The Use of Cryptographic Key Management in Practice

By Derek Yam

ACC 626
Introduction

Cryptography has become inherent in our daily working environment due to the advancement of technology. The volume of keys and key certificates continues to grow as cryptography is used in networks, end-user devices, and business collaboration software. Cryptographic key management is the design, implementation and execution of safeguarding information using access controls and keys. Therefore, cryptographic keys need to be securely created and managed until its termination. The scalability and extensibility of using keys has become a well-known topic in network security today and requires efficient and effective solutions to help companies achieve secure transactions while continually improving performance.

Encryption is vital in today’s society

The traditional, perimeter-based approach was to centralize information and control access at a central location. The introduction of a freer information flow makes the traditional approach impractical and ineffective. Therefore, there is a movement towards the information-centric approach where information can freely flow across networks and organizations and still be protected by the use of tools such as encryption, as long as an infrastructure is in place.¹

Encryption is the act of translating information into an unreadable form unless the individual has a unique translator, known as the key. The Aberdeen Group (2007) found in a survey that the leading driver for the use of encryption was to protect sensitive data (66% of respondents), whereas protecting against the threat of external attacks was a distant second at 19%.² However, external and internal threats, and the increase mobility of the sensitive information are becoming more prevalent as motivation to increase the use of encryption.

Per the survey, companies have used encryption to protect stationary data on end-user devices, focusing on file encryption (45%) and full-disk encryption (20%) on computers, and more have indicated the switch to full-disk encryption. Also, companies are beginning to attempt to gain more control over data flow to the end-user devices like smart phones, PDAs, iPods and

other USB drives. Aberdeen also provided suggestions to create a better key management system for companies:

1) Identify and classify their information assets

2) Establish consistent policies across the encryption keys’ life cycle, from generation to termination

3) Implement an appropriate portfolio of enabling technologies for encryption and key management. Some examples include Hardware Security Modules, standalone Key Management solutions, Public-Key Infrastructure (PKI), and Smart Card Issuance systems.

4) Establish controls to ensure compliance with both internal policies and external regulations. There should be formal awareness and end-user training programs. Policies should lay out clear responsibilities and accountabilities of individuals.

In an IDC survey in 2007, 75% of respondents said their expected use of encryption will increase. The survey also questioned how much they value security, confidentiality, platform compatibility, cost, expiration, among other criteria with security and confidentiality as items ranking the highest.

Standards and Guidelines for Cryptography

The Organisation for Economic Co-Operation and Development (OECD), known for its security guidelines by the information systems society, also has set out 8 principles on cryptography. There are also other standard setters from the government and the private industry – the International Organization for Standardization (ISO), IEEE, American National Standards Institute (ANSI), National Institute of Standards and Technology (NIST) and the Internet Engineering Task Force (IETF). However, with this many standards, most key management schemes are not transferable because most solutions provide their own

---

3 Ibid, page 14
4 Ibid, page 15-16
7 Ibid, page 10.
cryptographic functions that are based on specific specifications and standards that may not apply to other companies\(^8\).

Cryptography is now required by federal banking laws and by the big-three security-compliance standards: the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Biley Act, and the Sarbanes Oxley Act. However, it was reported in 2004 that companies do not use cryptography routinely because of the following factors\(^9\):

1) Hard to implement  
2) Not transparent to users  
3) Often can’t be decrypted by the recipient  
4) “User hostile” – difficult for users to manage.

Since then, cryptographers have taken advantage of the situation and as encryption became the prevalent theme for security, the demand for their services have increased and thus creating better encryption solutions have been very profitable.

A new federal standard was introduced recently in 2007 to place stricter key management protocols and updates testing for software modules and physical protection. The Cryptographic Module Validation Program, a joint effort by the United States’ NIST and the Canadian Communications Security Establishment, is responsible for publishing the Federal Information Processing Standard (FIPS) 140. With FIPS 140-2 already established for 6 years, FIPS 140-3 helps clarify key management techniques and update the old standards. This includes testing using new attacks against encryption modules such as advanced approaches using lasers to induce and disrupt electrical currents and the power level involved in guessing the cryptographic keys\(^10\).

