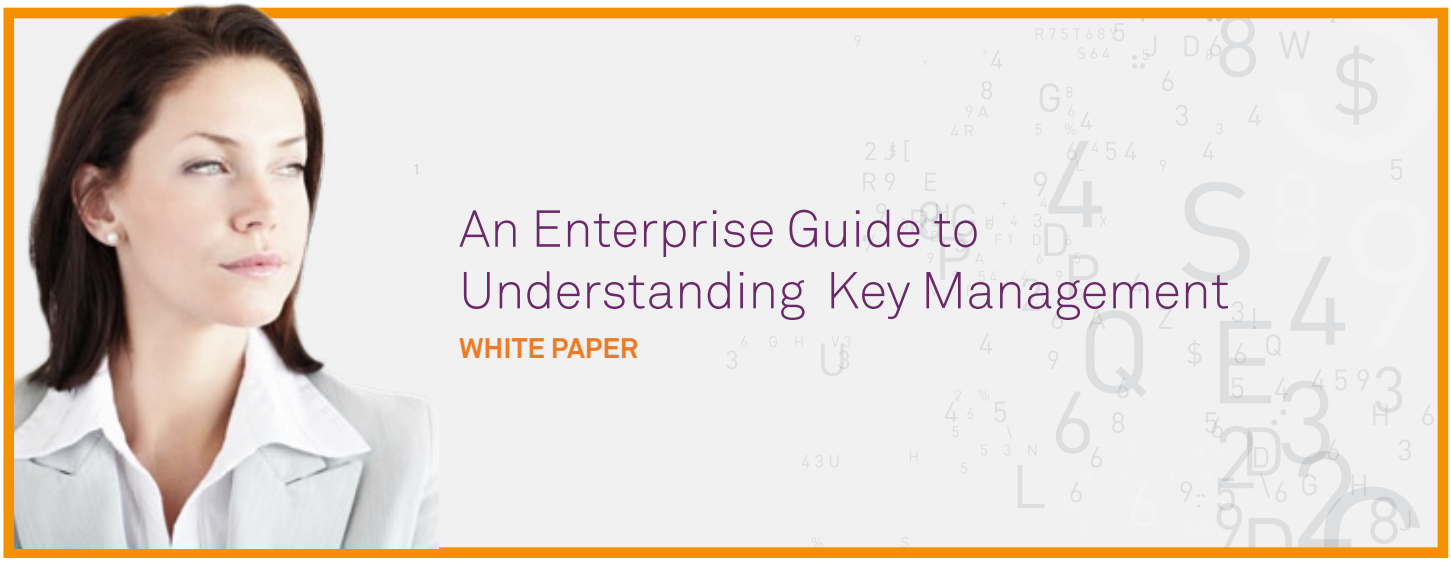

An Enterprise Guide to Understanding Key Management

WHITE PAPER

Executive Overview

Establishing effective key and policy management is a critical component to an overall data protection strategy and lowering the cost of ongoing management.

A policy-based approach to key management provides the flexibility and scalability needed to support today's dynamic networking environments. Policy-based key management ensures the secure administration of keys throughout their entire lifecycle, including generation, distribution, use, storage, recovery, termination, and archival. This will also enhance business processes and relieve often over-burdened IT staff by breaking down the "islands of security" and "security silos" that are too often typical to enterprise environments.

Each business has its unique network and operational requirements, which results in the need for tailored key management policies. While policies can be based on standardized specifications, it is a best practice to conduct a comprehensive risk assessment to reveal specific considerations in designing key management policies and procedures. For a more comprehensive look at applying enterprise-level key management, please refer to the white paper, Applying Enterprise Security Policy and Key Management.

The information presented in this white paper discusses various approaches to cryptography and key management, and can be used as a starting point for developing an effective policy-based key management solution. Taking a proactive approach to data protection—planning, policies, and process—results in a smoother implementation and a positive return on investment. Unlike disparate, multi-vendor point solutions that can create limited "islands" of security, SafeNet's approach provides an integrated security platform with centralized policy management and reporting. This is ideal for seamless, cost-efficient management of encrypted data across databases, applications, networks, and endpoint devices. Centralized encryption and key management also provides a uniform and ubiquitous way of protecting data while reducing the cost and complexity associated with compliance and privacy requirements.

