SNIA
Advancing storage & information technology

Security Technical Work Group (TWG)

Encryption of Data At-Rest

Step-by-step Checklist

Version 2.0

September 9, 2009

Revision History

Revision	Date	Sections	Originator:	Comments
1.0	8/30/2006	All	Eric Hibbard	Initial SNIA Whitepaper
2.0	3/27/2009	All	Eric Hibbard	Put into SNIA template
2.0	8/28/2009	All	Roger Cummings	Incorporate ballot comments, harmonize with tutorial, add introduction, background & bibliography, update PCI-DSS annex. (Note, Was originally identified in error as Rev 3.0)
2.0	9/08/2009	Cover page, Introduction, Definition of Terms & Acronyms, Brief Encryption Background, Step 7, Author Details	Roger Cummings	Incorporate comments from ballot closing 2009-09-08

Table of Contents

Executive Summary

Public disclosures of data "indiscretions" have become regular enough and embarrassing enough that many organizations are exploring encryption options to simply stay out of the headlines.

However getting the most out of encryption involves much more than purchasing a device with encryption features and connecting it to an existing storage infrastructure. Existing management and control structures will need to evolve, information locations changed, and support is even required from the legal department!

This paper defines a nine-step process that should be performed to effectively implement at-rest data encryption. While not all steps will be needed in all cases, they each merit consideration in every case. The steps are:

1. Understand Drivers
2. Classify the Data Assets
3. Inventory the Data Assets
4. Perform a Data Flow Analysis
5. Choose appropriate Points-of-Encryption
6. Design the Encryption Solution
7. Begin Data Re-Alignment
8. Implement the Encryption Solution
9. Activate Encryption

Introduction

Over the past several years, companies along with their customers and consumers have been subjected to the headaches associated with data compromises or exposures. Whether through malicious attacks against computer systems or inadequate data handling procedures, the financial toll for all parties involved has been significant. With cyber crime surpassing the profitability of trafficking in illegal drugs, governments have been obliged to force public disclosure as well as to levy penalties for some of these data indiscretions.

As preventative measures, many organizations have implemented perimeter-based security strategies with firewalls, sought to control remote users with virtual private networks (VPNs), introduced intrusion detection systems (IDS) to monitor and respond to suspicious network traffic, and deployed multi-layer malware (antivirus) protection mechanisms to limit the introduction of malicious code. However these major enterprise security endeavors have proven inadequate to prevent the unauthorized disclosure of sensitive data. Consequently, many organizations are now faced with a fifth security initiative – data encryption.

Like the technologies listed above, implementing data encryption optimally requires much more than just purchasing a device with encryption features and connecting it to an existing storage infrastructure. The location of the device in the infrastructure needs to be carefully chosen, and arrangements made to provision that location with keying material. The data to be processed needs to be identified, and in some cases its location needs to be changed. Logs need to be created that didn't exist before and requirements for their creation, protection & use agreed.

The main portion of the remainder of this document outlines process that organizations may use to identify their needs for securing data at-rest, and then to implement an encryption approach that is optimal for their situation. The process is decomposed into nine separate steps: each step is then further expanded to include several checklist items. It's recognized that not all items will be relevant in all cases, but they all merit consideration. Before the checklist is described, however, a set of key terms and acronyms is defined, and a brief background to encryption described.

The document also contains three appendices that summarize portions of definition and requirements documents produced by other organizations that are relevant to the process. The definitions summarized are:

- The Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook – Information Security
- The Information Systems Audit and Control Association (ISACA) IS Standards, Guidelines, and Procedures for Auditing and Control Professionals
- The PCI Data Security Standard (PCI DSS) and the related Security Audit Procedures

The summarized requirements are provided for information purposes only, and the complete document should be consulted when defining encryption-related policies, procedures and requirements.

Definition of Terms & Acronyms

Seven key terms that are used throughout this document are formally defined here as follows:

Plaintext: Original information (intelligible) that is used as input to an encryption algorithm (cipher).
Ciphertext: The encrypted (unintelligible) output from an encryption algorithm.
Encryption: The conversion of plaintext to encrypted text with the intent that it only be accessible to authorized users who have the appropriate decryption key.
Cipher: A mathematical algorithm for performing encryption (and the reverse, decryption).
Key: A piece of auxiliary information used by a cipher during the encryption operation.
Data At-Rest: Data that resides in databases, file systems, in other structured storage methods, and on storage media
Data In-Flight: Data that is moving through a network, including wireless transmission

The following acronyms are also used in this document:

CA SB 1386/AB 1950: Two California State Laws relating to privacy that require organizations to notify Californians if their personal information is disclosed during a security breach.
CDP: Continuous Data Protection
DLP: Data Loss Prevention
DR/BC: Disaster Recovery/Business Continuity
EU: European Union
HIPAA: Health Insurance Portability and Accountability Act (USA 1996)
IS: Information Systems
IT: Information Technology
MAC: Message Authentication Code
NAS: Network Attached Storage
OS: Operating System
PCI DSS: PCI Data Security Standard
TCO: Total Cost of Ownership

For more terms related to storage networking and encryption, please refer the SNIA Dictionary (see the Bibliography)