**Encryption in Practice**

Security has become a major concern for internet users as web-based applications are increasing exponentially over the years. Unicast security has been well-addressed, with strong cryptographic methods that exist to support the point-to-point communication between a single user to a single receiver. However, with the introduction of collaborative work applications that require multicasting (communication between one sender and multiple receivers) such as white-

---

\(^8\) Ibid, page 14.  
boards, audio and visual teleconferencing and multi-user gaming software, security using encryption has become relevant once again. To maintain a secure group communication network, a group key is distributed to members of the group, which is used to encrypt messages. However, two problems arise in the use of group keys:\(^{11}\):

1) There is an inherent risk of external interception of encrypted messages over the Internet
2) It is possible for group members who have left the group to continue to decrypt messages

This requires re-keying of the group key to maintain secure communication, which requires updating all previous communications and managing previously used keys. For small groups, re-keying does not result in significant costs or constraints; however, scalability to a larger and more dynamic group can impair performance. Annadurai and Padmavathi (2005) believed the three important components of a secured multicast protocol are\(^{12}\):

1) Group access control by issuing capability certificates or preparing an access control list
2) Key distribution through a logical key tree
3) Dynamic membership management.

Most existing methods perform at a Big-O level of \(O(N)\) or \(O(\log N)\), meaning they operate at a proportional rate to the number of group members (N) or the log of the number. If the group grows exponentially (such as in situations of e-classroom lectures given to staff members around the world), key management would be difficult.

The access control policy is important when dealing with management of distribution of resources\(^{13}\). De Santis, Ferrara, Masucci (2004) noted that if we can split users into different security classes, we can construct a cryptographic key assignment scheme for any arbitrary access control policy. The key will protect each class’ data through a symmetric cryptosystem. The drawback is that it will penalize the high-level classes as they will be required to memorize and manage more information than low-level users\(^{14}\). Key management forces strong access control on the group keys and communication. However, it can be noted that there is no unique solution that can achieve all requirements of each class and the best solution for one application

---


\(^{12}\) Ibid, page 297


\(^{14}\) Ibid, page 200.
may not be the best for another. “A solution for secure group communication should complement a multicast application rather than drive its implementation”\textsuperscript{15}.

The PricewaterhouseCoopers (PwC) Cryptographic Centre of Excellence produces a quarterly journal which discusses many of the issues regarding cryptography that companies face. Geoffrey Grabow, then leader of the group, stated that “Weak security is worse than no security” as no security will result in transactions with no real value, as opposed to being unaware of high-value transactions being vulnerable in an insecure environment\textsuperscript{16}.

The emergence of e-commerce has also increase the demand for trust and authentication models for secure transactions. The PwC Journal explains the value of PKI, as one of the main functions it does is to verify the identity of its users. The certification authority (CA) signifies whether the information is valid and authenticated, thus providing the verification process. Once verified, the CA signs and issues digital certificate to give to the user. Once the user has obtained the certificate, this proves to the other parties that the user can be trusted, as approved by the CA. The weakness in PKI is when the certificate authority’s root key that is used to sign digital signatures is compromised\textsuperscript{17}. Thus, the root key must be protected from system failures such as crashes or viruses, or any external and internal intrusions.

There are software and hardware barriers to protect the root key. Both barriers have their own imperfections, and ultimately do not protect a company from the primary source of attacks which are from the employees\textsuperscript{18}. Software is susceptible to viruses, manipulation from hackers and system failures and physical barriers are cost-prohibitive to implement and maintain by many companies. There are multiple criteria the PwC publication mentions to evaluate hardware solutions:

1) Security  
2) Scalability  
3) Standards-Based  
4) Total Cost of Ownership for Security.

\textsuperscript{17} Ibid, page 9.  
\textsuperscript{18} Ibid, page 10.
The article concludes that hardware is the most viable way to protect the root key against all forms of attack and at a relatively lower cost\textsuperscript{19}.

Historically, Secure Socket Layer (an Internet protocol for transmitting private documents) keys and administration keys are example of keys that are not much of concern for management. The main concern lies with the complication of using PKI as “the need to manage the issuance, management, revocation and auditing of keys is increasing dramatically”\textsuperscript{20}. Most computers used in business now have embedded cryptographic devices on the motherboard chip called the Trusted Platform Management (TPM) chip, hence requiring for proper management and back-up of information on these computers\textsuperscript{21}. Although cryptographic keys help secure information due to the complexity of the process, it may also hurt users who forget and lose their keys, which is why backing up data is necessary. Back-up keys should be stored separately from the data to prevent another party use back-up storage media and reconstruct the information using the keys. However, hackers can attempt to compromise the key management system itself to bypass the encryption mechanisms. Therefore, PKI deployment can mitigate this problem. For the time being, the best solution is to educate management to fully understand the cryptographic key and document the management lifecycle\textsuperscript{22}.