Introduction

The first recorded organized usage of cryptography was during the reign of Julius Caesar in the early Roman Empire. Caesar recognized the importance of secret communications to successfully managing the political and military structures and processes of the Empire. Throughout history, this theme has been played out in many different forms of secret communications for a wide variety of purposes.

With the need for secret communications also comes the need to effectively manage the associated cryptographic keys and the most successful systems for secret communications have been the ones with the most effective key management. Conversely, some of the most famous failures of secret communications have come about, at least in large part, because of weaknesses in key management (the Ultra program to exploit the German Enigma is perhaps one of the most familiar examples).

Since the early 1970's, cryptography has played an increasingly significant role in protecting commercial and personal, rather than only high-level military and political, communications. This has been a tremendous enabling influence in the development of what has come to be accepted as electronic commerce.

The growth of e-commerce and associated cryptography presents relatively new challenges to the enterprise. The typical implementation of cryptography has been to put up protective walls around either the transmission channel, for data being communicated, or the storage medium, for data at rest. To provide this walled protection, it is typical for disparate end-point solutions to be deployed to tackle what is perceived as isolated problems. Unfortunately, the disjoint security rule sets in end-point solutions (VPN, TLS, encrypting HD, tape & HD storage encryptors, etc.) makes it difficult for the enterprise security professional to match the security with the data in various locations and lifecycles.

How does an enterprise "manage" security and cryptography, in particular, in the face of the many disjoint security rule sets in place? The answer documented in this white paper is to show the reader that shifting the focus of cryptography and key management from protecting the transmission and storage media to protecting the data itself is the effective way to address enterprise security requirements for both the present and future. Changing from a technology-driven approach, focused around the individual end-point solutions, to a policy driven approach that provides a much needed framework for cryptography (regardless of the details of the end-point solutions) will equip the enterprise for robust key management capable of handling security needs presented by the very nature of e-commerce; multiple applications, partners and customers accessing the corporate network.

Background

This section presents a brief background of the relationship between security policy and key management. It is intended to provide a foundation for subsequent sections.

Cryptographic services support the transition to digital identification of individuals, access control, and audit and non-repudiation functions. Managing the cryptographic keys used to provide these services is the foundation for defining and enforcing security controls in the digital world that are equivalent to those in the "bricks and mortar" world. For example:

- A cryptographic key is used to lock and unlock cryptographic data protection just as physical keys lock and unlock a padlock protecting physical items.
- In the digital world, asymmetric key pairs provide an interesting twist to the padlock analogy by offering the equivalent of a "seal". The sender locks the data using a private key that is known to belong only to him/her. The recipient is sure of the sender's identity by virtue of unlocking the data using a publicly available key that only corresponds to the sender's private locking key.
- The act of providing a key to an individual grants him or her access to the protected resources – the same principle applies to both physical and digital resources.

Elements of Effective Enterprise Security Policy

- Entity (users & devices) definition – who, what is covered?
- Asset definition and classification – what is covered and how is it broadly categorized according to protection needs?
- Authorization – who is allowed to access which assets through which access mode?
- Accountability – associating an operation uniquely with an entity.

- Security controls on access to keys can be used to proxy for controls on access to protected resources – e.g., signing out a key can proxy for access to assets in a locked room and the key issue log is the audit record for access to those assets. The same applies in the digital world.
- Key pairs and digital certificates provide a means of authenticating an individual's identity equivalent to a photo ID.

The decisions regarding which security controls to employ including their strength generally begin with a security policy. The security policy can be formal, designed to stand up to the strictest scrutiny. One might expect this for military or other government systems or, perhaps, large financial institutions. Alternately, the security policy could simply be expressed implicitly in the way in which the organization has organized its security controls. Whether it is explicit and formal or implicit and informal and whether it exists in the physical world or the digital world, there are a few fundamental aspects that must be considered in developing any security policy.

