



## A Strategic Approach to Enterprise Key Management

**EXECUTIVE SUMMARY:** In response to security threats and regulatory mandates, enterprises have adopted a range of encryption technologies, but without effective enterprise key management in place, the success of any of these technologies can be jeopardized. This white paper offers guidance into enterprise key management, outlining the critical system components required, and the essential criteria with which to evaluate an effective solution.

**INTRODUCTION:** As the financial impact and reported number of information security breaches continues to increase and regulatory compliance becomes mandatory, many corporations are focusing their security efforts and investments on data encryption. Proven technologies are now available which allow administrators to encrypt data at the application, database, file or storage level, on laptops as well as on storage media such as disks, tape, optical or other electronic media. A number of advanced authentication and access control mechanisms can be used to ensure that only authorized users are permitted to encrypt and decrypt sensitive data.

Regardless of which of the above techniques is implemented, cryptographic keys are the essential foundation of the security solution. If private keys fall into the wrong hands—whether through negligence or a malicious internal or external attack—the security of your encrypted data is permanently compromised.

What are the essential elements of an effective key management implementation, and what are the most important factors in selecting a solution? This white paper addresses these questions and provides essential insights into ensuring that encryption implementations effectively secure sensitive data.

## What is Enterprise Key Management?

Key management comprises all of the processes that are used to create, store, distribute, rotate, archive, and delete keys. To ensure encryption meets its objectives, all these phases must be conducted in a manner that is secure, reliable, and auditable.

Further, to effectively manage keys within an enterprise, security teams need a single solution that can be integrated with multiple key management and security products from a range of vendors. For example, in an enterprise that has implemented database, application, and storage encryption technologies, the cost and management overhead of implementing a vendor-specific key management solution for each product could be prohibitively high. Multiple different resources would need to be trained and managed. Auditing and record keeping would be extremely complex. Overall, there would be increased risk of either not meeting compliance requirements or not being able to recover data because of misplaced keys.

## The Key Management Lifecycle

For security measures to be effective, a key must be managed from the moment it is generated to when it is deleted. These two events mark the beginning and the end of a multi-phase key lifecycle that can sometimes span several years.

The key lifecycle is illustrated below in Figure 1:

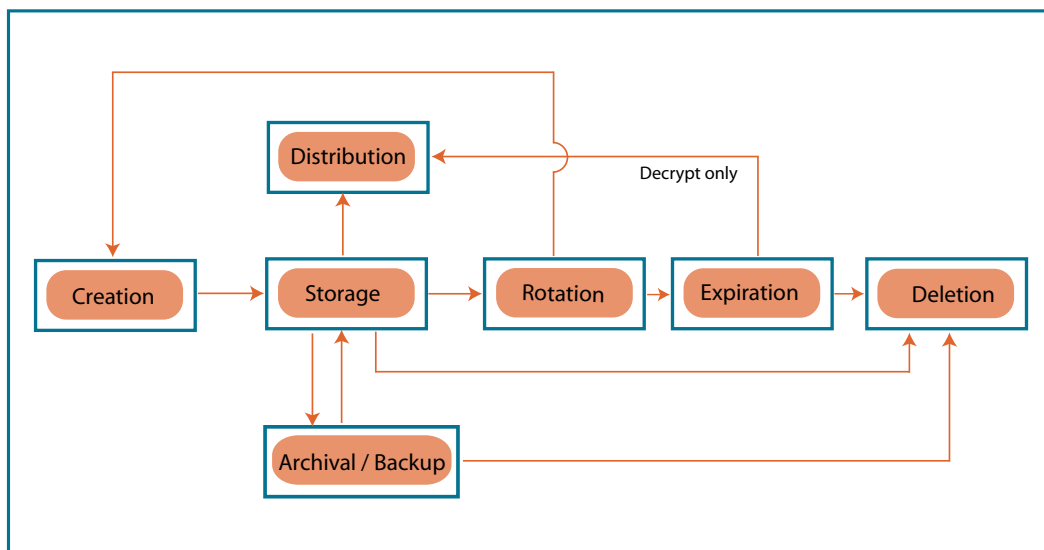


Figure 1: Key Management Lifecycle

To better understand the potential complexity of managing keys in an enterprise, particularly for a large, global corporation, it is useful to understand each of these phases:

### Creation

The most secure methods for creating a key use a FIPS-validated random number generator. As an alternative, properly generated keys can also be imported into a system from a trusted source over a secure communication channel. For optimal security, the amount of data that is encrypted with each unique key should be limited to the smallest manageable increment. In the event of a key being breached, this limits the degree of exposure.