To establish, implement and maintain good key management policies and practices, a company may follow KPMG’s key management life cycle framework as shown in Appendix A, taken from KPMG’s publication “Key Management Policy and Practice Framework”. Nevertheless, it is important to realize there should not be a generic set of key management practices and procedures for all applications or organizations\textsuperscript{23}. Periodic examinations by an independent third party using industry-recognized standards should be an important aspect of risk management and to ensure the key management practices are up to date.

Digital signatures are just another name for using public key cryptography. Instead of the old-fashion handwritten signatures, people have become increasingly familiar stamping their digital signatures on documents and emails as companies begin to move into a paperless

\textsuperscript{19} Ibid, page 11-12. 
\textsuperscript{21} Ibid, page 14. 
\textsuperscript{22} Ibid. 
workplace. There are difficulties for client-generated digital signatures to be effectively managed and secured. A study done by Lekkas and Lambrinoudakis (2006) showed in order to relieve management of this burden, companies should outsource digital signatures to a third-party as it is technically and legally feasible\textsuperscript{24}. The article concludes “passing the control to a signing authority rather than the signer is not a stronger commitment than the dependence on an identity certificate issued by a Certificate Authority”. Advantages for outsourced signatures include elimination of key management on the client side, reduced cost of the infrastructure, reduced complexity, existence of centralized archive of signatures and easiness for implementing time stamping\textsuperscript{25}.

As mentioned earlier, an important control that a company should have is access control, as it involves authentication, authorization and administration. Since each component of access control is interconnected and rely on each other, we should ensure that the IT solution is continually updated and maintained. Mattsson (2006) discusses a practical implementation of a transparent methodology to keep sensitive data protected, using policy-driven encryption and key management. The primary weakness of a database- and file-level encryption is that they do not protect against application-level attacks as the encryption is only implemented within the database management software\textsuperscript{26}. Data privacy solutions should include an automated and secure mechanism for key rotation, replication, and backup\textsuperscript{27}. The paper also suggested the following conclusions\textsuperscript{28}:

1) Policies are the foundation of good key management. Without a strong culture at the top of the company, even the most sophisticated encryption techniques may fail
2) Encrypted information should also be stored separately from encryption keys
3) Strong authentication should be used to identify users before they decrypt
4) Access to keys should be monitored, audited and logged, and sensitive data should be encrypted end-to-end

\textsuperscript{25} Ibid, page 443.
\textsuperscript{27} Ibid, page 17.
\textsuperscript{28} Ibid, page 18.
Another example of key management in practice is within the Payment Card Industry (PCI), such as the use of Visa, MasterCard and other Smart Cards. Companies that store, process or transmit cardholder data are subject to the PCI Data Security Standard (DSS), which is composed of twelve fairly straightforward and detailed requirements explained in a 17 page document. The standard revolves around six components:

1) Build and Maintain a Secure Network
2) Protect Cardholder Data
3) Maintain a Vulnerability Management Program
4) Implement Strong Access Control Measures
5) Regularly Monitor and Test Networks
6) Maintain an Information Security Policy.

Key management can help achieve PCI compliance as the PCI specification requires keys to have strong controls in place during the key lifecycle as they are generated, stored, retrieved, revoked and archived.

In addition to the PCI DSS, VISA International has also compiled a complete set of requirements for the security of Personal Identification Numbers (PIN) used by individuals for personal banking at locations such as the Automated Teller Machines (ATM). Although limited in use, the protection of PIN numbers is a high priority as most working individuals would have credit or bank cards.

There are several cryptographic solutions that are available for management to use. Sun Microsystems offers a Secure Digital Archive solution involving cryptographic key management by using the Sun Crypto Key Management System to help businesses achieve data privacy as well as reliable and efficient authentication. There is also nCipher’s keyAuthority Solution Suite, which provides a centralized cryptographic key management and automated key management.

---


distribution to security applications because nCipher believes that centralizing user management controls and policies can simplify the audit and compliance process\textsuperscript{33}.

**Conclusion**

“Protecting customer data is much less expensive than dealing with a security breach in which records are exposed and potentially misused”\textsuperscript{34}. Improving the strength of encryption and efficiency and performance simultaneously is a continuous effort by companies within today’s digital age. Cryptographic key management has been a well-researched topic and many researchers and practitioners believe a good encryption system depends on good management stemming from policies and attitudes of management. Looking forward, the current structure of encryption could evolve to quantum cryptography. Quantum cryptography borrows the concept from quantum mechanics and results from two users of a common communication space to create a shared body of information, without the hassle of exchanging keys in essence\textsuperscript{35}. However, this would imply new policies and standards will need to be created, leaving costly transitions in the future.


Appendix A

KPMG Key Management Policy and Practice Framework – Key Life Cycle

Figure 1: Key Life Cycle

---

Works Cited