Security Policy and Services

This section outlines the important considerations when designing a security policy and the ecurity services that can be employed to enforce the policy. Cryptographic services that can be used to implement the various security services are also introduced.

Figure 1 Elements of Effective Enterprise Security Policy

Elements of Effective Enterprise Security Policy

The following fundamentals must be considered in designing an effective enterprise security policy:

- Entity (users & devices) definition – who, what is covered?
  - Authentication – how is identity proven?
  - Roles – how are users grouped for authorization purposes?
- Asset definition and classification – what is covered and how is it broadly categorized according to protection needs?
- Authorization – who is allowed to access which assets through which access mode?
- Accountability – associating an operation uniquely with an entity.

Additionally, the threats that may impact system resources (assets and services) must be understood in order to assign the correct controls at the appropriate strength.

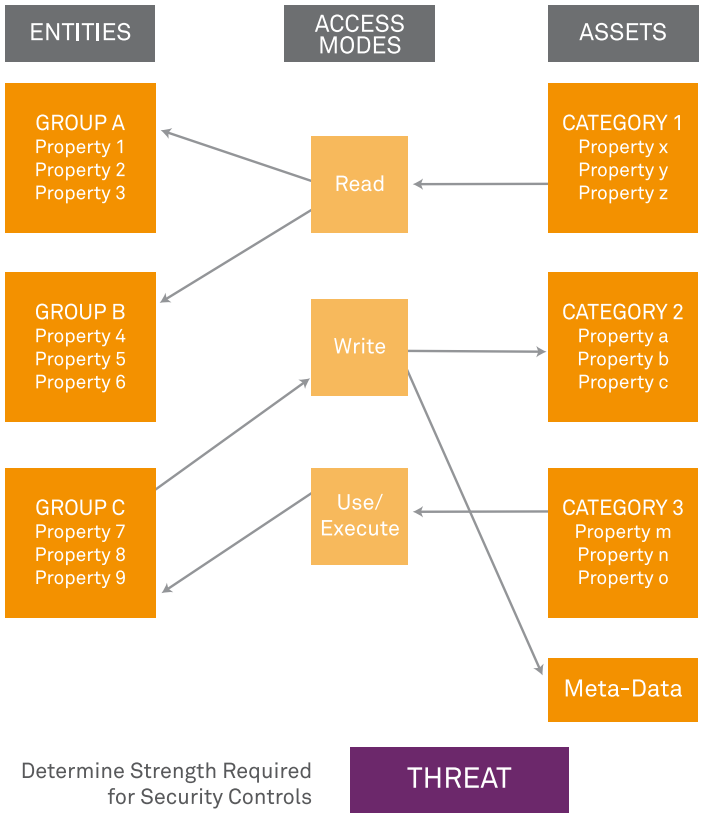

Figure 2 Security Policy Fundamentals

Security Services to Enforce Security Policy

The following core security services can be used to enforce the enterprise security policy:

- Access Control
- Identification and Authentication
- Confidentiality
- Integrity
- Non-repudiation
- Audit
- Availability Protection

Cryptographic Services to Implement Security Services

- Encryption/decryption – Confidentiality
- Message digest – Integrity
- Digital signature – Integrity, Authentication, Non-repudiation

Access control, I & A, Audit and Availability are also supporting services for cryptography & key management.

Cryptography Basics

This section presents a brief overview of the fundamental concepts of cryptography and some terminology definitions to ensure proper understanding of later discussions.

Symmetric

Symmetric cryptography is used primarily for encryption/decryption to provide confidentiality services. It can also be used with message digest to provide authentication and integrity services.

As the name implies, symmetric cryptography requires that both sender and intended recipient(s) share the same key, which must be kept secret by all parties participating in the communication. The same symmetric key is used by the sender to encrypt a message and by the recipient(s) to decrypt the message. In a many-to-many communications scenario, key management can become extremely burdensome since the number of symmetric keys that must be managed by each member of the network grows as N2. The fact that each key must be bound to the content it has encrypted, but at the same time protected so that only authorized individuals can access it compounds the key management problem.

