual private network (VPN) encapsulates and encrypts data within IP packets. There are two popular VPN approaches described in this section. The first is the Point-to-point tunneling protocol (PPTP) which is included within Microsoft Windows NT and Exchange. The second approach is using IPSec. There are many commercial products that implement IPSec.

Microsoft Certificate Server

The Microsoft certificate Server version 1.0 will be bundled with the Microsoft Internet Information server version 4.0. It performs the same certificate generation functionality of the CAW found in the DMS environment. One Certificate Server should support a WAN with a large number of users at a number of site locations. The NIST has expressed their intent to include additional algorithms into future Government standards. The intent was published in the Federal Register. The NIST expects to include RSA and Diffie-Hellman algorithms in their standards. These algorithms are currently bundled with Microsoft and other COTS products.

User-to-user Approach

The simplified diagram below, workstations use the NT operating system. The NT operating system includes complete C2 security functionality. Cryptographic algorithms implemented in a C2 operating system can achieve a Level 2 rating as defined within FIPS Pub 140-1. This level is comparable to many of the available hardware products. Many of the existing hardware products are still to be tested in a NIST approved voluntary lab. The Figure below illustrates how the software encryption would actually enhance the security of the system example. In this environment, the encryption occurs at each workstation. All sensitive LAN traffic is encrypted. The software encryption protects sensitive information from sniffer attacks.

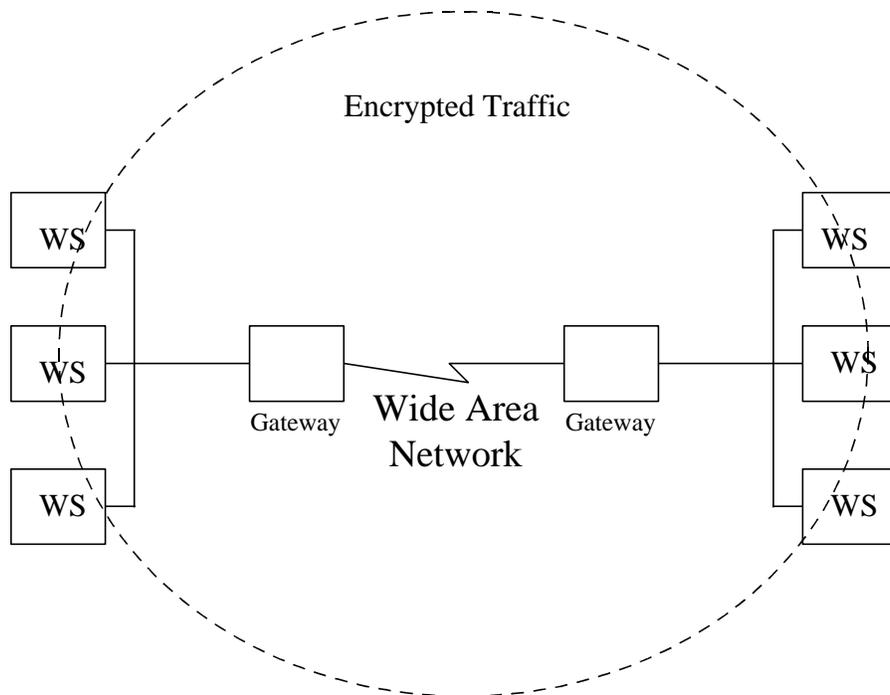


Figure 3 Software Approach

Starting with Microsoft NT version 4.0, the operating system includes a CAPI. When combined with the Microsoft Service Pack 3 for Windows NT 4.0, the CAPI includes DES and triple DES encryption algorithms.

Legacy Systems

There exist a number of legacy applications that currently do not use encryption. The information being passed across untrusted networks includes proprietary, resource, acquisition, medical, personal, and Privacy Act information that requires protection. In legacy systems, due to the cost of hardware implementation of the DES, encryption was waived. When hardware has been implemented, considering the dynamics of evolving encryption standards such as the AES, any move in a legacy system to encrypt using hardware encryption will only require replacement or reprogramming. If legacy systems are to move to the National will, software implementations of cryptography are far more cost effective and are easier to upgrade .

Public Key Infrastructure Pilot

It is expected that the Department of the Army (DA) will fund a proof of concept PKI. The pilot will use certificate servers to generate certificates and revocation lists. The certificate server will send the certificates to Microsoft exchange servers using LDAP. Once Windows NT 5.0 is expected to have a distributed directory scheme that will accommodate certificates. One goal of the pilot is to have interoperability amongst the Federal government. The Federal PKI

will most likely consist of a top down architecture as shown in Figure 4. The PKI will be based on COTS products.

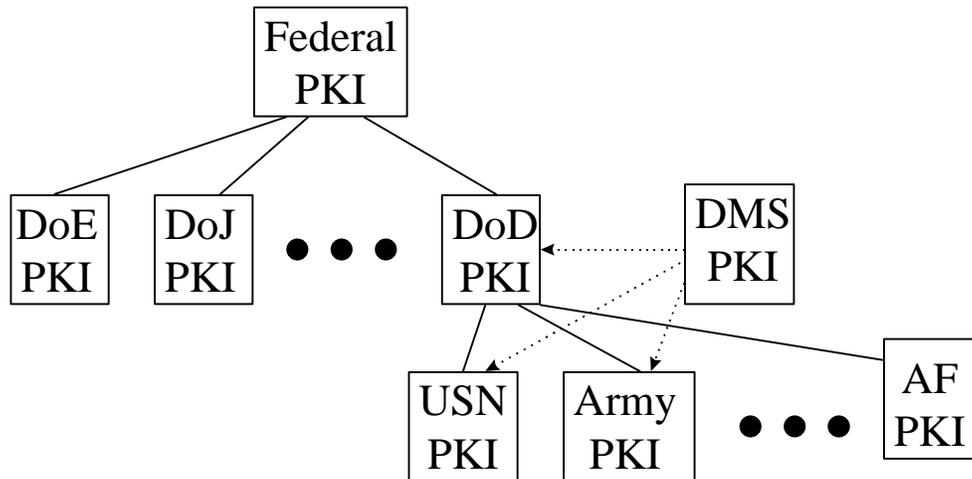


Figure 4 Federal PKI

The pilot will attempt interoperability with the DMS infrastructure. This will be accomplished using either the DAP or LDAP to populate the exchange servers. Once certificates are resident in exchange, users should be able to retrieve them using either DAP or LDAP. The current version of exchange (version 5.0) does not support DAP. It is expected that the next version of exchange will include DAP support. Additionally, the NSA has indicated they will support the LDAP protocol thereby making the DAP issue inconsequential. Figure 5 provides a snapshot of the pilot objective architecture.

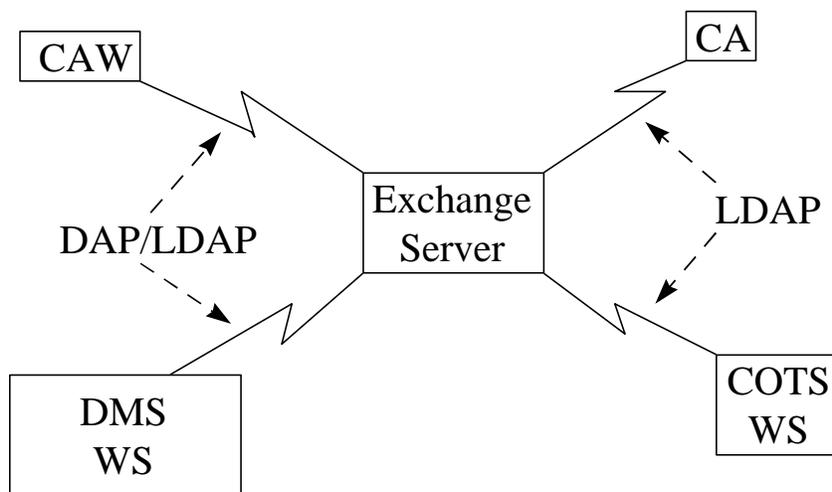


Figure 6 DMS PKI Objective

Summary

In scarce resource environments, that we all find ourselves throughout the Federal Government, software encryption offers an attractive and affordable alternative to the costly hardware approaches. The answer is not to waive the encryption and software encryption is better than no encryption at all.

Acronyms

AES	Advanced Encryption Standard
ATA	Army Technical Architecture
CA	Certificate Authority
CAPI	Cryptographic Application Program Interface
CAW	Certification Authority Workstation
COMPUSEC	Computer Security
COMSEC	Communications Security
COTS	Commercial-Off-The Shelf
CSP	Cryptographic Service Provider
DA	Department of the Army
DAP	Directory Access Protocol
DES	Data Encryption Standard
DMS	Defense Message System
DoD	Department of Defense
DSA	Digital Signature Algorithm
DTS	Defense Travel System
EES	Escrow Encryption Standard
FIPS	Federal Information Processing Standard
IP	Internet Protocol
IPSec	IP Security
JTA	Joint Technical Architecture
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Codes
MIPS	Million Instructions Per Second
MISSI	Multilevel Information System Security Initiative
MISPC	Minimum Interoperability Specification for PKI Components
NSCS	National Computer Security Center
NIST	National Institute of Standards & Technology
NNTP	Network News Transport Protocol
NSA	National Security Agency
PCMCIA	Personal Computer Memory Card International Association
PKI	Public Key Infrastructure
POP	Post Office Protocol
PPTP	Point-To-Point Tunneling Protocol

RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm
SBU	Sensitive But Unclassified
SSL	Secure Sockets Layer
VPN	Virtual Private Network
WAN	Wide Area Network

References

- [1] Fulghum, David A., *Pentagon Budget Suffers New Cuts*, Aviation Week and Space Technology, volume 146, number 6, pages 24-25, February 10, 1997.
- [2] Covault, Craig, *Cyber Threat Challenges Intelligence Capability*, Aviation Week and Space Technology, volume 146, number 6, pages 20-21, February 10, 1997.
- [3] Chandtasekaran, Rajiv, *1,000,000,000,000 Calculations a Second*, Washington Post, page A1, December 17, 1996.
- [4] FIPS Publication 140-1, Security Requirements for Cryptographic Modules, NIST, January, 1994.
- [5] FIPS Publication 46-2, Data Encryption Standard, NIST, December, 1993.
- [6] Electronics Systems Division, Air Force Systems Command, Computer Security Developments Summary, report MCI-74-1, December, 1973.
- [7] National Computer Security Center, Final Evaluation Report of Computer Security Corporation Sentinel, CSC-EPL-87/004, 1987.
- [8] FIPS Publication 185, Escrowed Encryption Standard, NIST.
- [9] Schneider, Bruce, *Applied Cryptography*, Copyright 1996 by Bruce Schneider, second Edition, published by John Wiley & sons, Inc., pages 223-225.
- [10] "COMSEC Integration Alternatives," Proceedings of the 11th National Computer Security Conference, pages 122-125, October, 1988.
- [11] Thompson, Ken, "Reflections on Trusting Trust," Communications of the ACM, volume 27, number 8, pages 761-763, August 1984.
- [12] FIPS Publication 140-1, Security Requirements for Cryptographic Modules, NIST, January, 1994.
- [13] Stallings, William, Article by Ross J. Anderson, *Why Cryptosystems Fail*, Practical Cryptography for Data Internetworks, copyright 1996 by the Institute of Electrical and Electronic Engineers, Inc. pages 316-323.