



Enterprise Key Management: A Strategic Approach

White Paper
February 2010
www.alvandsolutions.com

Overview

Today's increasing security threats and regulatory mandates have forced enterprises to adopt a wide range of encryption technologies which in order to be effective require an Enterprise Key Management strategy. This whitepaper offers insights into Enterprise Key Management, outlines the required system components and the evaluation criteria to determine an effective solution for your organization.

Topics covered include:

- A Definition of Enterprise Key Management
- The Key Management Lifecycle
- Criteria for Effective Key Management
- Enterprise Key Management Architectures
- Best Practices

Introduction

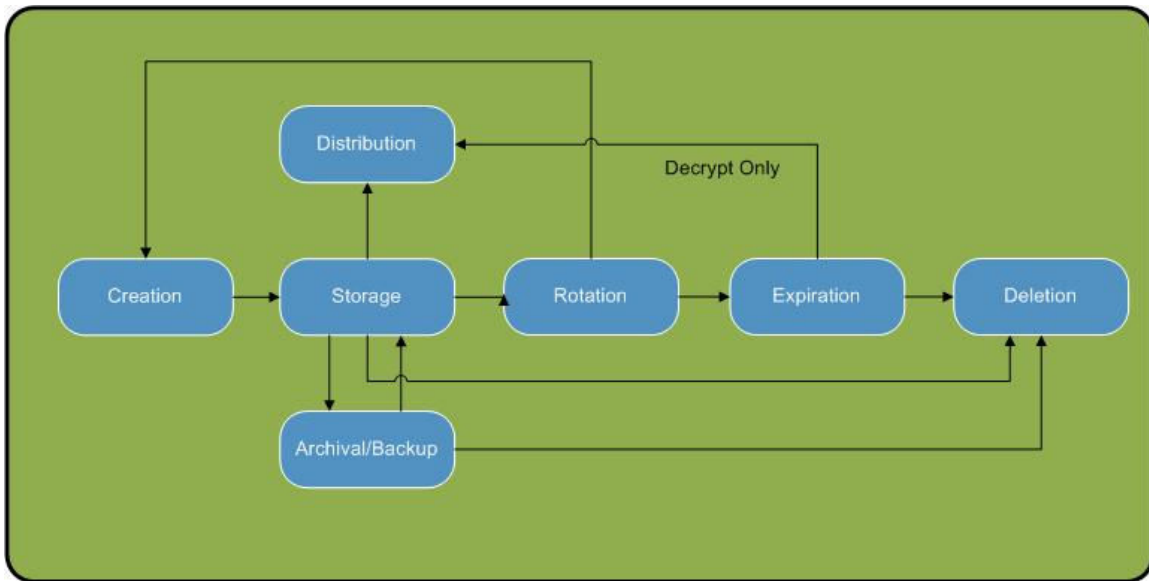
As information security breaches continue to grow and regulatory compliance becomes increasingly mandatory, many organizations have switched their security effort to focus on data encryption. Whichever level organizations wish to encrypt data at – application, database, file or storage level, laptops and other storage media – there are proven technologies available to administrators. There are also a number of authentication and access control mechanisms that can be used ensuring only authorized users can encrypt and decrypt data; regardless of the implemented technique cryptographic keys form the foundation of the security solution. If these keys are compromised then the security of your encrypted data is likewise compromised. So what are the essential elements of an effective key management implementation? What criteria are important in selecting your solution? This white paper addresses these questions and provides insights into how your sensitive data can be securely encrypted.

What is Enterprise Key Management?

The essential processes involved in key management are used to create, store, distribute, rotate, archive and delete keys. A single solution that integrates with multiple vendors' key management and security products enables security teams to effectively manage keys without excessive cost and management overhead. Furthermore, to ensure encryption meets its objectives, all the key management phases must be conducted in a manner that is secure, reliable, and auditable.

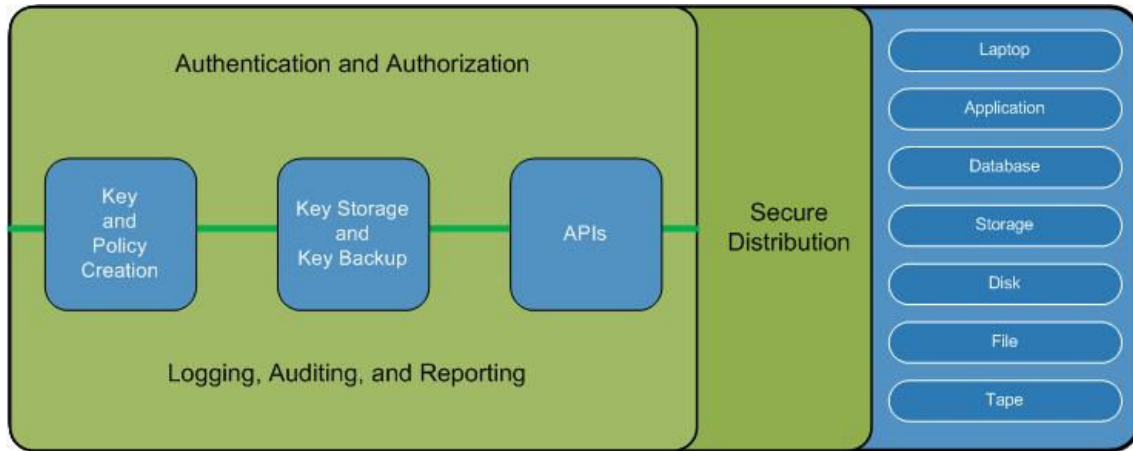
Key Management Life Cycle

As described in the illustration below, a key must be managed from the moment it is created to when it expires and is deleted for security measures to be effective.



Components of an Enterprise Key Management

The diagram below describes the major components of enterprise key management. Certain components are closely matched to specific phases in the key management lifecycle, for example key creation or key storage. Other aspects, such as logging, play a role in every phase of the key lifecycle.



Criteria for Effective Enterprise Key Management

Enterprise key management often means balancing several different and occasionally apparently contradictory requirements. Typically, all of the following criteria must be considered:

- **Security:** Administrators, users, partners, and customers need to know they can trust their data and identities are safe at all times.
- **Performance:** The system must function in a manner that is transparent to legitimate data users and business processes, and it must scale easily.
- **Flexibility:** The system must be adaptable to a range of environments and be capable of integration, through standard interfaces, with all types of data encryption systems from a range of vendors. Interoperability and adherence to industry standards is also an important consideration.
- **Manageability:** Key and policy management must be simple and intuitive so that administrators fully understand—and granularly control—system status at all times. There must also be capabilities for logging and auditing all administrator and user actions.
- **Availability:** The system must be able to recover in the event of one or more network or equipment failures, or even a widespread disaster.

Security

Security must be maintained at every phase of the key management lifecycle. Key factors to consider when selecting a key management solution are:

- **Centralized Management:** Administrators should be able to manage keys from a single, central repository.
- **Key Storage:** The solutions should provide a location for key storage that is separate from the location that holds the encrypted data.
- **Key Rotation:** The ability to rotate keys is an important security feature. Key rotation can occur on a regularly scheduled basis or may be required as part of the reaction to a breach.
- **Open Cryptographic Standards:** To support security best practices and eliminate the exposure of weaker or older encryption algorithms, key management must support keys for the most advanced open cryptographic standards available. It is important to implement industry standard cryptography algorithms, as they have been thoroughly tested by government agencies and standards bodies such as NIST, to ensure high levels of security.
- **Authentication:** Mutual authentication between a key management solution and systems requesting keys is imperative. Without mutual authentication it is possible for an attacker to execute a man-in-the-middle attack.
- **Auditing and Logging:** a comprehensive system of auditing and logging is required in order for administrators to spot any significant usage trends or to establish a forensic trail. There should be the ability to track every administrator, user, or system action.

Performance

Enterprise-scale key management needs to be able to handle a wide range of different environments and accommodate many thousands, sometimes even millions of keys. In order for key management to avoid becoming a bottleneck for business operations, the import and export of keys must be accomplished at an extremely fast rate. The time required to export a key should be in the order of milliseconds.

Flexibility

An enterprise key management solution should offer a single comprehensive approach that can interoperate with the entire enterprise environment, no matter how complex or heterogeneous. It needs to support not only data center applications, but also remote sites, such as retail point of sale (POS) and branch offices. The system must scale easily to accommodate future requirements for business growth or additional redundancy requirements. The system must support open APIs, which enable communication and interoperability with a range of Web servers, application servers, database servers, file servers, laptops, disk and tape storage, and other devices from multiple vendors.

Manageability

Manageability defines the ease with which administrators are able to configure and deploy key management to align with business and security policies and then interface with the system on an ongoing basis. This has important consequences, not only in relation to the resources required to configure the system initially, but more importantly in terms of ongoing operational and maintenance costs.

Following are some of the important questions to consider when evaluating the usability of the system:

- **Security Officer:** Who has been granted authority to create keys? How are policies defined and managed? Can I simply and quickly restrict specific users from access to the keys or the ability to encrypt or decrypt data? How granular are policies? Can I restrict usage by time of day or number of transactions? Can I easily implement an effective separation of duties?
- **Administrator:** How easy is it to manage ongoing operations, such as setting up administrator permissions, using syslog and SNMP to do auditing and log retention, upgrading software, doing backup and recovery, and rotating keys?

The ability to address these requirements effectively is critical and in some cases mandatory. One of the newer PCI requirements, for example, is to have a strong key retention and key rotation policy.

Availability

Enterprise key management needs to be able to provide service even in the event of a sharp increase in demand or in the event of one or more network or equipment failures. A complete approach to ensuring availability requires the implementation of replication, load-balancing, and recovery capabilities.

Enterprise Key Management Architectures

There are two classic types of architectures that can be applied to key management:

- **Centralized:** the administrator has centralized control over every part of the key management lifecycle
 - Advantages:
 - Tight control
 - Efficient centralized audit and logging
- **De-centralized:** for geographically dispersed enterprises users can access key management functions at a regional level rather than through a central location
 - Advantages:
 - Limits exposure in the event of a breach
 - Disadvantages:
 - Lack of enterprise-wide audit trail
 - No centralized management

In practice, especially for large corporations, it is best to consider a distributed architecture that combines elements of both of these architectures. In such a scenario master control and enterprise-wide system monitoring can be retained at the data center, while at the same time optimizing performance through delegation of selected functions to remote locations. The architecture can be configured so that remote locations can fail over to the central location.

Best Practices

The following is a basic list of recommended best practices:

- Ensure the enterprise's business and security objectives are well understood before choosing and deploying key management.
- Plan for all aspects of the key management lifecycle and for future scalability in terms of both system size and diversity.
- Ensure access controls are implemented with as much granularity as practical.
- Never transmit or store keys in an unencrypted format.
- Use standard cryptographic algorithms and utilities.
- Back up keys on a regular interval to a separate dedicated hardware device.
- Continually monitor or audit all automated and manual actions.
- Ensure procedures are in place to ensure the integrity and security of logs.
- Authenticate and sign logs for non-repudiation.
- Restrict access to audit logs to prevent tampering or deletion.

Enterprise Key Management from Alvand Solutions

Alvand Solutions through its partnership with SafeNet, a global leader in information security, offers a solution that brings unparalleled cost effectiveness, security, and control to enterprise key management. The SafeNet platform features secure centralized management, highly granular control and comprehensive auditing and logging using an integrated, appliance-based approach that significantly reduces maintenance costs. The SafeNet platform can interoperate seamlessly with other security solutions and enables organizations to manage multi-vendor security deployments with unprecedented ease.

Proven daily in over 100 of the Fortune 1000 companies, SafeNet platforms:

- Offer an integrated key management solution that can support a range of enterprise encryption environments that protect data at the web, application, database file, storage, tape and device-level.
- Provide a cost-effective, centralized solution for enterprises that need to support key management at thousands of branch locations or retail outlets.

With Alvand Solutions organizations gain the ability to leverage a common enterprise key management architecture that supports heterogeneous enterprise environments regardless of size or complexity.

About Alvand Solutions - At Alvand Solutions, we strive to deliver significant value to organizations through the innovative implementation and support of IT solutions. Our Enterprise Data Protection, Management of Offshore Projects, and Application Development Services offerings will help secure your return on investment. Our team includes professionals with significant industry and related information technology experience. For more information please visit our website at <http://www.alvandsolutions.com> or email us at info@alvandsolutions.com.