In many instances, access to symmetric keys is controlled based on an individual's need or authorization to access specific information. As such, they must be securely transportable from one entity (person, application or device) to another according to an organization's

security policy and an entity's access rights. As discussed in the next section, the use of asymmetric key pairs in a public key infrastructure (PKI) provides a scalable way to enable this key sharing. PKI, however, is not the only solution and may not be the best solution given an organization's business needs and IT environment. A number of other approaches to symmetric key management have been employed for many years and continue to be used today.

Often it is best, from the security policy, performance and availability viewpoints, to keep symmetric keys protected inside a central key management system and provide them to end entities as their access rights are granted and confirmed. The key management system then becomes both a long-term key repository for the organization and a primary point of security policy enforcement.

Asymmetric

Asymmetric (public key) cryptography relies on key pairs – one private (kept secret by the creator) and one public. The best known asymmetric algorithm is known by its authors' initials – RSA for Rivest, Shamir and Adelman. In its original form, the public key of the intended recipient is used to encrypt a message and the recipient uses his/her private key to decrypt the message. Early in the development of RSA, however, it was realized that the processing model could be reversed to allow a sender to encrypt a message using his private key and that anyone receiving it could decrypt the message using the corresponding public key. Because the private key is kept secret by its creator, encryption with a private key could then form the basis of a digital signature – this has become the most well-known usage of asymmetric cryptography.

Asymmetric key pairs are normally bound to an identity – a person or system – and can be used for signing, authentication and encryption/decryption for key transport. In the case of key transport, asymmetric keys are not used to directly encrypt data, but rather to protect a symmetric key (used to encrypt the data) and, in some applications, bind a symmetric key to an individual (by encrypting it under a user's public key).

A signing key should never leave the control of the individual or system that is performing the signing – otherwise non-repudiation is compromised. This is the philosophy behind HSM backup strategies that strongly bind asymmetric keys to a specific HSM domain, representing the authority or sphere of control of a signatory.

Key Management

The Basics

Key management is a broad concept with a variety of different implementation approaches based on the needs of the target business application and user community. No matter what form key management takes it cannot stand alone and must be interpreted in the context of

Objectives of Enterprise Key Management include:

- Securing keys throughout their lifecycle
- Secure key storage
- Key usage authorization
- Accountability

supporting a higher-level enterprise security policy. Enterprise key management can be seen as the means of translating the enterprise security policy into terms suiting the cryptographic services used in implementing all or part of the security policy. In its most general form, enterprise key management can be broken down into the following high-level objectives:

Secure Key Lifecycle: This provides the means to ensure the security of keys throughout their lifecycle while subject to operations such as:

- key and key pair generation,
- key transport and sharing,
- key backup and restoring from backups,
- key and key pair usage monitoring and control (time-based, volume/operations-based),
- key rotation, renewal or roll-over,
- meta-data maintenance (e.g., changing status from encrypt/decrypt to decrypt only), and
- secure key destruction or archival at the end of a key's service life.

Secure Key Storage: Keys must be securely stored throughout their operational life. Details regarding storage media and protection requirements depend heavily on the keys' roles in supporting the various elements of the security policy. Keys are often stored in hardware devices intended to strongly protect the keys. Examples of these devices include identity tokens (smartcards, USB tokens); trusted platform modules in desktop computers; embedded modules in special purposed devices (i.e. tape/disk drives) and, of course, hardware security modules.

Key Usage Authorization: Measures must be provided to ensure that keys can be used only for authorized purposes by authorized entities and that authorized access to keys cannot be interrupted by others. Access control, authentication of users and confidentiality protection are all critical to meeting this objective.

Accountability: Records of all state changes and usage, or attempted usage, of key material must be created and maintained. The records must conform to regulatory requirements for security audit and be sufficient to ensure non-repudiation.

Because of the importance attached to these high-level security objectives, many organizations insist on having the core components of their key management systems certified according to a recognized standard and certification scheme such as NIST's Security Requirements for Cryptographic Modules, FIPS 140-2, or the Common Criteria, ISO 15408.