Brief Encryption Background

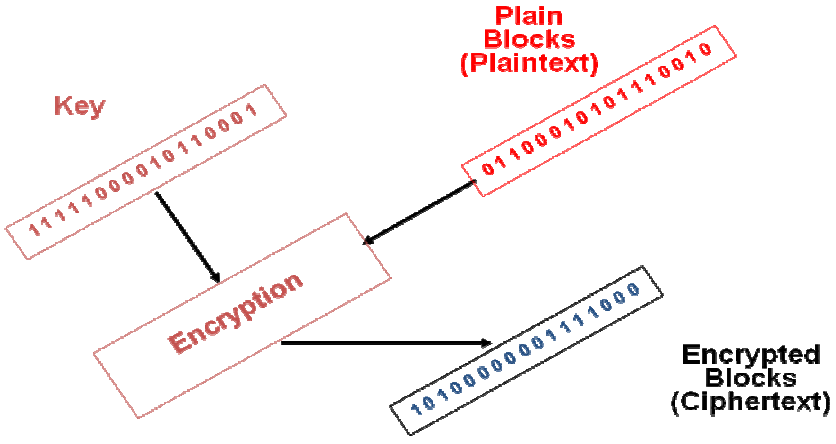
This section provides a brief background on what encryption is and how it has been used throughout history. This is a much-abridged version of a section in a booklet in the SNIA Technical Tutorial Series called “Storage Network Security” (see the Bibliography).

The basics of encryption date to the time of Julius Caesar who, during the Gallic wars, is reputed to have used a simple cipher where each letter of the alphabet was replaced by the letter four places following it in the alphabet (i.e. in the following two lines replace each letter in the top line by the one underneath it):

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
```

This process is formally known as “substitution”, and is one of only two fundamental processes involved in encryption: the other is “transposition” in which the order of the letters in a message is altered.

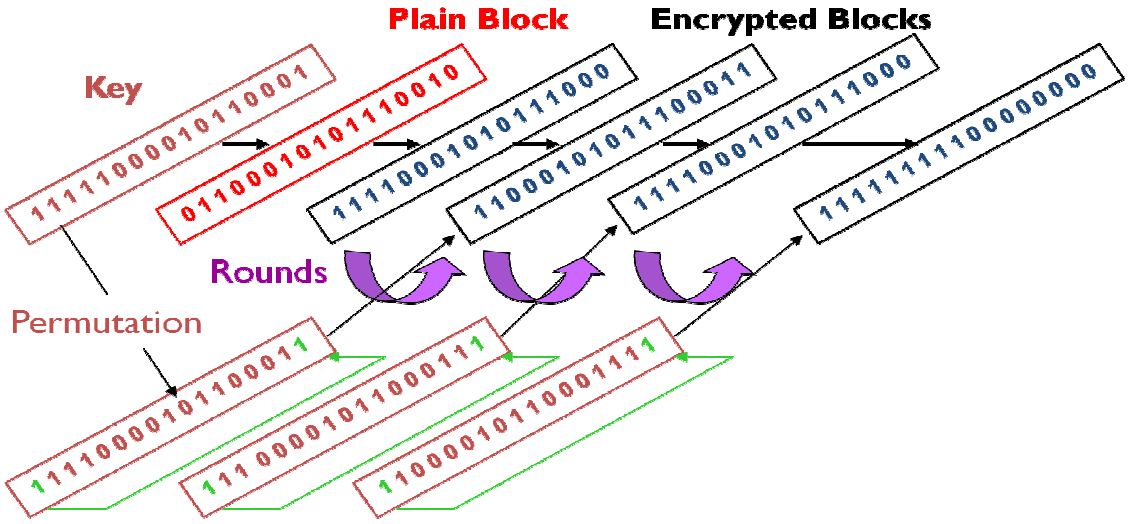
The formal name for the mathematics underlying encryption is “cryptography”, and this is derived from the Greek “cryptos" (hidden) + "graphia" (writing). Formally encryption is a process that accepts two inputs, namely plaintext and a key, and produces a single output, namely ciphertext.



Decryption is therefore the reverse process, in which two inputs, namely ciphertext and a key), produces a single output, namely plaintext.

There is a fundamental principle in cryptography ascribed to Kerckhoff that holds that only the key needs to be secret; the algorithm does NOT need to be secret.

There have arguably been two major advances in cryptography since the time of Caesar. The first of these is mechanization, which makes it practical to perform multiple encryption processes in series for further strength.



Each process is known as a round, and the cryptographic "mode" defines how output of one round becomes input of another.

Note that this mechanization predates computers – several mechanical devices were constructed in the 18th and 19th centuries as cryptographic aids.

The second major advance is asymmetric cryptography. All of the schemes described above were "symmetric" in that the same key was used in both the encryption & decryption processes, and thus the key had to be distributed to both parties who wished to communicate before secure communication could take place – this is a "chicken & egg" problem. In contrast asymmetric cryptography employs two different keys, one Public (open) key and one Private (secret) key. What one encrypts, the other can decrypt, and vice versa. It is not feasible to calculate one key given the other. The first practical scheme developed was the Diffie-Hellman Key Agreement, but it required a number of communication steps, and thus was succeed by the well-known RSA scheme. Note that asymmetric cryptography is also called Public Key Infrastructure (PKI) Cryptography, because a trusted infrastructure is needed to distribute the public keys.

It should be noted in passing that there is another use of cryptography that is separate from encryption and decryption. Hashing does not encrypt data, but provides a transformation used to verify data integrity. The hash algorithm digests data and represents its bits and bit patterns by fixed-size equivalent - a Hash Value – whose size is fixed by the algorithm (e.g. SHA-1 is 20 bytes). Hashes do not require the use of keys, but a related construct called a Message Authentication Code (MAC) uses a hash derived from both data & a secret key. HMAC is the best known of these constructed, and it's defined by the Internet Engineering Task Force (IETF) RFC 2104. A hash may also be used in a "digital signature" scheme.

Checklist

Step #1 – Understand confidentiality drivers

Understanding the reasons for pursuing an encryption strategy is important from the outset. Such a strategy is most effective when it is one component of an overall Information Assurance plan. It's essential to engage executive management in the identification of specific risks to the organization, but to do that effectively the impact of those risks must be expressed in monetary terms. Failure to capture the full set of drivers can result in an inadequate and/or unusable solution.

- ☐ Identify all relevant regulatory and other obligations that impact data security and data privacy (e.g., Sarbanes-Oxley, HIPAA, Payment Card Industry Data Security Standard (PCI DSS), EU Data Privacy, CA SB 1386/AB 1950, etc.)
- ☐ Identify all relevant legal obligations that impact data security (e.g., court orders, contractual obligations, due care, trade secrets, competitively sensitive information, national security, intellectual property, etc.)
- ☐ Identify all relevant executive management concerns (e.g., public image, thwarting and detecting criminal activity, protecting intellectual property) and trace them back to quantifiable obligations and requirements.
- ☐ Review organizational policies associated with data protection and data security (e.g., retention, destruction, privacy/confidentiality, etc.)
- ☐ Review organizational IS/IT strategic plans to identify desired future states with defined data protection and data security dependencies
- ☐ Review recent IS audit results/findings to identify data privacy/confidentiality deficiencies
- ☐ Determine whether compliance or data security requirements serve as the primary need for confidentiality measures
- ☐ Determine the role of monitoring and reporting (auditing)

Step #2 – Classify the data assets

In some instances, it is reasonable to encrypt all of an organization's data; however, a more likely scenario is one in which a subset of the data is encrypted, due to cost constraints, the sheer volume of data, geo-political reasons, etc. In these situations, both the data sensitivity and criticality must be considered.

- ☐ Begin with a small number of coarse classifications
- ☐ Identify the organizational classifications of ***data that has high value to the organization,*** and is therefore worthy of data protection measures (redundancy,

resiliency, business continuity, disaster recovery, continuous data protection (CDP), out-of-region replication, etc.)

- ☐ Identify the organizational classifications of most ***sensitive data*** worthy of data security measures (confidentiality, access control, data integrity, immutability, etc.)
- ☐ Establish the organization's confidentiality priorities by cross-correlating the criticality and sensitivity classifications
- ☐ Determine the organization's ***confidentiality categories*** (e.g., most confidential, competitively sensitive, personally identifiable information or PII, top secret, restricted financial, …, cafeteria menu) to be subjected to encryption measures.

Step #3 – Inventory data assets

Once the encryption drivers are understood and a classification scheme has been established, it is time to chase the data. Specifically, the data associated with each of the confidentiality categories must be identified along with the underlying technology/ media on which it resides.

- ☐ Identify the applications that generate, process, modify, and preserve the data that are to be encrypted
- ☐ Determine which hosts/servers (including flavors of operating systems) that access, use, and store the data
- ☐ Identify the data owners, custodians, stakeholders, and business units having a vested interest in the protection measures and a need to access the data
- ☐ Determine which storage devices are visible to which servers
- ☐ Determine the networks which are used to transport the data
- ☐ Determine which servers might export data (e.g. via NAS interfaces)
- ☐ Determine the geographic locations in which the data may reside
- ☐ Perform a risk assessment (with an eye to unauthorized disclosure or deletion, loss of control etc.) on the identified data and adjust the encryption priorities to reflect findings

Step #4 – Perform data flow analysis

Simply knowing where the data resides is not enough to ensure adequate confidentiality. Often, the data will go through multiple transitory locations before arriving at its final resting point. In addition, the data may be mirrored, replicated, copied, backed up, etc. as part of the organization's data availability/resiliency strategy. Each of these must be considered as part of the encryption approach.

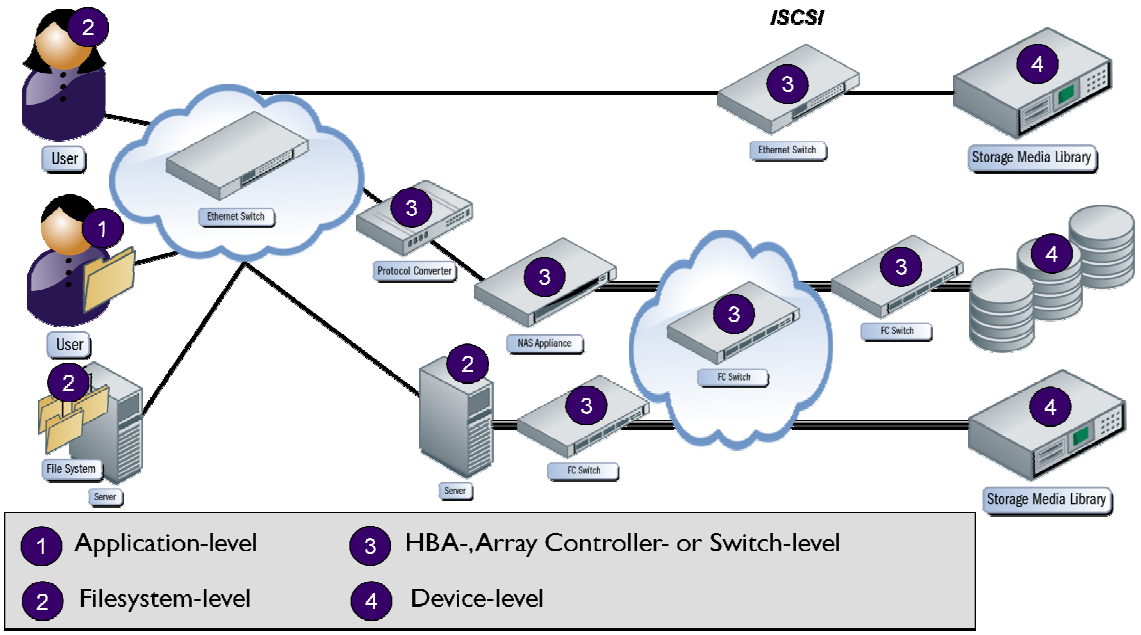
- ☐ For each application associated with data to be encrypted, identify all temporary storage usage (e.g., cache files and temporary workspace) as well as data protection measures (e.g., internal data mirroring).
- ☐ For each host/server associated with data to be encrypted, identify all temporary storage usage (e.g., cache files and temporary filesystems) as well as data protection measures (e.g., data mirroring).
- ☐ Determine the importance and role of mobile systems and storage devices
- ☐ Determine the importance and role of backup/recovery & archive mechanisms, at both local and remote sites
- ☐ Determine the importance and role of Continuous Data Protection (CDP), Data Loss Prevention (DLP), Disaster Recovery/Business Continuity (DR/BC), or other similar mechanisms
- ☐ Determine the importance and role of replication (synchronous and asynchronous) at remote sites for business continuity and disaster recovery
- ☐ Determine the impact of data reduction schemes (e.g. compression, deduplication)

Step #5 – Determine the appropriate Points-Of-Encryption

Eventually, a basic decision has to be made as to where the encryption should be applied. This point-of-encryption is important because it represents the location within the IT infrastructure that the data must be brought to before it is decrypted and usable. A common security perspective is to encrypt as close to the source as possible, as this tends to maximize the protection provided. The following represent common points-of-encryption (see also the figure):

- **Application-level** – under the control of specific application or database; finest granularity of control and maximum insight into the data (type, users, sensitivity)
- **Filesystem-level** – under the control of the OS or OS-level application; control at file-level with insights into the users
- **HBA-, Array Controller-, or Switch-level** – under the control of the network
  - File-based (NAS) – control at the share/filesystem-level (possibly file-level) with moderate insights into the users
  - Block-based – control at the logical volume level with limited insights in the "community of users"[1]
- **Device-level** – under the control of the end-device; control at the logical volume level with limited insights in the "community of users"[1]

[1] The specific user community is unknown, as are their individual access rights. The community is defined by the hosts/servers that have access to the individual logical volumes.



- ☐ Determine the importance of access control (e.g., specific user, workgroup, communities of users, etc.) to be used in conjunction with encryption for the confidentiality categories
- ☐ Determine the granularity needed for the encryption (e.g., fields within a database, files or filesystems, logical units, media, etc.)
- ☐ Determine the importance of In-Flight encryption protection
- ☐ Determine the importance and role of At-Rest encryption measures such as disk or tape media encryption (recognizing that in some cases data must be compressed before encryption)
- ☐ Determine the importance of technology obsolescence, refresh, or upgradeability (e.g., swapout of the crypto modules)
- ☐ Determine the risks to be mitigated by the encryption solution
- ☐ Identify the preferred point-of-encryption (technology neutral) for each confidentiality category, remembering that each point has to be authenticated to be provisioned with keys

Step #6 – Design encryption solution

Systems design can be thought of as the process or art or science of defining the hardware and software architecture, components, modules, interfaces, and data for a computer system to satisfy specified requirements. Designing an encryption solution is no different, but it does require attention to compliance, export controls, and industry standards (e.g., PCI DSS).

- ☐ Develop and document the organization's encryption strategy
- ☐ Develop and document the organization's encryption architecture/framework
- ☐ Determine the importance of long-term (persistent) key management (e.g., centralized versus de-centralized, key import/export, key archival, key escrow services, key integrity, key recovery, etc.)
- ☐ Identify where keys are managed, how they are communicated, who is responsible for the operation and security of key management
- ☐ Determine the importance and role of encryption within the organization's business continuity and/or disaster recovery measures (including plans)
- ☐ Determine the importance of proof-of-encryption measures (as part of compliance audit logging)
- ☐ Determine the criteria used to select the type of encryption/cryptographic algorithms (e.g., widely known & accepted versus banking industry standards)
- ☐ Determine the importance and role of import and export and/or re-export controls on the encryption/cryptographic algorithms selected for use, including end use
- ☐ Set the right expectations for performance/throughput impacts
- ☐ Determine the importance and role of data recovery (decryption) without the primary encryption mechanism
- ☐ Document the specific encryption requirements for the organization's data
- ☐ Document the information to be collected to prove to an auditor (or the organization's legal department) that the media containing the information was correctly encrypted and the key has been under control since the media was created, and how the authenticity & integrity of that information is to be proven
- ☐ Validate the encryption requirements with the organization's stakeholders and business units
- ☐ Define the hardware and software architecture, components, modules, and interfaces necessary to protect the confidentiality of the organization's data
- ☐ Develop implementation cost estimates and TCO estimates; validate these estimates with the organization's stakeholders and business units

Step #7 – Begin data re-alignment

In some situations, the design makes certain assumptions about the storage infrastructure and location of the data. In addition, cost constraints may limit the full use of the design. To address these issues, data may need to be migrated or re-aligned to take full advantage of the expected encryption solution.

- ☐ If not already done, identify and document data location and/or data migration assumptions and requirements associated with the encryption design
- ☐ Identify and document exception cases (e.g., legacy systems) to the data

location/migration assumptions and requirements

- ☐ Identify acceptable (reduced) performance and throughput levels as well as increased risk exposures (availability, increased attack surface) and note where these are above and beyond the tolerances used during the design process
- ☐ Determine whether data re-alignments improve the organization's ability to encrypt data At-Rest as the costs and efforts to re-align the data may negate the benefit
- ☐ Identify specific data to be relocated and develop an action plan to re-align this data
- ☐ Begin the data re-alignment efforts, including making changes to the storage infrastructure (including virtualization)
- ☐ Change data protection schemes and related CDP, DLP, compression & deduplication processes in light of the re-alignment

Step #8 – Implement solution

Implementing the encryption solution is where the rubber hits the road. The specified components are acquired and/or developed, tests are conducted, the systems are deployed, and the solution is certified[2].

- ☐ Determine the approach (e.g., multi-phased, outsourced, etc.) to be used to field the encryption solution.
- ☐ Select (when multiple options are available) and acquire/develop the specified components to be used for the encryption solution while exercising due care to address liability issues
- ☐ Deploy the encryption technology into the organization's IT infrastructure (per the design) without activating the encryption capabilities
- ☐ Ensure that the key management, key synchronization, and key archiving mechanisms are secured and working properly.
- ☐ Integrate the encryption technology with existing logging (proof of encryption), authentication, directory services (authorization and access control), and network time infrastructure.
- ☐ Complete the end-to-end testing with the encryption capabilities temporarily enabled
- ☐ Develop and document the roll-back plan (including procedures for loss of hardware)

[2] Within the context of this document, certification comprehensively assesses information technology system security features to determine if they meet the security policy and accreditation is the official acceptance of the management of risk in the information technology system. Accreditation by an external entity may be a good idea.

Step #9 – Activate encryption

The final step is focused on those activities that transition the encryption solution into operational use. At a minimum, it should include management acceptance of the solution and approval to proceed to a production state (e.g., management accreditation[2]).

- ☐ Complete informal or formal management accreditation of the encryption solution (i.e., acceptance of the solution) and obtain approval to operate
- ☐ If appropriate and needed, perform data re-alignment activities that were not possible prior to implementation
- ☐ Turn on the actual encryption capabilities (e.g., activate background encryption on existing data)
- ☐ Run point tests to prove that the data can be processed & recovered & results can be audited, making sure the right keys are available & logs working
- ☐ If appropriate, complete final data re-alignment activities that were not possible prior to activation of encryption

Summary

Encryption can be used as a preventative control (protect data from disclosure to unauthorized parties), a detective control (discovery of unauthorized changes to data), or both. There are multiple considerations that need to be made when evaluating the deployment of an encryption process, including, but not limited to:

- Properly used, encryption can strengthen an organization's systems.
- Encryption has the potential to weaken other security aspects (e.g., inspection of data, anti-virus, etc.).
- Although necessary, encryption carries the risk of making data unavailable should anything go wrong with data handling, data transformations such as compression, key management, or the actual encryption.
- Encryption may potentially include significant overhead cost/impacts on hosts and networks.

According to the Information Systems Audit and Control Association (ISACA), "The most critical aspect of encryption is the determination of what data should be encrypted and where and when it should be encrypted." To re-enforce this point, ISACA has developed a specific procedure that an IS auditor should use when evaluating an organization's management controls over encryption methodologies (see Appendix B). Likewise, the Federal Financial Institutions Examination Council (FFIEC) and the Payment Card Industry (PCI) have developed their own guidance on encryption (see Appendix A and C, respectively).

The bottom line for encrypting data at-rest is that all data should be evaluated 1) from a risk perspective for unauthorized viewing and 2) the justifiable business need given the cost vs. benefit or risk reduction.

Bibliography

"Storage Networking Security", published by SNIA as part of the SNIA Technical Tutorial Series, July 2004. See
http://www.snia.org/education/storage_networking_primer/storage_security/

The SNIA Dictionary - a glossary of storage networking and data and information management terminology. Published annually by SNIA and available online, see
http://www.snia.org/education/dictionary/

SNIA tutorial "ABCs of Encryption", published twice yearly by SNIA in collaboration with the StorageNetworkingWorld conferences. Past versions are available online, see
http://www.snia.org/education/tutorials/

Appendix A – FFIEC & Encryption

The Federal Financial Institutions Examination Council (FFIEC), in its *IT Examination Handbook – Information Security*, provides examiners with a checklist that can be used to assess the quantity of risk and the effectiveness of an institution's risk management processes as they relate to the security measures instituted to ensure confidentiality, integrity, and availability of information and to instill accountability for actions taken on the institution's systems. A subset of this body of work addresses encryption and it is presented in the following table along with the more general data security elements.

K. ENCRYPTION

1. Review the information security risk assessment and identify those items and areas classified as requiring encryption.
2. Evaluate the appropriateness of the criteria used to select the type of encryption/ cryptographic algorithms. ▪ Consider if cryptographic algorithms are both publicly known and widely accepted (e.g. RSA, SHA, Triple DES, Blowfish, Twofish, etc.) or banking industry standard algorithms. ▪ Note the basis for choosing key sizes (e.g., 40-bit, 128-bit) and key space. Identify management's understanding of cryptography and expectations of how it will be used to protect data.
3. Determine whether cryptographic key controls are adequate. ▪ Identify where cryptographic keys are stored. ▪ Review security where keys are stored and when they are used (e.g., in a hardware module). ▪ Review cryptographic key distribution mechanisms to secure the keys against unauthorized disclosure, theft, and diversion. ▪ Verify that two persons are required for a cryptographic key to be used, when appropriate. Review audit and security reports that review the adequacy of cryptographic key controls.
4. Determine whether adequate provision is made for different cryptographic keys for different uses and data.
5. Determine whether cryptographic keys expire and are replaced at appropriate time intervals.
6. Determine whether appropriate provisions are made for the recovery of data should a key be unusable.
7. Determine whether cryptographic keys are destroyed in a secure manner when they are no longer required.

L. DATA SECURITY

1. Obtain an understanding of the data security strategy. ▪ Identify the financial institution's approach to protecting data (e.g., protect all data similarly, protect data based upon risk of loss). ▪ Obtain and review the risk assessment covering financial institution data. Determine whether the risk assessment classifies data sensitivity in a reasonable manner and consistent with the financial institution's strategic and business objectives. ▪ Consider whether policies and procedures address the protections for data that is sent outside the institution. Identify processes to periodically review data sensitivity and update corresponding risk assessments.
2. Verify that data is protected consistent with the financial institution's risk assessment. ▪ Identify controls used to protect data and determine if the data is protected throughout its life cycle (i.e., creation, storage, maintenance, transmission, and disposal) in a manner consistent with the risk assessment. ▪ Consider data security controls in effect at key stages such as data creation/acquisition, storage, transmission, maintenance, and destruction. Review audit and security review reports that summarize if data is protected consistent with the risk assessment.
3. Determine whether individual and group access to data is based on business needs.
4. Determine whether, where appropriate, the system securely links the receipt of information with the originator of the information and other identifying information, such as date, time, address, and other relevant factors.

Source: Federal Financial Institutions Examination Council (FFIEC), *IT Examination Handbook – Information Security*, July 2006, http://www.ffiec.gov

NOTE: The procedures provided above should not be construed as requirements for control implementation. The selection of controls and control implementation should be guided by the risks facing the institution's information system. Thus, the controls necessary for any single institution or any given area of a given institution may differ from the specifics that can be inferred from the following procedures

Appendix B – ISACA & Encryption

The Information Systems Audit and Control Association (ISACA) with its *IS Standards, Guidelines, and Procedures for Auditing and Control Professionals* has developed a body of work that is widely recognized by the auditing community. The IS Auditing Standards, within this document, are mandatory requirements for certification holders' (CISA and CISM) reports on the audit and its findings; the IS Auditing Guidelines and Procedures are detailed guidance on how to follow those standards. The ISACA *Evaluation of Management Control over Encryption Methodologies* (see table below) includes important information for organizations considering the use of encryption.

Aspects of Encryption	Suggested Procedures

Organisational management	▪ Verify that written procedures/policies exist, including clear definition of roles and responsibilities for key management, including key generation/creation; loading, including a controlled elevation process (to the production environment) for changes; transporting, storage; recovery; retirement/destruction; theft and frequency of required use. Included with these procedures should be requirements over securing the key and controlling the elevation of the key into the production processing environment.
	▪ Ascertain if there is a clearly defined written procedure defining what data are considered sensitive, requiring encryption. In addition, ascertain if this procedure included requirements for when and how the encryption is to be applied. Specifically, determine if the encryption should be applied to data residing in static database or file form or only when transmitted over the Internet.
	▪ In conjunction with the above, ascertain if a list has been made and approved of the data to be protected and its characteristics. Furthermore, determine if an estimate has been made of the financial value of each data item to be protected and of the costs of protection?
	
	Note: Consider the following in reviewing the list of information assets requiring full confidentiality via encryption. Data transmitted over the unsecured network (Internet) requires more security than a controlled database residing on an internal network segment that relies only specific static internal workstation IP addresses. In addition, verify that there is no duplication of encryption where data is encrypted in the database and then encrypted a second time during transmission, unless there is a risk assessment to validate the additional need for this.
	▪ In summary, the IS auditor should verify that policies and procedures exist to determine what information is to be encrypted, the level of encryption and methods to determine who has access to decrypt the information. The IS auditor should communicate to the auditee that the success of encryption technologies is based on effective organisation, appropriately formalised.
	▪ Verify that management has instituted controls over the number of manual procedures and people involved in cryptographic system management, and at a minimum:
	  ▪ Dual control should be maintained on all keys that require physical handling.
	  ▪ The strength of cryptographic systems depends upon the secrecy

	of the keys. Ideally, no one should be allowed to handle encryption keys or see them. ▪ Keys should be comprised of two separate key components and should only be known under the concepts of split knowledge and dual control. ▪ Keys should be maintained on a computer that is not accessible by any programmers or users, such as router controls for logical access and strong physical controls with an air gap in a secured area/room.
Design criteria of a cryptographic system	▪ Verify that the process the enterprise uses to make its selection of an encryption algorithm is the most effective and efficient. In determining which is the best algorithm to choose, management should consider the environment where the cryptographic system is to operate: ▪ Type of processing and transmission system to ensure satisfactory integration ▪ Transmission paths, including compression requirements to ensure performance service levels ▪ Users' and operators' skills and training to use the system and key ▪ Integration with the operating environment to ensure communication is secure and reliable ▪ Algorithm is effective with regards to the application and the objectives ▪ Obtain and review documentation from management attesting that the chosen algorithm ensures all the protections at the desired level (according to the risk analysis) and is cost effective and convenient. For example, a stronger encryption system may be expensive and computer resource consuming and may not be necessary given the protection needed for internal organisation transmissions. ▪ Verify that management has collaborated with other IT functions to ensure minimal effect on interfacing and other systems. When selecting such a cryptographic system, all of the major functional areas, such as systems programming and UNIX administration within IT, should be considered—along with data confidentiality and integrity needs—regarding the importance (and economic value) of data being protected. ▪ Verify the integration with system architecture. The encryption system should not interfere with normal operation affect the system architecture. ▪ Obtain management documentation attesting to whether the chosen algorithm takes the deciphering cost by an authorised user to a sufficiently cost-prohibitive level. As computers become faster, new algorithms and longer keys are needed. The cost to decipher the encrypted message should not exceed the value of information itself. ▪ Determine if management has applied respected standards in making the cryptographic system compatible with the applications. Standards exist for encryption systems, such as SSL, which ensure compatibility among various hardware/software platforms. ▪ Ascertain if management has considered and respected all local and international laws and regulations (where applicable). Many countries have established laws and regulations to discipline the use of encryption technologies. Many vendors have operating rules as well. ▪ Obtain from management and review documentation attesting that the system is strong and not attackable. Knowledge by the interceptor of encryption algorithms or hardware/software used does not impair

	reliability. It may be more effective to use a known and tested algorithm to generate the key, rather than to create an algorithm for the organisation. Security of good (strong) encryption systems does not depend on the secrecy of the algorithm, but only on the secrecy of the keys.

Change control over the cryptographic system including key management	▪ Verify, via audit testing, whether changes and updates to the cryptographic system are controlled and performed only by authorised individuals in accordance with existing written policies and procedures. Verify that key transmission is controlled according to a specific procedure. The risk of having a key disclosed is higher when the key has to be transmitted to the recipient(s).
	  ▪ Determine if the retirement of keys based on time is in accordance with policy or best industry standards. Incorrect or unnecessary changes and updates may impair the effectiveness of the cryptographic system.
	  ▪ Caution should be used when inputting keys into an application, as this presents security weaknesses. Specifically, keys should only be stored in tamper-resistant modules and never in clear text of programs or operating systems, where keys could become compromised without management's awareness.
	  ▪ Elevation of keys into production should occur by select security personnel and only during time periods where security over elevation is maintained. n Copies of keys should not be maintained within the testing environment or any environment accessible by programmers and users.
	  ▪ Verify that users and operators do not handle keys. Automatic key management systems can reduce the risk of disclosing an encryption key.
	▪ Verify that the key of the cryptographic system ensures all the required properties, including the length, composition and management of the key.
	▪ Ascertain if the key of the cryptographic system is easy to generate and modify, so the key can be changed expeditiously if suspected to have been compromised, as well as changed periodically based on requirements.
	▪ Ascertain that management employment of the key to access the cryptographic system (or the password to unlock its use) is not easily guessable.
	▪ Ascertain, via discussion with the security engineer or applicable auditee, that the key of a cryptographic system is easy to modify given the ease of use of the cryptographic system (algorithm). Given the risk of unauthorised viewing of data, there may be a requirement to change the key often.

Digital Signature	▪ Determine if management has instituted controls to verify that private keys are never backed up. By backing up a private key, exposure is increased. However, the public keys should be backed up to verify old signatures after expiration or revocation. ▪ Ascertain if management uses different key pairs for encryption and digital certificates. Governmental units may require the private encryption key. However, verify, if applicable, that the governmental unit does not receive the key for the digital signature simultaneously.
Validity conditions of a cryptographic algorithm	▪ Ascertain if management has considered the need for the mathematical equations and formulas to be so complicated that they prevent its resolution by means of exhaustive, analytic and statistic attacks. Robustness is the propriety which, although the algorithm part

	of the clear text and its corresponding cipher text are known by the intruder, it is impossible to recover the whole text without using the encryption key. ▪ Verify that management has taken into consideration, where mathematically less-complicated algorithms are used, that the cost and the time necessary to recover the message should be prohibitive, in terms of programming steps or computer memory utilisation. The cost of deciphering should exceed the value of the information the encryption system is supposed to protect.

Source: Information Systems Audit and Control Association (ISACA), *IT Audit and Assurance Tools & Techniques, Procedure 9* (Evaluation of Management Controls Over Encryption Technologies), © 2009, 15 May 2009, http://www.isaca.org/standards

Appendix C – PCI DSS & Encryption

The Payment Card Industry (PCI) has identified a set of data security requirements that apply to all members, merchants, and service providers that store, process, or transmit cardholder data. These requirements are codified in the PCI Data Security Standard (PCI DSS); the PCI Security Audit Procedures provide additional details and are used to validate compliance with the PCI DSS.

The following table lists the encryption-related elements from the PCI Data Security Standard.

Requirement 3: Protect Stored Data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed and not sending PAN in unencrypted e-mails.

Please refer to the PCI DSS Glossary of Terms, Abbreviations, and Acronyms for definitions of "strong cryptography" and other PCI DSS terms.

REQUIREMENTS	TESTING PROCEDURES
3.4 Render PAN, at minimum, unreadable anywhere it is stored, (including data on portable media, in logs) by using any of the following approaches: • One-way hashes based on strong cryptography • Truncation • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key management processes and procedures. The MINIMUM account information that needs to be rendered unreadable is the PAN. *Notes*: • *If for some reason, a company is unable render the PAN unreadable, refer to Appendix B: Compensating Controls.* • *Strong cryptography" is defined in* the PCI DSS Glossary of Terms, Abbreviations, and Acronyms.	**3.4.a** Obtain and examine documentation about the cryptographic system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that data is rendered unreadable using one of the following algorithms: • One-way hashes based on strong cryptography • Truncation or masking • Index tokens and pads, with pads being securely stored • Strong cryptography, with associated key management processes and procedures **3.4.b** Examine several tables from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text). **3.4.c** Examine a sample of removable media (for example, backup tapes) to confirm that the PAN is rendered unreadable. **3.4.d** Examine a sample of audit logs to confirm that the PAN is sanitized or removed from the logs.
3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:	**3.5** Verify processes to protect keys used for encryption against both disclosure and misuse by performing the following:
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	**3.5.1** Examine user access lists to determine that access to keys is restricted to very few custodians.

3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	**3.5.2** Examine system configuration files to determine that storage of cryptographic keys in encrypted format and storage of key-encrypting keys separately from data-encrypting keys.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	**3.6.a** Verify the existence of key-management procedures for keys used for encryption of cardholder data. *Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov* **3.6.b** For service providers only: If the service provider shares keys with their customers for transmission of cardholder data, verify that the Service Provider provides documentation to customers that includes guidance on how to securely store and change customer's keys (used to transmit data between customer and service provider). **3.6.c** Examine the key-management procedures and perform the following:
3.6.1 Generation of strong cryptographic keys	**3.6.1** Verify that key-management procedures are implemented to require the generation of strong keys
3.6.2 Secure cryptographic key distribution	**3.6.2** Verify that key-management procedures are implemented to require secure key distribution
3.6.3 Secure cryptographic key storage	**3.6.3** Verify that key-management procedures are implemented to require secure key storage
3.6.4 Periodic cryptographic key changes • As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically • At least annually	**3.6.4** Verify that key-management procedures are Implemented to require periodic key changes at least annually.
3.6.5 Retirement or replacement of old or suspected compromised cryptographic keys	**3.6.5a** Verify that key-management procedures are implemented to require the retirement of old keys (for example: archiving, destruction, and revocation as applicable). **3.6.5.b** Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.
3.6.6 Split knowledge and establishment of dual control of cryptographic keys	**3.6.6** Verify that key-management procedures are implemented to require split knowledge and dual control of keys (for example, requiring two or three people, each knowing only their part of the key, to reconstruct the whole key).
3.6.7 Prevention of the unauthorized substitution of cryptographic keys.	**3.6.7** Verify that key-management procedures are implemented to require the prevention of the unauthorized substitution of keys.
3.6.8 Requirement for cryptographic key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.	**3.6.8** Verify that key-management procedures are implemented to require key custodians to sign a form specifying that they understand and accept their key-custodial responsibilities.

Source: PCI Security Standards Council, *PCI Data Security Standard (PCI DSS)*, ©2008, Version 1.2.1, July 2009, https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

About the Author(s)

Eric A. Hibbard

Mr. Hibbard is the Chief Technology Officer Security & Privacy for Hitachi Data Systems where he is responsible for developing and leading the execution of the company's storage security strategy and serves as the principle storage security architect. He has significant experience architecting complex ICT and security infrastructures for large enterprises. Prior to joining HDS, he held key technology positions within government (DoD, NASA, DoE), academia (University of California at Lawrence Berkeley National Laboratory), and industry (Raytheon and QSS Group). In addition, Mr. Hibbard holds a unique combination of security (CISSP, ISSAP, ISSMP, and ISSEP from ISC2), IS auditing (CISA from ISACA), and storage (SCP and SCSE from SNIA) certifications. He is currently the Chair of the SNIA Security Technical Working Group, the International Representative for INCITS/CS1 (Cyber Security), the Vice Chair of the American Bar Association – SciTech Law – eDiscovery & Digital Evidence Committee, Vice Chair of the IEEE Information Assurance Standards Committee (IASC), and the Vice Chair of the IEEE P1619 (Security in Storage Work Group) as well as a member/participant of INCITS/T11 (Fibre Channel Interfaces), IETF, W3C, the IEEE-USA Critical Infrastructure Protection Committee (CIPC), the Distributed Management Task Force (DMTF), and the Trusted Computing Group (TCG).

Roger Cummings

Mr. Cummings is a Technical Director in the Office of the CTO for Symantec Corportation. He currently serves as Co-Chair of the SNIA Long Term Retention (LTR) Technical Working Group (TWG). He is a former Co-Chair of the SNIA Security TWG and a former member of the SNIA Technical Council. He has more than 35 years of development experience with Logica (UK), Control Data (Canada), and StorageTek, Adaptec, & Symantec (USA). He has been involved in storage standards work since the early 1980s, most notably as an officer of the INCITS Technical Committee (TC) T11 (Fibre Channel) committee from 1990–1998 and 2002-2007, and is currently also active in INCITS TC T10 (SCSI).

Many thanks to the following for their contributions to this paper.

Richard Austin, CISSP
Walt Hubis
Robert Lockhart
Jim Norton
Vinodraj Daniel
Larry Hofer, CISSP, PE
Andrew Nielsen, CISSP, CISA

About the SNIA

The Storage Networking Industry Association (SNIA) is a not-for-profit global organization, made up of some 400 member companies and 7,000 individuals spanning virtually the entire storage industry. SNIA's mission is to lead the storage industry worldwide in developing and promoting standards, technologies, and educational services to empower organizations in the management of information. To this end, the SNIA is uniquely committed to delivering standards, education, and services that will propel open storage networking solutions into the broader market. For additional information, visit the SNIA web site at www.snia.org.

About the SNIA Security Technical Work Group

The Security Technical Work Group (TWG) consists of storage security subject matter experts, from the SNIA membership, who collaborate to develop technical solutions to secure storage networks and protect data. The Security TWG provides architectures and frameworks for the establishment of information security capabilities within the storage networking industry. Additionally, it provides guidance on the application of information assurance to storage systems/ecosystems as well as on matters of compliance as it relates to data protection and security. The focus of the Security TWG is directed toward both long-term and holistic security solutions.

About the SNIA Storage Security Industry Forum

The SNIA Storage Security Industry Forum (SSIF) is a consortium of storage professionals, security professionals, security practitioners, and academics dedicated to increasing the overall knowledge and availability of robust security solutions in today's storage ecosystems. The SSIF applies their deep body of knowledge and practical experiences in security and storage to produce best practices on building secure storage networks, provide education on storage security topics, and participate in standards development. SSIF educational, technical, and engineering activities influence the design, use, and management of storage technology to better protect and secure information. For more information, and to join, visit www.snia.org/forums/ssif.