### Storage

It is important to securely store keys so that they can be easily and quickly retrieved when needed. Many government regulations and industry standards mandate that certain types of encrypted data be kept for specific lengths of time, in some cases 6 to 7 years.

### Archival/Backup

To safeguard against the loss or unintentional destruction of a key, keys must be replicated and stored in an offsite backup. Mechanisms are required to ensure that backups are synchronized with the primary key store.

### Distribution

Keys must be distributed to the users or systems that will encrypt and decrypt sensitive data. Enterprise key management accomplishes this through automated electronic key distribution over secure network links. Strong multi-factor authentication, including the use of certificates, should be established before key distribution.

### Rotation

When a key is rotated as part of a precautionary routine, it is expired and a new key is created to replace it. Periodic key rotation is part of security

best practices, and is now mandated by the Payment Card Industry (PCI) standard. Keys for archived data are typically not rotated as part of a regular routine, however if there is reason to believe an old key has been compromised, rotation can be manually initiated so that previously encrypted data is decrypted and re-encrypted with a new key.

### Expiration

A key that is expired following a rotation can no longer be used for encryption although it can be used to decrypt data already encrypted.

### Deletion

If keys are stored on vulnerable media and have potentially been compromised, or if a key has been replaced as part of a routine key rotation, it is important to delete the key to prevent it from being used by a malicious party to access encrypted data. All instances of the key, including backups, need to be deleted. Deletion is usually combined with the re-keying of previously encrypted data.

All of the phases in the above key management lifecycle need to be implemented in line with role-based policies that map to the business and security requirements of the enterprise. No one administrator should ever have sufficient permissions to allow him/her to compromise data. In addition, all user, administrator, and system actions at each stage of the lifecycle must be logged and audited.

## Components of Enterprise Key Management

The major components of enterprise key management are shown below. Certain components match closely to discrete 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.

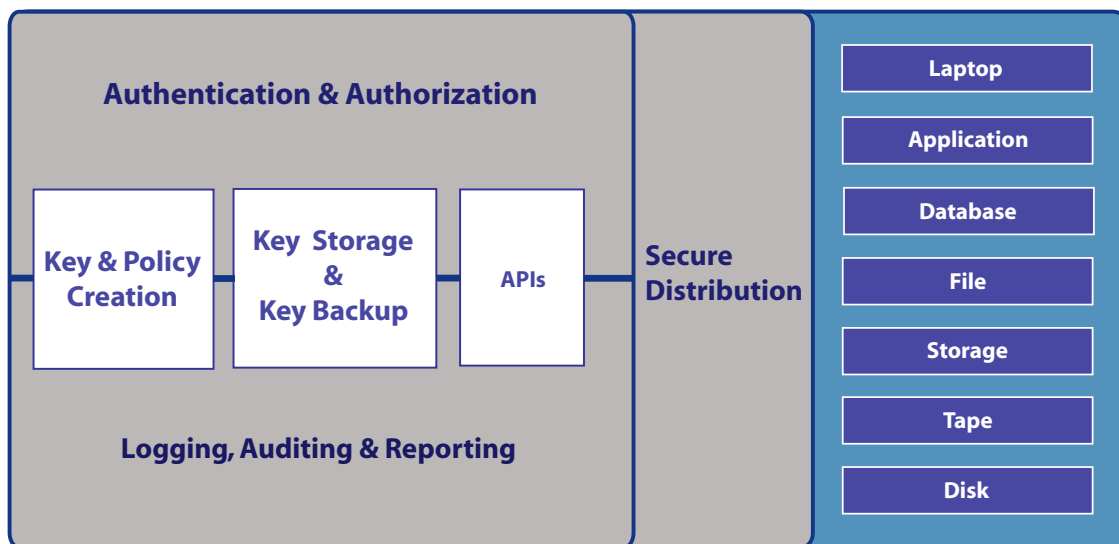


Figure 2: Components of an Enterprise Key Management

## Criteria for Effective Enterprise Key Management

Enterprise key management will often mean balancing a number of different and sometimes apparently contradictory requirements. In general, all of the following criteria must be considered:

### Security:

Administrators, users, partners, and customers need to know they can trust that 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.

The remainder of this section will look at each of these criteria in more detail.

## Security

Security must be maintained at every phase of the key management lifecycle.

### Centralized Management

The first step in ensuring security is to deploy a key management solution that enables administrators to manage keys from a single central authority. A good key management system should also let you know what other devices have copies of a key. Ideally, it would be able to set limits on how long those other devices can keep copies of a given key, although this requires some trust that the other device will actually delete the copy. The central authority may decide to delegate authority to other parts of the organization, but should have the ability to take back control in the event of system abuse or failure. Centralized logging and auditing is also enabled so that all user and administrator actions can be tracked.

Secure key management must also enforce separation of duties. This is required in order to prevent an administrator from having sufficient permissions to carry out an internal attack. For example, one administrator might only be given access to network configuration functions, while another might only be given access to certificate management controls. An enterprise should also be able to use multi-credential techniques to protect against malicious administrators who might attempt to grant themselves unauthorized access to create or delete keys. This level

of granular access control enables organizations to control and closely monitor administration operations, and significantly reduce the risk and exposure from internal attacks.

### Key Storage

The system should also provide a location for key storage that is separate from the location that holds the encrypted data. As mentioned above, storing keys on the same application or database servers that hold sensitive data presents significant security risks when compared to storing keys on purpose built security appliances. When cryptographic keys are stored on unsecured platforms, attackers can gain access to them very quickly. While a system that stores keys and data in the same location may still be compliant with some security standards, clearly encryption is worthless if such a location has been compromised.

There are primarily three ways for securely creating and storing keys:

A hardware security module, or HSM, is the most secure method. An HSM is typically a PCI card specifically designed for securely generating and storing keys. Physical security is the fundamental difference between an HSM and other methods. In the event of physical theft or tampering, keys stored on an HSM are destroyed. To ensure the HSM provides maximum physical security, it must be at least FIPS 140-2 level 3 validated.

Using a hardened security appliance is another method for providing secure key generation and storage. Hardening is the process of securing a system against attackers, this often includes removal of unnecessary accounts and services, encrypting the file system, removing root access, and marking highly sensitive files as read-only. Often an HSM is integrated with the security appliance to provide physical security.

The last method is software-based key management. With this method keys are often encrypted using a hard-coded master key and/or split apart with each piece stored in a different area of the system. Often software-based key management solutions run on systems that have not been hardened, thus making them more susceptible to application layer attacks and malicious administrators. One example is that an administrator could very easily attach a debugger to the key management solution, allowing himself to easily extract the key(s) undetected. Further, particularly in a large enterprise environment, where the application and database servers often number in the hundreds, it becomes increasingly difficult to manage the cryptographic keys residing on these servers. In addition, as the complexity of key management increases, the risk of not backing up a key, or exposing a key, increases exponentially. Software solutions also do not protect against physical attacks.

### 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. In both cases, it is important for the system to remain online as new keys are introduced. Historical information, such as information stored offline on tape, can be encrypted in addition to online data if there is reason to believe the keys have been compromised.

### 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, including RSA 2048 and AES 256.

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.

There also needs to be the option to protect data and keys in transit using SSL or another secure transport technology.

### Authentication

It is important to require mutual authentication between a key management solution and systems requesting keys. Without mutual authentication it is possible for an attacker to execute a man-in-the-middle attack. One way to address this is to require a password and username and a certificate. For additional security, the key management solution can access the client user name from the certificate. That user name can be compared against the user name provided in the authentication request. If the user names match up and the password provided is correct, then the user is authenticated. In addition to traditional methods, solutions can also offer ways to restrict access to keys based on the IP address that originated the request.

To facilitate integration into existing environments the key management solution should have the ability to use an LDAP server for authentication. In addition, it is an added convenience and cost saving if the key management solution is able to operate as a certificate authority. This eliminates the cost of working with a third-party certificate authority.

In order to ensure that administrators are promptly advised of any suspicious activity, automatic alerts, such as industry-standard SNMP traps, should be triggered if security thresholds are exceeded.

### Auditing and Logging

Lastly, 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. Some examples of information that should be audited and logged include:

- + Key and policy generation, edits, deletion, etc.
- + Device configuration including name, network, logging, etc.
- + System events for monitoring threshold boundaries and sending alerts
- + Encryption and signature requests.

Enterprise Key Management should provide logs that are crypto-

graphically protected against malicious modification. For example a software solution running on the same host that's using the keys and logging to a plain file would allow an attacker who can compromise the box to not only get keys but also modify the logs to cover his tracks

### 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.

In order to assure availability in the event of network or equipment failure, device synchronization or the real-time replication of keys, policy, and configuration data among multiple devices is required.

### 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.

The system must also integrate seamlessly with the existing information and security management systems that are part of the enterprise infrastructure. This includes PKI, identity management, logging, and information lifecycle management (ILM) solutions.

Figure 3, shows a view of the recommended platform architecture:

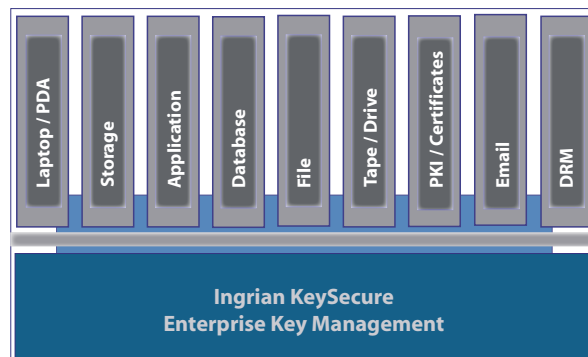


Figure 3: Enterprise Key Management

It is advisable to choose a vendor that has a well-structured partner certification program and has a demonstrated track record for establishing business partnerships and system interoperability with security offerings from other 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 newest 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.

These are illustrated in Figure 4 below:

This example features a company with two data centers: one in San Francisco and another in New York.

All of the key management appliances for this company have been configured for replication. All of the appliances automatically share the same configuration for keys, groups, users, and authentication policies. This gives each of the appliances sufficient information to backup any of the others.

Load balancing is a client-side feature that enables a client to balance its load, typically in round-robin fashion, between multiple appliances. In this case, each of the two data centers shares its load between the appliances that are in the same geographic location. Each of these groups is configured as a load balancing group.

To provide recovery in the event of a network or system failure, a system administrator configures a second load balancing group as a backup tier that can take over in the event that the primary load balancing group (or tier) is disabled. Health-checking is used to continually monitor the status of all appliances in the system to determine when recovery is required. This example shows just two tiers, a primary in San Francisco and a secondary in New York, however there should be the capability of setting up a tertiary tier if desired.

Having capabilities for replication, load-balancing, and recovery provides the ability to configure a fault tolerant architecture that ensures service will continue, even in the event of multiple network or equipment failures.

## Enterprise Key Management Architectures

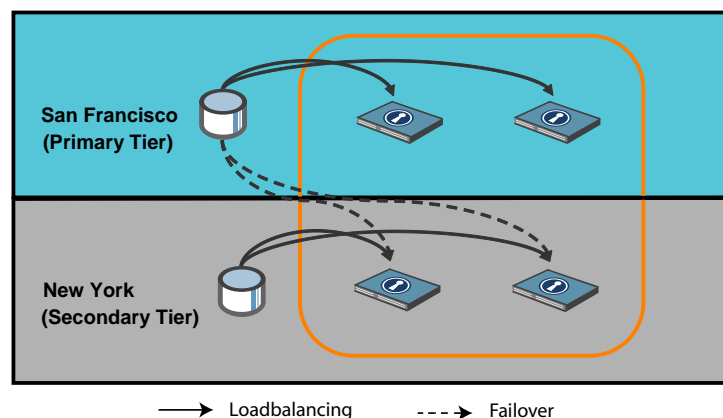
There are two classic types of architectures that could be applied to key management:

### Centralized:

in which the administrator has centralized control over every part of the key management lifecycle

- + Advantages: tight control, efficient centralized audit and logging

Figure 4: Configuring Multiple Key Management Appliances for System Availability



### De-centralized:

for enterprises that are geographically dispersed, 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.

An example of such an architecture using Ingrian Networks' Enterprise Key Management is illustrated below in Figure 5..

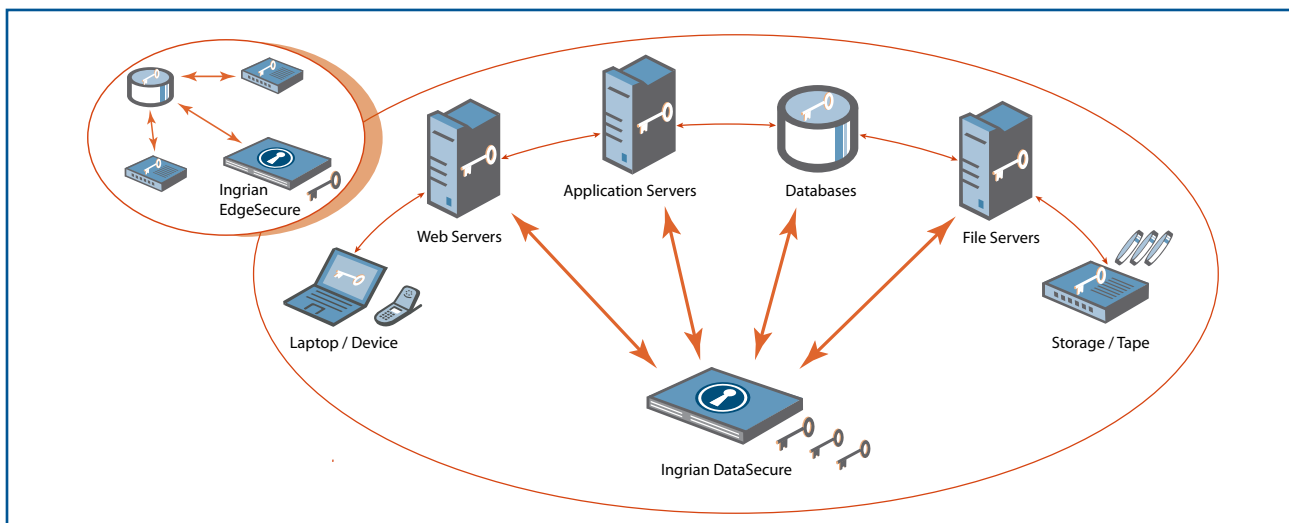


Figure 5: Enterprise Key Management Architecture

## 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 Ingrian Networks

Ingrian Networks offers a solution that brings unparalleled cost effectiveness, security, and control to enterprise key management. The Ingrian platform features secure centralized management, highly granular control and comprehensive auditing and logging using an integrated, appliance-based approach that significantly reduces maintenance costs. Ingrian 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, Ingrian 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 Ingrian, organizations gain the ability to leverage a common enterprise key management architecture that supports heterogeneous enterprise environments regardless of size or complexity.

---

**ABOUT INGRIAN NETWORKS:** Ingrian Networks brings complete data privacy to the enterprise. With Ingrian DataSecure Platforms, organizations can protect critical data from both internal and external threats, and ensure compliance with legislative and policy mandates for security. DataSecure features a dedicated security appliance and specialized software that enables organizations to encrypt critical data in applications and databases. With its capabilities for granular encryption, seamless integration, and centralized security management, DataSecure enables organizations to guard against a range of security threats, with unparalleled ease and cost effectiveness. Ingrian is a privately held company backed by such investors as Globespan Capital Partners (formerly JAFCO Ventures), Prism VentureWorks, HighBAR Ventures, and Partech International. For more information, visit [www.ingrian.com](http://www.ingrian.com).

---

Ingrian Networks Inc.  
350 Convention Way  
Redwood City, CA 94063  
650.261.2400  
866.INGRIAN  
[www.ingrian.com](http://www.ingrian.com)