Key Management and Security Policy

In general, each organization will have its unique security policy characteristics that must be reflected in key management policy requirements that are equally unique to the enterprise. However, a great deal of common ground with respect to security needs allows for a standardized, core set of key management policies and techniques. The sub-sections that follow briefly discuss a few of the major standards and guidelines and some of the aspects that are typically unique to the individual organization.

NIST Key Management Recommendations

The NIST Key Management Recommendations are published in SP 800-57 and consist of three parts. Part 1 provides generally-applicable guidance and best practices for managing key material. Part 2 provides guidance on policy and security planning requirements specifically for U.S. government agencies. Finally, Part 3 provides key management guidance for commonly used IT security-related systems.

Part 1 contains introductory and background material and presents a high-level framework for the discussion of key management issues. The framework categorizes the various cryptographic services and key material according to its usage (e.g., for confidentiality, integrity, etc.) and introduces the concept of security strength as a common metric for the strength of the protection provided by a given algorithm/key length combination.

Part 2 is intended primarily for U.S. Government departments and agencies and is focused around the concept of a public key infrastructure (PKI)-based key management infrastructure (KMI). Although many of the organizational and management recommendations may not be generally applicable outside of the Government arena, the KMI concept and the descriptions of the services provided by it are useful in any context.

Part 3 discusses the key management issues and requirements associated with a number of IT security-related application systems such as PKI, Transport Layer Security (TLS) IP Security (IPSec) and Kerberos authentication & authorization.

IEEE Key Management Infrastructure

The IEEE Key Management Infrastructure (P1619.3) is primarily designed to address the issues of symmetric key management for data at rest encryption/decryption. It presents a centralized key management system employing key management servers for key generation, key storage, key distribution, key archival and audit services to clients. Service agents act as the local interface between the client and the key management server. It specifies an XML-based messaging system to communicate policies and key material. It specifies key types and attributes associated with keys and data. It also describes a method for matching the data to be protected attributes with the attributes of the keys used for protection.

OASIS Key Management Interoperability Protocol (KMIP)

The Key Management Interoperability Protocol (KMIP) does not include any specification or description of a key management framework or infrastructure. It specifies the objects to be managed, their attributes, the key management operations that can be performed and the messages required to complete those operations. It does not discuss the cryptographic services for which keys are required and does not provide any method for creating a policy association of keys with the data to be protected.

Key Lifecycle Considerations

Cryptographic keys typically follow a sequence of lifecycle states from their initial generation through to end-of-life and destruction. Understanding these lifecycle states is important to properly plan key usage. The following lifecycle description is based on concepts presented in both the NIST Key Management Recommendations and the IEEE Key Management Infrastructure.

Lifecycle Phase	State	Key Activities
Pre-operational	Pre-active	Generate, certify, provision, backup
Operational	Active	Encrypt, decrypt, sign, verify
	Limited Use	Decrypt, verify
Non-operational	Disabled/Suspended	None. Can be restored to operational service
	Compromised	None. Cannot be restored to service
Post-operational	Destroyed	Securely destroyed, cannot be restored

Table 0 1 Cryptographic Key Lifecycle States

Figure 3 Key Lifecycle Activities

Key Management Policy Management Elements

To accommodate the desire for centralized key management within a scalable, distributed architecture, there are three distinct elements involved in the implementation of a key management policy. These are described in the following sub-sections and illustrated in Figure 4. These three elements are architectural constructs and can, of course, be physically and logically implemented in many different ways. In particular, it is possible to have an implementation that co-locates all three elements, just as it is possible to have an implementation in three distinct logical layers with a central policy definition point and multiple instances of the other two elements.

Policy Definition Point

This is the policy element responsible for the definition of policies for key management. This element is typically centralized at the highest level within the enterprise management infrastructure. The Policy Definition Point has no operational role that is directly associated with the end-point clients. It serves primarily as the central point for policy definition and coordination and may also serve as the "root of trust" for the infrastructure. As the "root of trust", it may be closely associated with a PKI Certification Authority or with a Zone or Domain Master key in a symmetric key-based system.

