

BITS

FINANCIAL SERVICES
R O U N D T A B L E

Enterprise Key Management

**A Publication of the
BITS Security Working Group**

May 2008

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
INTRODUCTION	4
Importance of Key Management.....	4
Scope	4
Audience	5
ENTERPRISE KEY MANAGEMENT BEST PRACTICES	6
Enterprise Key Management Program Critical Success Factors.....	6
Governance and Business Management Oversight	7
Key Management Lifecycle	9
KEY GENERATION	9
KEY DISTRIBUTION	11
KEY USAGE	13
KEY STORAGE	14
KEY STORAGE - OPERATIONAL STORAGE	14
KEY STORAGE - BACKUP STORAGE	15
KEY STORAGE - ARCHIVE STORAGE	15
KEY RECOVERY.....	15
KEY REISSUE.....	16
KEY ESCROW.....	16
KEY RETIREMENT	16
KEY RETIREMENT - KEY REPLACEMENT (ROLLOVER, UPDATE AND RENEWAL)	16
KEY RETIREMENT - KEY DEREGISTRATION	17
KEY RETIREMENT - KEY REVOCATION	17
KEY RETIREMENT - KEY DELETION	18
Password-Based Encryption – Specific Practices	19
ACKNOWLEDGEMENTS	21
APPENDIX I: ENCRYPTION AND KEY MANAGEMENT OVERVIEW	22
APPENDIX II: INDUSTRY STANDARDS & REFERENCES.....	24

EXECUTIVE SUMMARY

Financial institutions recognize the necessity to maintain secure, confidential and lawful treatment of data, including personally identifiable information as defined by the country in which the business is conducted. Encryption is increasingly important as a tool for protecting such data, particularly personally identifiable information from disclosure to unauthorized parties. For encryption to be effectively utilized across large enterprises, the encryption keys must be managed with the similar care given to the confidential data they protect for the duration of their entire lifetime to ensure that they are not easily guessed, disclosed or lost, and so that the data they encrypt can be recovered by authorized individuals.

This paper describes general framework, best practices, and additional considerations regarding key management in the enterprise. It offers high-level definitions and examples of critical components of an enterprise-wide key management system, including key generation, distribution, archival and storage. Appendix One provides an overview of Encryption and Key Management, while Appendix Two provides a list of Industry Standards and References relating to the topics of Encryption and Key Management.

The target audience of this document is primarily security professionals, business managers, risk managers and purchasing managers. This document does not address the specifics of any platform nor of any technical details. As these are best practices, not all may be applicable or practical for all financial institutions. They are offered for consideration as companies build or align their current practices related to key management with the internal risk management and compliance controls, and various industry, government and regulatory guidelines.

INTRODUCTION

Importance of Key Management

Financial institutions recognize the necessity to maintain secure, confidential and lawful treatment of data, including personally identifiable information as defined by the country in which the business is conducted. To meet these obligations to their customers, business partners, employees, and to avoid costly data compromise disclosures, financial institutions are frequently employing cryptographic techniques, such as encryption, in their data protection strategies.

The encryption employed in commercial and open source solutions is used by financial institutions for a variety of purposes:

- Maintaining the privacy of customers' personal and corporate information (confidentiality);
- Preventing data from being altered (data integrity);
- Authenticating users prior to transacting business (authentication);
- Replacing handwritten signatures with the electronic equivalent (transaction signing); and
- Limiting the risk associated with the electronic transactions (non-repudiation).

For encryption to be effective, the encryption keys must be protected against unauthorized disclosure, misuse, alteration or loss. Although a number of encryption techniques in use today have been submitted to the scrutiny of experts via industry standards bodies (e.g., ISO, ANSI, NIST), key management on a large-scale in a complex, multi-purpose IT environment has not received sufficient attention. Improper techniques used for the storage, distribution, archival and retrieval of keys can expose the keys to unauthorized individuals. In turn, this disclosure can lead to compromises of the data the organization is attempting to protect.

The lack of common enterprise-wide encryption key management frameworks, best practices, or interoperable solutions coupled with the increased use of encryption in the enterprise presents a significant technical, operational, administrative and management challenge for financial services companies.

Scope

This document outlines a set of best practices that serve as the starting point for development of a high-level enterprise-centric encryption key management framework of technical, operational, administrative and management processes. As these are best practices, not all may be applicable or practical for all financial institutions. They are offered for consideration as companies build or align their current practices related to key management with the internal risk management and compliance controls, and various industry, government and regulatory guidelines.

The initial focus of this effort is on internal key management needs and requirements of enterprises to protect the confidentiality and integrity of data and informational assets they maintain internally. Thus, the scope will not include interactions between 'individuals'

/consumers and enterprises (i.e., user's public/private key pairs) and specialized retail payment key management (e.g., Visa/MasterCard, ATM).

Audience

The target audience of this document is primarily security professionals, business managers, risk managers and purchasing managers. This document does not address the specifics of any platform nor of any technical details. Rather, it provides generic models from which to develop working processes. These reference processes are presented for businesses to use as they develop key management processes and procedures specific to their platforms, applications and requirements.

ENTERPRISE KEY MANAGEMENT BEST PRACTICES

The control of cryptographic keys is critical to the integrity of cryptographic systems. Commercial products do not always address all aspects of the key management lifecycle. As a result, businesses are forced to supplement commercial products with additional technical solutions or manual processes to fill the gaps in the lifecycle management. The additional effort of ‘supplementing’ commercial products results in increased cost and complexity of the data protection efforts.

Enterprise Key Management Program Critical Success Factors

To ensure effective and efficient deployment of key management across the enterprise, an *Enterprise Key Management Program* should be developed and maintained. Such a program should consist of the following elements:

- Governance and Business Management Oversight
 - Meet business, regulatory and legal requirements
 - Define, maintain and enforce policies, standards and common practices
- Well Defined Key Management Lifecycle
 - Key Generation
 - Key Distribution
 - Key Usage
 - Key Storage
 - Key Storage - Operational Storage
 - Key Storage - Backup Storage
 - Key Storage - Archive Storage
 - Key Recovery
 - Key Reissue
 - Key Escrow
 - Key Retirement
 - Key Retirement - Key Replacement (Rollover, Update and Renewal)
 - Key Retirement - Key Deregistration
 - Key Retirement - Key Revocation
 - Key Retirement - Key Deletion

Constructed effectively, a good key management program can assist in accomplishing the following:

- Improve usability and effectiveness of key and key usage
- Increase reliability and efficiency of key structure and key implementation
- Reduce costs by leveraging common infrastructure and administrative processes
- Reduce complexity and improve transparency by re-using well-defined processes and interfaces
- Automate manual steps to reduce human error and improve consistency
- Support a variety of keys consumed by a variety of encryption/decryption processes delivered via commercial, open-source and customer-developed applications on multiple platforms
- Allow for segregation of key management from encryption/decryption operations

- Improve transparency by aligning and integrating with the business processes
- Provide evidence of having implemented sound and secure practices

Governance and Business Management Oversight

Compliance with Enterprise Policies, Standards and Guidelines. Use of specific encryption and key management algorithms, modes of operation, key length, protocols and other implementation aspects of encryption processes should be prescribed by, and in compliance with, the enterprise's policies, standards and guidelines.

If a witnessing of certain activities such as creation or destruction of 'master keys' is required, the necessary processes should be established and documented in accordance with the governing guidelines to ensure correctness, reliability and sound security. The enterprise is accountable for assignment and fulfillment of the 'witness' roles to appropriate individuals.

Compliance with Sovereign Government and Regulatory Restrictions. As part of the compliance review, risk managers should pay special attention to the applicability and impact of various regulatory and sovereign government restrictions related to import, export and use of encryption technology (including disclosure to appropriate agencies). In particular, organizations engaging in global businesses should be aware that there are countries that require the use of weak encryption, as well as those that forbid encryption.

Data Classification of the Keys. Encryption keys should be classified in accordance with the enterprise's 'Information Classification' practices. Typically, encryption keys are classified at the enterprise's most confidential level of classification for data, and access to such data must be controlled in compliance with the enterprise information security practices for protection of such classified data from unauthorized disclosure during use and storage. Generally, access to the keys should be strictly limited to those who have a need-to-know.

Availability and Support. The business continuity plans should include procedures to ensure availability of key management services, including cryptographic system, keying material, and other related services.

Recovery of Encrypted Data. Procedures should be established and documented to ensure that all keying material is properly stored for key recovery, or that alternatives exist to recover encrypted data to its original readable version. The recovery procedures and processes should be tested periodically under appropriate control and accountability (assume the worst-case scenario).

Training and Awareness. All end-users, system and security administrators, risk managers, and other personnel that are expected to interact with the applications and associated processes utilizing encryption and key management as part of the business activity should be provided appropriate training commensurate with their use of the application/processes.

Automation. Use of automated encryption and key management systems and processes is preferred whenever such facilities are available. Properly implemented automated systems

reduce human error, increase efficiency and effectiveness, enhance audit tracking and the ability to provide evidence of activities should it be required.

Separation of Duties. The design of the duties assignments associated with key management should be subject to a risk assessment/analysis process. Generally, for staff that manage keys across the enterprise (i.e., manage the enterprise key management system), the key management systems and applications using encryption keys should be designed such that no single person has full knowledge of, or access to, encryption keys. This can be achieved by carefully planning activities performed within the enterprise and assigning roles and responsibilities so that important activities are not performed by the same individual (e.g., requesting and approving key disclosure). When enterprises consider the management of keys associated with a single application/system, applying this same precept (i.e., not vesting full knowledge in a single person) may be more operationally difficult. Enterprises are encouraged, however, to use their risk assessment processes to determine if the underlying information involved suggests application of the principle. The roles and responsibilities of the assigned personnel should be documented and reviewed periodically.

Separation of Production and Non-Production Usage. Similar to the general security practice of restricting the use of Production data in Non-Production environments, all keys and associated materials used in the Production environment should not be used in non-Production where the controls may not be adequate. For example, the same encryption key used in a Production environment should not be used in non-Production (e.g., UAT, Dev, SIT, etc).

Business Management Approval. The use of encryption and key management tools and products prior to appropriate authorization from a business manager, or other appropriately designated individual within the enterprise (e.g., information asset owners), should be restricted. The business manager's authorization, combined with careful planning, will prevent enterprises from potential data recovery or compliance issues. The business manager should work in tandem with the appropriate risk manager to ensure management, operational, technical and compliance aspects of the solutions are considered prior to the approval.

Document Decisions and Changes. Considerations evaluated during critical decisions should be documented as part of the management decisions. Similarly, all changes impacting technical, operational, administrative or business use of the keys and associated key management system should be carefully reviewed and documented (ideally, as part of the enterprise change management process).

Functional Organizational Placement. With regard to the governance of the key management process, there is potentially another consideration for those organizations that have already commenced the use of encryption, but have not yet established strong governance processes. That consideration relates to the organizational structure and placement of the key management function. Some organizations choose to centralize this function, while others choose to manage it in a more distributed fashion. The decision as to structure and placement is beyond the scope of this paper, and is largely dependent on each organization's overall operational model. Enterprises should weigh the risks and operational considerations associated with each model in light of the other principles stated in this paper.

Key Management Lifecycle

The Key Management Lifecycle is the collection of processes and procedures required to generate, renew, distribute, revoke and dispose of cryptographic keys. Other lifecycle components include key storage, as well as key backup, archiving, and escrowing. However, the business and security requirements of each application may not necessitate following all of the stages of the key management lifecycle.

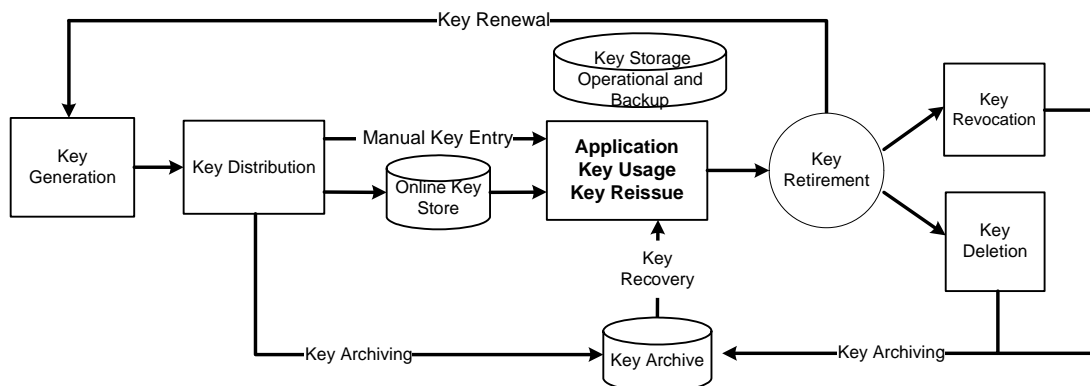


Figure 1: Key Management Lifecycle

KEY GENERATION

Key Generation is the process of creating an encryption key (symmetric encryption) or key pair (asymmetric encryption). Keys should be generated when setting up an application that uses encryption or digital signature. Care must be taken to maintain secrecy of the keys during their generation.

Randomness of Encryption Keys. Whenever encryption is used, the employed keys must be generated by means which are not practically discernable by an adversary, and which will yield keys that are difficult-to-guess. Typically, a random or pseudo-random number generator is used based on industry acceptable standards such as FIPS¹. Generating random numbers is a non-trivial problem and for cryptographic applications that require keys to be generated, care should be taken to ensure that any vulnerabilities in the key generator or key generation algorithm are fixed.

Protection of Encryption Keys. Consider encrypting ‘data encryption keys’ that might otherwise be accessible by unauthorized persons. This means that such keys should not be:

- Stored in the main memory on a multi-user machine unless they are in encrypted or secured form (e.g., temper-resistant security module); or

¹ FIPS - Federal Information Processing Standards are publicly announced standards developed by the U.S. Federal government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.)

- Exposed to a single individual, wherever operationally feasible, in clear text (certain operations such as Key Generation and Key Distribution should be under dual-control²).

Protection of Digital Certificate Root Keys for Certificate Authorities. Cryptographic processes such as digital signatures and digital certificates critically depend on Root Keys (master keys). Therefore, it is imperative that the protection of the Root Keys is commensurate with their criticality to the business activities. Typically, some of the protection elements include: rigorous physical security, dual control, and separation of duties.

- Rigorous physical security generally means storing sensitive information in safes, requiring badges for physical access to equipment, keeping logs of who had access to equipment, etc.
- Dual control, or ‘Four Eyes’ Principle, refers to the use of no less than two people to perform critical acts such as generating Root Keys and/or using a master key, including the Additional Decryption Key used in many S/MIME PKI implementations.
- Separation of duties refers to the use of different people to perform an activity, so that checks and balances are inherent in the workflow.

Validation of Key Components. Once key components³ are generated, it is advisable to ensure that the key components may be re-combined by conducting an encryption/decryption validation test prior to their use. Typically, if there are N components, with a minimum of M to be present to retrieve the key, then the number of tests required is no more than N/M rounded up to the next integer.

Maintenance of Key Meta-Data. A log should be maintained and retained in compliance with the organization’s ‘Information and Data Retention and Destruction’ practices. The log should contain meta-data necessary to track the key usage, ownership and other relevant facts throughout the key’s lifecycle. For certain keys (such as CA root key), paper-based records should be considered in addition to digital logs. Examples of meta-data to maintain include:

- Date of the activity
- Description of the activity (generated components, generated keys, loaded keys, etc.)
- The type of key(s) and key check values
- If generating components, the equipment and/or software used
- If generating/loading keys, the application or device into which they were loaded
- If encrypting a clear key under a master key, the master key name and key check value
- Where the key(s) or component forms are stored

² The purpose of the ‘dual-control’ is to ensure these individuals are supervising and aware of the actions of the other. This creates “mutual surveillance” which aids in compliance and improves the ability to reproduce all critical events.

³ Key Components are a set of two or more unique parts of an encryption key, such that a minimum of two or more is required to unlock protected objects, which are divided in such a manner that no component reveals information useful in attacking the whole key.

- Names of Key Custodians participating
- Signatures of Key Custodians (as the evidence of their witnessing the process and accepting the responsibility of Key Custodian)

Encryption Keys Should Have a Stated Life. Encryption keys should have a stated life and should be changed on or before the stated expiration date. The frequency of key change should be established prior to the key's use and should be based on the organization's practices, including a risk assessment process that would typically consider the following factors:

- Regulatory requirements (i.e., at least annually, see PCI-DSS)
- Operational impact of frequent key changes
- Potential data exposure if compromised

KEY DISTRIBUTION

Key Distribution (sometimes called 'Key Transport') is the process by which keys are securely distributed from where they are generated or stored to where they will be implemented using manual transport methods (e.g., file transfer, key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods.

Secure key distribution is the basis for integrity and trust in any cryptographic system. The goals of any key distribution process should:

- Ensure that the keys are distributed to proper recipients only;
- Ensure that the keys sent are the correct keys for that recipient;
- Ensure that the keys arrive to the proper recipient with confidentiality protections intact;
- Ensure that the keys arrive with integrity intact;
- Ensure that the mechanism of transport provides for secure key import; and
- Ensure proper storage or disposal of the transport medium (especially for distribution of keys or components using paper or removable magnetic media).

Separate Storage for Encryption Keys and Encrypted Data. Encrypted data and the encryption keys used in the encryption process should not be stored on the same storage media. Use of hidden files or hidden directories for the unencrypted storage of these keying materials is highly discouraged (i.e., practicing "Security by Obscurity" is not recommended). Organizations may consider the storage of encryption keys on portable media that is properly protected both physically and logically. A further consideration is to place part of the key on one portable media device and another part of the key on a second; physically and logically giving control of the two devices to different individuals.

Understanding and Acceptance of Key Custodian Responsibilities. Key Distribution activities, roles and responsibilities, notification, escalation and in-transit compromise processes should be documented, reviewed and agreed upon by designated/authorized senders and recipients (i.e., Key Custodians). Typically, Key Custodians should document

their understanding and acceptance of the organizational practices and Key Custodian responsibilities related to their duties prior to commencement of the activity.

Integrity of Encryption Keys During Transport. Keys should be transported in the form of cipher text, or under the principles of split-knowledge and dual-control for clear-text key components. The automated distribution system or manual processes should be implemented with appropriate integrity protection against modification or substitution of key material. Secondary protection measures, such as approved temporary storage mediums, should be cleansed and applicable passphrases changed after each distribution. The default passphrases supplied by vendors should not be used. Enterprises may also consider the use of hash or digital signature controls to assure the integrity of a key upon its arrival.

Recoverability of Encryption Keys During Transport. To ensure availability, keys should be properly archived for recovery in case of temporary storage medium loss during transport. If requested, a disposal of the keys should be executed upon the recipient's positive receipt acknowledgement (see [Key Deletion](#)).

Secure Distribution of Symmetric Keys (Out-of-Band Communication). The information protected with encryption should be transmitted over a different communication channel than the keys used to govern the encryption process, to raise the level of effort for an attacker. Typically, this means that keys should not be sent or stored on the same media transporting the encrypted information.

Secure Distribution of Symmetric Keys (In Clear Text). If transported in clear text form, key components (usually two or more) should be sent to separate, authorized recipients (i.e., designated Key Custodians) via separated delivery methods, such as different courier service firms or the same courier on different delivery dates. Special care should be taken to ensure that deliveries of the key components are not converged to a single individual at the same time, such as an organization's mailroom. Typically, special pre-numbered, opaque temper-evident envelopes are used. The number of the envelope is communicated to the recipient by another trusted communication channel (phone, fax, email, etc.). Upon receipt of the item, the recipient should inspect the envelope for tampering, verify the serial number on the envelope, and communicate this information back to the sender.

Secure Distribution of Asymmetric Keys. Asymmetric public keys may be sent through a medium that offers no security, however, a secure medium should be used to validate the key using fingerprints or hashes prior to their use via another trusted, out-of-band channel (e.g., snail mail, SMS, etc).

Supervision of Encryption Keys During Physical Transport. Any key components should be at all times during its transport, conveyance or movement between any two organizational entities:

- Under the continuous supervision of a person with authorized access to this component or be monitored/tracked by such a person if being transported by a third party courier;

- Locked in a security container (including temper-evident packaging) in such a way that it can be obtained only by a person with authorized access;
- Entered into a temper-evident/temper-resistant security module; and
- As noted previously, if using a third party to transport the key, the key components associated with the key (e.g., passphrase necessary to unlock the key) should be transported separately.

Notification and Escalation. The transport method should include delivery to a specific, named recipient (e.g., designated Key Custodian) and require notification to the recipient that a component is coming. The named recipient should visually inspect the delivered materials for temper-evidence and provide a positive receipt acknowledgement to confirm a non-tampered delivery using returned receipt to the sender, phone, email, etc. If there is evidence of tampering in transit, the key component should not be used and the established notification process should be followed. If the transported key and associated materials are incomplete, the recipient should notify the sender of the problem and send the materials back to the sender. Incomplete materials should not be accepted.

KEY USAGE

Key Usage describes the need of the target applications and systems to follow established enterprise guidelines and procedures in order to maintain the security and integrity of the keys.

Use of Separate Keys for Each Cryptographic Function. Separate keys should be used for encryption, message authentication and/or digital signatures. The intention is to prevent an adversary who gains possession of one key from compromising multiple functions such as encryption and digital signature systems. For example, a key used as the 'key encryption key' should not be used for any other purpose (such as encryption of data).

Validation of Decryption of Encrypted Data. The application performing data encryption should validate that the encryption process is able to recover encrypted data (cipher text) to its original readable version (non-encrypted) prior to placing an application into production. This is typically done during the development and Quality Assurance processes and as part of User Acceptance Testing. This validation detects any malfunction in the encryption process early on, thus assures recovery of the encrypted data. Typically, this involves encrypting the data, then decrypting it, and then comparing the result with the original readable version of the data. In addition, if the enterprise modifies the application or the underlying data structure, it should retest the encryption process. Although this can have a high performance impact, businesses should consider adopting validation of data before committing the change as part of their operating procedure (either partially or completely depending on their tolerance to risk). Some organizations also test the decryption process prior to deleting/discarding the data, though given the high costs of this process, organizations should base their decision to do so upon a risk assessment of the need.

Secure Use of Private Keys in Clustered Environments. The application that requires the use of the same private key in a distributed/clustered environment should protect each

instance of the same key (see [Operational Storage](#) section). Each instance of the key should have its own unique meta-data associated with it to uniquely identify that instance wherever possible with transparency to the clustered application. For example, applications may either use the same digital certificate/private key copied to multiple servers in the cluster, or have each server instance in the cluster use a unique digital certificate (same keys and common name with slight variance in the domain name).

KEY STORAGE

Key Storage defines different and important functions for data management of cryptographic key material. The proper use of these functions depends on the key type, protection requirements and lifecycle stage. Generally, the functions are described as:

- Operational storage
- Backup storage
- Archive storage

When keys are required for operational use, the keys are acquired from operational storage when not present in active memory. If the key in active memory or operational storage is lost or corrupted, the key may be recovered from backup storage. After the end of a key's active life (i.e., cryptoperiod), the key may be recovered from archival storage. Certain key types, such as PIN keys and master keys, are required to always be stored in physical hardware and never resident in a software system, including backup and archive systems.

Key Storage - Operational Storage

While, as stated earlier, the preference would be to store keys separately from the data they encrypt, at times application system design may require immediate availability to the keys by an authorized application. In those cases, a key may need to be stored for normal operations during the key's active lifetime for use in encrypting and decrypting information in a location where the application or encrypted data resides. Typically, operational storage occurs on the device that uses the key, such as encryption key store or key ring on the local hard disk of a server, or a hardware storage module attached to a server or directly connected to a network. Storing the active key in operational storage allows quick access to the key in the event that the system is restarted or connections must be torn down and re-established.

Protect Encryption Keys in Storage. 'Data encryption keys' stored in an "Operational Storage" scenario should be subject to the various controls mentioned in the "[Governance and Business Management Oversight](#)" section of this paper. In addition, and in particular if the key storage is a database, the database administrator should not have access to the keys in the clear text form. In case of an administrator stealing a copy of the database, s/he would not be able to use them to read encryption data. Regardless of the media, the storage media must be protected by strong physical and logical security such as dual control and rigorous access logs. In addition, the keys should not be stored in the following manner:

- Write key values into the startup instructions or computer code
- Write key values in the procedures manuals

Regular Inventory and Integrity Inspection. An inventory of the keys should be taken at regular intervals to ensure that the key-related contents of the storage media remain accurate; integrity remains uncompromised, and the key-related information remains in good condition.

Key Storage - Backup Storage

The backup of keys on an independent, secure media is typically done to provide a mechanism for enterprises to recover key data in case of data loss or corruption of the operational storage. However, not all keys should be backed up as their intended use/purpose may be undermined. Typically, for example, keys used for digital signature should not be backed up so as not to compromise the ‘non-repudiation’ property. The final determination for backup of keys should be made in the context of the application’s use of the key.

Key Storage - Archive Storage

A Key Archive is a repository containing keys of historical interest (i.e., keys enabling a business to recover old encrypted data). In short, backup addresses the challenges of data management for today, whereas archive storage addresses the data management challenges of tomorrow. Typically, archived data is stored separately from active data in operational storage. As with backup storage, not all keys need to be archived. The control principles in the [“Governance and Business Management Oversight”](#) section of this paper apply to the storage of archived keys as well, including segregation of keys from the underlying data and segregation of duties.

KEY RECOVERY

Key Recovery is the process of retrieving keys from backup or archive storage. Key recovery is a broad term that may apply to several different key recovery techniques which result in the recovery of a key and other information associated with that key. Examples of when Key Recovery processes are used include:

- Loss or corruption of the media upon which keys are stored
- Decrypting old encrypted data, such as that on an encrypted backup tape
- Lost smart cards or tokens that contain keys or key components
- Forgotten passwords that control access to keys

Understanding and Preventing Compromise During Key Recovery. Administrative procedures for executing key recovery should be well-documented and enforced, including distinct treatment of ‘normal’ and ‘emergency’ recovery procedures. Typically, the recovery planning should include an impact assessment to determine the potential impact to the organization should the recovered key be compromised. For example, the process for recovery of the master key used by the organization’s Certificate Authority for authentication may negatively impact the entire user population and undermine the transactions which had relied on the infrastructure to-date.

Key Recovery from Operational Storage. Since the keys are active and accessible to registered users of the system, the keys should only be re-distributed to the requesting user

should the original instance of the keys become inaccessible, lost or corrupted. For example, the keys are re-issued from Operational Storage to the authorized encryption sub-system in the event a sub-system requires a restart and its memory cleared.

KEY REISSUE

Key reissue is a process of making existing keys available to an alternate application or server other than the original application or server, by creating a new key entity. This should not be confused with key recovery from a backup or an archive since the object of the key recovery is to make keys available to the original application/server again. While these key entities have an identical cryptographic keying material element, records of the new usage should be maintained either via the key record meta-data (which may be different as it reflects the affiliation with different applications/servers) or other methods such as key management logs.

KEY ESCROW

Key Escrow is the process of an organization depositing the keys for storage, maintenance and recovery on behalf of another organization (i.e., similar to Software Escrow services offered by Iron Mountain). Typically, the Key Escrow process is relevant in the outsourcing arrangements known as ‘white-label’ or ‘private-label,’ where a service provider acts on behalf of the customer organization and may be required to escrow the keys should the customer want to change service providers. For example, the customer organization may want to have the keys recovered, stored and maintained by another service provider as part of changes in the outsourcing arrangements, while maintaining the ability to recover the previously encrypted data.

Avoid Key Escrow if the Need for It Does Not Exist. In the typical business environments where the need for Key Escrow does not exist, the cost and complexity should be avoided. If Key Escrow is necessary, its purpose and operations should be well-documented and tested. Distinctions between Key Escrow and Key Archival should be made clear.

Control of Key Escrow. Where Key Escrow is required, the organization accountable for the keys should retain controls of the keys directly, contractually or via other means, at all times. It should also make the decision on whether control over storage and maintenance of the keys in the escrow repository should remain with itself, its service provider, or another trusted third party. Enterprises should assure that any third party holding keys in escrow exercises the same level of control over those keys that would be expected within the enterprise. The enterprise should validate the third party’s control environment using the same controls it uses for any third party responsible for housing its most sensitive data.

KEY RETIREMENT

Key Retirement - Key Replacement (Rollover, Update and Renewal)

Commensurate with the enterprise’s data classification and usage, the key must be changed on a periodic basis. The final determination of the appropriate frequency of change must follow established enterprise guidelines and procedures. The key’s end of life is usually

defined at the time of key generation. To allow the applications relying on the keys to continue their operations, the keys need to be replaced on or prior to the key's stated end of life through a 'rollover' process that should be well documented. When keys reach their scheduled end of life, they should no longer be used unless for the purpose of old encrypted data recovery. Businesses with data retention requirements must archive keys beyond their scheduled end of life to allow for decryption of legacy data until the data retention requirements have lapsed.

Keys can be replaced using a number of techniques. A new key can be generated and distributed using the [Key Generation](#) and [Key Distribution](#) steps outlined above to replace the old key. Alternatively, some encryption applications include capabilities whereby the current key or a master key is modified to securely create a new key.

Key Retirement - Key Deregistration

Key Deregistration is a process of taking keys out of operational storage/use when it reaches its scheduled end of life. Deregistration is a scheduled process that takes place when there are no further requirements for retaining keys or its association with an entity.

Key Retirement - Key Revocation

Key Revocation is the process of containing the risk of additional exposure once a key is compromised, disclosed, misused or when there is a reasonable cause to suspect compromise. Affected keys must be revoked in a proper and timely fashion to limit the negative impact on the system or encrypted data. The process should include removing all instances of affected keys out of operational storage and usage, and replacing them with a new set of keys to allow continuation of business operations. Note that it is possible the enterprise will need to decrypt all data encrypted with the old key, then re-encrypt it with a new key (after making sure the system is safe) before removing the old key(s). Minimally, the enterprise should validate if this is necessary before changing the keys so as not to lose all ability to decrypt the old data.

Document, Test and Maintain Compromise Management Plan. A procedure for determining how to handle a key compromise situation must be developed and communicated to all business and key management staff that would be involved in a key compromise and key replacement situation. For example, the plan should include:

- Names and contact information for key personnel, such as the business organization management, business owners of the key, Key Managers, Key Holders, business line organization management, computer operations, technical support, etc.
- Contact information via a calling-tree for participants
- Roles and responsibilities of participants
- Keys that could be affected (the hierarchy of keys: master vs. working keys)
- The risk analysis process and criteria for determining when a compromise has occurred
- Replacement keys and process for implementing them (whether reserved keys, which are generated in advance but not in operational usage, should be used)

Establish and Maintain Notification Process. As part of the Compromise Management Procedure, the impacted applications, their owners and other parties may need to be notified as part of the Key Revocation process. Therefore, the necessary notification mechanisms should be established and accurate meta-data maintained. If the compromised key is shared with an external party; that party should be informed of the key compromise and they, in turn, need to do what is required to remove that key from their environment. These steps should be well documented and reinforced with contractual obligations with the third party as necessary.

Assess Impact as Part of Incident Response. The risk and impact should be analyzed as part of the established incident response process. Inventory management and accuracy of meta-data are important elements in the assessment process. The decision to change the keys and/or re-encrypt the previously encrypted data under the new key should be made as part of the Incident Response.

Do Not Delete the Keys. Key Revocation should not include key deletion as revoked keys may need to be used for forensic evidence purposes or to recover the encrypted data. However, once there is no existing information encrypted under the compromised key, that key should be destroyed (see [Key Deletion](#) section).

Key Retirement - Key Deletion

Key Deletion is the process of permanent removal of keys from all systems for all intended purposes. This includes operational stores, backup stores and archive stores. Once removed, any data that has been encrypted with the deleted key may not be recovered. Therefore, organizations are advised to undertake Key Deletion with extreme caution.

Destruction of Encryption Key Materials. All instance of keys and supplies used for the generation, distribution and storage of keys such as carbon copies, printer ribbons and the like should be destroyed by pulping, shredding, burning or other approved destruction methods when no longer needed.

Retention of Encryption Key Meta-Data. The destruction should be recorded and stored as documentary evidence of the destruction in compliance with organization's data retention policies. For sensitive keys, the maintenance of proper paper-based records should be considered in addition to digital logs.

Password-Based Encryption – Specific Practices

Today, password-based encryption (or passphrase⁴) is one of the most widely used and available technologies included in the software used by regular users on a daily basis, such as Microsoft Word, Excel, PowerPoint, WinZip, Adobe, PGP, GnuPG, and OpenSSL. Because the users expect to be able to invoke options such as “Read-only Password” as needed from time to time, organizations should provide guidance to their users in the form of corporate security policies or guidelines. Furthermore, organizations are encouraged to perform awareness training and manual audits of the user population from time to time to ensure that the recommended procedures are being followed.

Use of User-Provided Passwords or Keys

Use of user-provided passwords or keys should be reviewed and authorized in the context of the intended usage and adequacy of the mitigating controls (see [Password-Based Encryption](#) section). The common risk scenario which should be considered include:

- Password or keys are lost
- Password or keys are forgotten
- Password or keys are deliberately withheld

Generally, users should not be able to exclusively control access to an enterprise’s encrypted data (no separation of duties exists). The review of the intended use will assist business managers in making appropriate decisions based on the potential risk, available alternatives, mitigating controls and costs.

Importance of Passphrase

In the Password-Based Encryption methods, the single most important element of your key is the passphrase (i.e., if you have the passphrase to an encrypted WinZip file you will be able to access the encrypted data).

Use of Passphrase

The passphrase should be used even if the application or tool allows for a ‘no-passphrase’ option (without a passphrase, anyone who gets hold of the encrypted data will automatically gain access to the unencrypted version of it as well).

Uniqueness of Passphrase

The passphrase should be unique; it should be different from any other passphrases used, especially any login passwords for computer, network account, encrypted disks, etc.

Structure of Passphrase

The passphrase should be sufficiently long, for example, a minimum of 8, and optimally 15-20, characters, and use a combination of alphabetic (abc...xyz) and numeric (123...0) characters, as well as punctuation (\$,!,-,!,=,+ , etc).

⁴ Passphrase: a sequence of words or other text often used to control both access to, and operation of, cryptographic programs and systems. A passphrase is similar to a password in usage, but is generally longer for added security.

Make Passphrase Hard to Guess

The passphrase should be hard to guess. Avoid the use of common or famous quotations to avoid automated computer matching, and refrain from using easily guessed passphrases such as names, birthdays, Social Security numbers, addresses, telephone numbers, etc.

Make Passphrase Easy to Remember

The passphrase should be easy for original user to remember, but very hard for others to guess (i.e. do not use your birthday or your spouse's name, or your automobiles license plate number). A good technique is to construct a passphrase you can remember from a combination of letters, numbers and punctuation.

Storage of Passphrase

The passphrase should not be written down, hard-coded into applications/scripts, or shared with others without appropriate mitigating controls. In situations requiring long-term storage of the passphrase, the 'key splitting' technique should be used (e.g., break up the passphrase into a number of parts and store each piece independent of each other under the care of independent entities). To reconstruct the original passphrase, a recombination of all X parts would be necessary. Alternatively, a dual-control to the storage media where the original passphrase is stored would be required to access it.

Disclosure of Passphrase

Take appropriate measures to ensure the passphrase is not disclosed to unauthorized third parties.

ACKNOWLEDGEMENTS

BITS would like to thank the following member participants who contributed to the drafting of this paper, under the leadership of the BITS Security Steering Committee and Working Group:

- Leonid Vayner, JPMorgan Chase & Co.
- Chia-Ling Lee, UBS
- Kathleen Niemeyer, The Bank of New York Mellon Corporation
- Rich Gunzel, Citigroup Inc.

We also thank Ody Lupescu of VeriSign for his review, input and comments.

BITS Staff who contributed to the paper include John Carlson, Paul Smocer, Matt Ribe, John Ingold and Ann Patterson.

APPENDIX I: ENCRYPTION AND KEY MANAGEMENT OVERVIEW

Cryptography Overview

Whenever a business relies on a cryptographic system as the means to achieve its business objectives, the integrity of such a system must be maintained. Processes, procedures and technical solutions must adhere to sound and secure key management best practices in order to assure system integrity.

There are many ways to implement cryptography and many end goals of an implementation. Typical goals of a cryptographic system include:

- data confidentiality;
- data integrity;
- system authentication; and
- digital signing of information.

Due to the complexity of cryptographic functions, only trusted solutions from reputable security vendors should be used. Technology implementation, infrastructure impact analysis, corporate standards, policy, business and legal compliance remain the responsibility of the business.

Much of the technology used in encryption is effectively managed by vendor offerings. The business should identify a product that meets its business requirements and is compliant with their corporate standards. After identifying a product, implementing an encryption solution becomes primarily an exercise in policy and procedure. Where the vendor product is deficient or inadequate in meeting enterprise key management best practices, workarounds or manual procedures will have to be deployed.

Type of Encryption

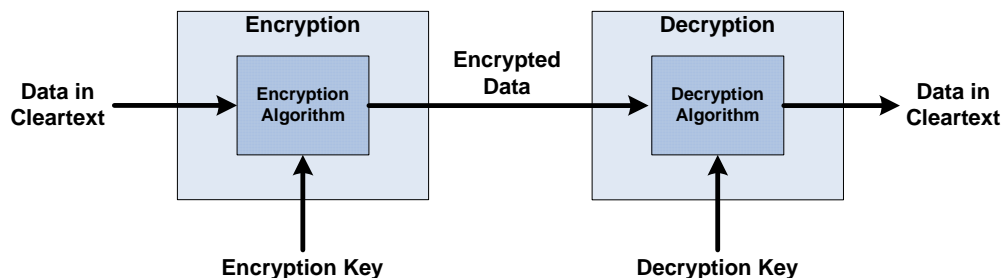


Figure 2: Encryption and Decryption

Encryption is the process of transforming original data into cipher text to prevent unauthorized persons from reading the original data, and has two primary components: the

encryption algorithm and the key. The algorithm is the mathematical method for encryption. A key is applied to encrypt and decrypt the data. There are two basic techniques for encrypting information: symmetric encryption and asymmetric encryption (also called public key encryption).

Symmetric Encryption

When using symmetric key algorithms, the same key is used for encryption and decryption. To provide confidentiality, this key needs to be kept secret. Therefore, maintaining the integrity of the key during distribution, storage and operations is extremely important. Typically, symmetric algorithms operate faster than their asymmetric counterparts.

Examples of symmetric algorithms include: AES, TDES, DES, BlowFish, TwoFish, etc. Typical application usage includes: laptop/ whole-disk encryption, USB memory stick encryption, backup tape encryption, VPN, ATM 'PIN' encryption, etc.

Asymmetric Encryption

The alternative to symmetric encryption is asymmetric encryption. Asymmetric encryption uses a pair of asymmetric encryption keys (complementary public and private key pair), where the public key is used for encryption and the private key for decryption. The key pair owner holds the private key, which is kept secret. The public key is distributed to all who wish to exchange encrypted data with the private key owner. Anybody having the public key is able to send encrypted data to the owner of the private key. Mathematical properties of the encryption algorithm ensure that data encrypted with the public key can only be decrypted by the associated private key.

Examples of asymmetric algorithms include: RSA, Elliptic Curve, Diffie Hellman (DH), etc. Typical application usage includes: secure emails with S/MIME or PGP/GPG, secure remote access with SSH, HTTPS, secure file transfer over SSL/TLS, etc.

Digital Certificates

Digital Certificates are digital documents that bind an identity to a public key. In addition, they may describe usage of the public key, constraints on the key and owning identity, lifetime of the key, as well as who is attesting to the binding. Since Digital Certificates contain public keys, they are a convenient means of exchange for public keys. Typical application usage includes: SSL/TLS certificates passed to a web browsers by a web server, with optional client authentication.

Password-Based Encryption

In Password-Based Encryption, the encryption key is derived from a password that is managed by the end-user. The end-user enters a password, which is used by the software to generate the key to encrypt the target data.

PKCS5 is an example of an asymmetric algorithm. Typical application usage includes: WinZip 9 encryption, Acrobat Writer Secure PDF, PGP self-decrypting archive, etc.

APPENDIX II: INDUSTRY STANDARDS & REFERENCES

ANSI – X9.24, *Retail Financial Services Symmetric Key Management*

BITS Key Considerations for Securing Data in Storage and Transport: Securing Physical Media in Storage, Transport, and for Data Erasure and Destruction, April 2006,
http://www.bitsinfo.org/p_publications.html

Federal Financial Institutions Examination Council (FFIEC): *IT Examination Handbook*, July 2006 (page 57),
http://www.ffiec.gov/ffiecinfbase/booklets/information_security/information_security.pdf

FIPS Publication 197, <http://csrc.nist.gov/encryption/aes/>

IEEE *Security in Storage Working Group* (P1619.3 – work in progress), <http://ieeep1619.wetpaint.com/>

IETF RFC4107: *Guidelines for Cryptographic Key Management*, June 2005,
<http://tools.ietf.org/html/rfc4107>

ISACA *IS Auditing Procedures: Evaluation of Management Control Over Encryption Methodology*, Doc #9, Jan 2005, <http://www.isaca.org>

ISO 11770, <http://www.iso.org>

MAS *Internet Banking Technology Risk Manager Guideline v1.2*, 2003 (sec 4.1.3)

MAS *Security Guidelines for Mobile Banking v1.1*, 2002 (sec 5.2)

NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002

NIST Special Publication 800-57, *Recommendation for Key Management - Part 1*, March 2007 & Part 2, April 2005

NYCE *Network Operating Rules (Best Practices for PIN Encryption)*, 2006

NYCE *Best Practices for PIN Encryption*, 2006,
http://www.nyce.net/pdf/PIN_debit_encryption.pdf

OASIS Enterprise Key Management Infrastructure (EKMI) Technical Committee (work in progress), http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ekmi

PCI Data Security Standard v1.1, Sept 2006, <https://www.PCISecurityStandards.org>

TCG Trusted Storage Key Management Services Subgroup (work in progress),
<https://www.trustedcomputinggroup.org>