Policy Application Point

This element is responsible for the dissemination of specific policies to lower-level elements within a given domain. There may typically be several of these elements within the infrastructure. The policy application point could be implemented, for example, in conjunction with a domain's LDAP directory implementation or as part of a domain management server. This element would also serve the role of a "key management server" in the NIST or IEEE KMI concept, generating keys or providing keys to end points in accordance with a given policy.

Policy Enforcement Point

The policy enforcement points are distributed throughout the infrastructure and must be implemented as closely as possible to (preferably within, although constraints on the end-points might make that goal impractical to achieve) the components that perform the crypto operations. They consume the policy definitions disseminated by their applicable Policy Application Points and are responsible to ensure that crypto operations are only performed in accordance with the defined policies. This element would be equivalent to the "service agent" in the NIST or IEEE KMI.

End-Points

The end-points or clients are the devices that hold local copies of keys for use and provide the cryptographic services required by the enterprise's business applications. Depending on the nature of the operational environment and the overall level of security required by the applications, these end-point devices may be either software or hardware implementations.

End-to-End Security in the Infrastructure

Although the focus of most of the discussion in this paper is on the ways in which key management policy can be defined and enforced in support of the enterprise's overarching security policy, it is important not to lose sight of the critical importance of security to the key management infrastructure itself. From the highest level at the Policy Definition Point through to the Policy Enforcement Points and end-point devices, consistent, strong security controls and mechanisms are needed to ensure the proper operation of the infrastructure.

It would be relatively easy to, for example, put a great deal of emphasis on security at the Policy Definition Point while allowing software end-point implementations to be used in largely untrustworthy environments. Conversely, it would be easy to imagine requiring the use of FIPS 140-2 Level 3 hardware solutions at the end-points with the Policy Application Points being implemented in software running on standard server platforms. As for any security system implementation, a proper risk assessment should be performed on the planned key management infrastructure implementation to be sure that appropriate security controls are in place at all levels of the infrastructure.

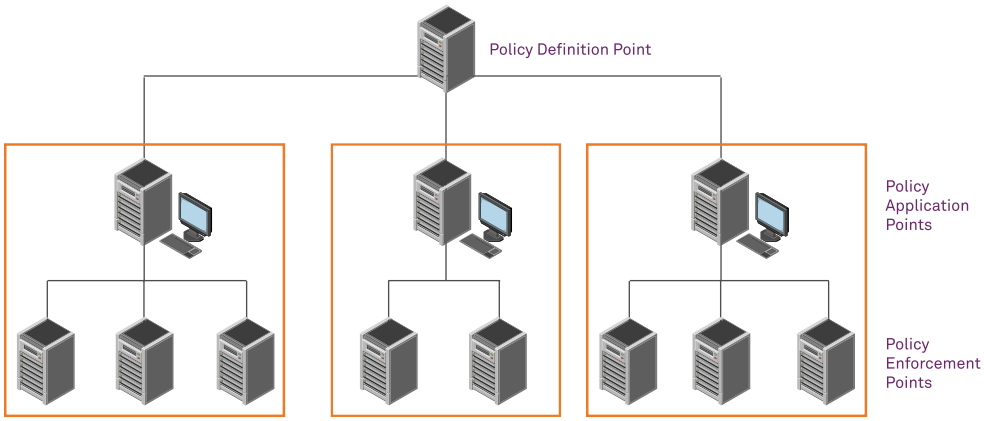

Figure 4 Key Management Elements

Conclusion

The key management approach described in this paper and the proposed solution implementation directly address the pressing need for cryptographic key management focused on satisfying enterprise security requirements by protecting data throughout its lifecycle regardless of its presence in the infrastructure. By taking this approach enterprise-level key management becomes an important enabler to solving business problems and not simply another piece of security technology. For a more comprehensive look at applying enterprise-level key management, please refer to the white paper, Applying Enterprise Security Policy and Key Management.

About SafeNet

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers' most valuable assets, including identities, transactions, communications, data and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises and government agencies and in over 100 countries trust their information security needs to SafeNet.

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected