Storage Networking Industry Association
Technical White Paper

Storage Security: Encryption and Key Management

August 26, 2015

Abstract: *The ISO/IEC 27040:2015 (Information technology - Security techniques - Storage security) standard provides detailed technical guidance on controls and methods for securing storage systems and ecosystems. This whitepaper describes the recommended guidelines for data confidentiality, including data in motion encryption, data at rest encryption, and key management. The practical implications of these recommendations are discussed from both an end user and storage vendor perspective.*

USAGE

DISCLAIMER

The information contained in this publication is subject to change without notice. The SNIA makes no warranty of any kind with regard to this specification, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The SNIA shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this specification.

Suggestions for revisions should be directed to http://www.snia.org/feedback/.

Revision History

Revision	Date	Sections	Originator:	Comments
V0.1	*8/25/2014*	All	Walt Hubis	Initial Draft
V0.2	*3/6/2014*	All	Walt Hubis	Review Draft
V0.3	*5/5/2015*	All	Walt Hubis	1st Ballot Draft
V0.5	*7/10/2015*	All	Walt Hubis	2nd Ballot Draft
V07	*8/15/2015*	All	Eric Hibbard	Post-Ballot Draft
V08	*8/18/2015*	All	Eric Hibbard	3rd Ballot Draft
V09	*8/26/2015*	All	Eric Hibbard	Final

Suggestion for changes or modifications to this document should be submitted at http://www.snia.org/feedback/.

Foreword

This is one of a series of whitepapers prepared by the SNIA Security Technical Working Group to provide an introduction and overview of important topics in ISO/IEC 27040:2015, *Information technology – Security techniques – Storage security*. While not intended to replace the standard, they provide additional explanations and guidance beyond that found in the actual standard.

Executive Summary

Increasingly, cryptographic mechanisms such as encryption and key management are being used in storage ecosystems to protect data transferred to (data in motion) and stored (data at rest) in data storage systems. To effectively use these technologies, organizations need to understand the benefits, issues, implications, and the limitations, especially when sensitive and high-value data are involved. This storage security whitepaper leverages the guidance in the ISO/IEC 27040 standard and provides value added information on encryption and key management as it relates to storage systems and ecosystems.

1 Introduction

The application of encryption to a storage ecosystem can afford very different protections depending on how and where it is integrated. For example, encrypting files or shares within a Network Attached Storage (NAS) file system can offer user-specific protections that are not possible with encryption at the drive level. Thus, it is important to understand the reasons encryption should be considered (that is, which threats are to be mitigated).

ISO/IEC 27040:2015 *Information technology - Security techniques - Storage security* provides detailed technical guidance on controls and methods for securing storage systems and ecosystems (see Appendix A for an overview). While the coverage of this standard is quite broad it does lack specific guidance for certain topics that could enhance the protections. This is partially true with regard to encryption and key management.

This whitepaper, which is one in a series from SNIA that addresses various elements of storage security, is intended to leverage the guidance in the ISO/IEC 27040 standard and build upon it with a specific focus on encryption and key management. In addition, it incorporates industry insights with certain security features and capabilities. The whitepaper provides background information on encryption and key management, summarizes the security options, explores the relevant ISO/IEC 27040 guidance, and offers addition information that can help in securing storage.

1.1 Confidentiality and Secrecy

Confidentiality is the property whereby information is available to authorized parties on demand but never available to unauthorized parties. Secrecy is a term that is often used synonymously with confidentiality. Cryptographic mechanisms are one of the strongest ways to provide confidentiality and other security services in applications and protocols for data storage. [1]

Confidentiality is often achieved using encryption to render the information unintelligible to unauthorized entities. The information is rendered intelligible to authorized entities by

[1] A general introduction to cryptography is *Cryptography Decrypted* by H. X. Mel and Doris Baker (Addison-Wesley:2000 ISBN 978-0201616477)

decryption. In order for encryption to provide confidentiality, the cryptographic algorithm and mode of operation must be designed and implemented so that an unauthorized party cannot determine the secret or private keys[2] associated with the encryption or be able to derive the plaintext directly without determining any keys.

1.2 Encryption Overview

The primary purpose of encryption (or *encipherment*) systems is to protect the confidentiality of stored or transmitted data. Encryption algorithms achieve this by transforming plaintext into ciphertext, from which it is computationally infeasible to find any information about the content of the plaintext unless the decryption key is also known. However, the length of the plaintext will generally not be concealed by encryption, since the length of the ciphertext will typically be the same as, or a little larger than, the length of the corresponding plaintext.

It is important to note that encryption may not always, by itself, protect the integrity or the origin of data. In many cases it is possible, without knowledge of the key, to modify encrypted text with predictable effects on the recovered plaintext. In order to ensure integrity and origin of data it is often necessary to use additional techniques.

There are three basic classes of cryptographic algorithms: hash algorithms, symmetric key algorithms and asymmetric key algorithms. The classes are defined by the number of cryptographic keys that are used in conjunction with the algorithm.

1.3 Key Management Overview

With the exception of hashing, the use of cryptography relies on the management of cryptographic keys. All ciphers, both symmetric and asymmetric, require all the communicating parties to have access to the necessary keys. This gives rise to the need for key management involving the generation, distribution, and ongoing management of keys. An overall framework for key management is given in ISO/IEC 11770-1 and NIST SP 800-57 Part 1.

As noted in NIST SP 800-57 Part 1 (R3), keys are analogous to the combination of a safe. If a safe combination becomes known to an adversary, the strongest safe provides no protection for its contents. Similarly, poor key management may easily compromise strong algorithms. Ultimately, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with keys, and the protection afforded to the keys. All keys need to be protected against modification, and secret and private keys need to be protected against unauthorized disclosure. Key management provides the foundation for the secure generation, storage, distribution, and destruction of keys.

[2] Secret keys are used in symmetric encryption while private keys are used in asymmetric encryption.

1.4 Cryptographic Strength

Cryptographic strength is a measure of the amount of work an attacker must invest to conduct a brute force attack on an unknown cryptographic key. For example, a strength of 112 bits implies that an attacker must try 2^112-1 keys, on average, before hitting on the correct one. However, cryptographic strength only tells part of the story. For this measure to be relevant, the brute force attack must be the only feasible attack available to the attacker. If the cryptographic algorithm has a weakness in its operation, then an analytic attack might be much easier. Or if there is a weakness in the implementation of an algorithm, this may simplify the attacker's task (for example, if the keys are not randomly chosen from the entire keyspace). Also, if the attacker can social engineer or gain access to the keying materials, there is no need to mount a brute force attack. Choosing a well-reviewed algorithm and a well-vetted implementation of that algorithm help avoid weaknesses that simplify the attacker's task. Strong key management will make it much more difficult to social engineer or otherwise gain access to the keying material. These practices leave the brute force attack as the only option for an attacker.

1.5 Storage Management

ISO/IEC 27040 highlights the importance of performing storage management (i.e., the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, provisioning and sanitization of storage systems) activities securely, and that it requires controls associated with authentication and authorization, protecting the storage management interfaces, maintaining accountability and traceability of systems and users, and ensuring the underlying systems used for storage management are adequately hardened. While not specifically addressed in this whitepaper, it is worth noting that failures in storage management can result in data breaches and loss of data. Data in motion encryption for the storage management communications protocols play an important role in protecting against these threats.

2 Data Storage Encryption

Inevitably, any encryption discussion associated with storage ecosystems will include a differentiation between data in motion and data at rest encryption. Although difficult to define it is important to understand the concepts, which can be summarized as:

- *Data At Rest Encryption* — encryption that protects data while it resides on the media. It involves encrypting data that will be decrypted when that data flows through the same point (or an equivalent) in the opposite direction. The point of encryption may be within a storage device (tape drive encryption) or the entity in which the data was created and/or consumed (end-to-end encryption) or at any point along the data path.
- *Data In Motion Encryption* — encryption that protects data while it is being transferred over a physical link between two communicating entities (e.g., example, host bus adapter or HBA and a switch). Either the two entities have negotiated and implemented

some form of communications encryption or the data is encrypted before it is transmitted.

As one can see in the descriptions above, an at rest encryption mechanism has the potential of protecting the confidentiality of the actual data as it traverses all of the down-stream communications links, but this protection depends on where in the data path the encryption is applied. Communications-based encryption (for example, IPsec, TLS, SSH, etc.) results in the communicating parties having access to the plaintext data, but it can also include integrity checks to ensure the ciphertext is not changed while it is in motion.

2.1 Data in Motion recommendations

High value or sensitive data[3] is frequently exchanged between systems over wide area networks using TCP/IP, Fibre Channel over IP (FCIP), Fibre Channel over Ethernet (FCoE), iSCSI, and other protocols. Data may also be transferred from host computer systems to storage devices through storage area networks (SANs) using Fibre Channel, Serial SCSI (SAS), and other SAN protocols. In each case, there may be specific security protocols available with each particular network protocol to provide a more secure transport of the data. In some cases, there may also be a transport level security mechanism which can protect data being transmitted. Choosing the specific protection mechanism and points of encryption are important factors not only in securing the data, but also in meeting applicable compliance requirements.

In general, encrypting data in motion is usually only a temporary protection of the data while it is in motion. Certain encryption schemes, such as encryption at the file system, application, or Host Bus Adapter (HBA) provide end-to-end protection, regardless of any intermediate switching or routing devices. When using these methods, encryption of data in motion may provide little or no additional data protection. Also note that, data reduction techniques (e.g., compression and deduplication) are usually ineffective with encrypted data. Further, best practices for data protection recommend an ephemeral key for data in motion and a long lived key for data at rest[4]. As a result, the overall system requirements must be considered before choosing points of encryption and decryption.

ISO/IEC 27040 provides specific recommendations for using TLS, IPsec, FC-SP-2, and other data protection protocols for data in motion. Issues associated with securing Fibre Channel networks are discussed in the *SNIA Storage Security: Fibre Channel Security* whitepaper in this series.

[3] *ISO/IEC 27040 Annex B* makes a distinction between low data sensitivity and high data sensitivity. Protective controls are required for both, since even low sensitivity data may have adverse impacts on businesses, governments, or individuals. See section B.1.2 *Data sensitivity classes*.

[4] Short lived or ephemeral session keys help reduce the likelihood that the data can be decrypted as it passes though the network. Long lived keys for data at rest help to reduce the number of times data must be re-keyed. See SNIA Whitepaper *Encryption of Data at Rest - a Step by Step Checklist*.

2.1.1 IP SAN

Two methods of using IP networks to provide storage protocols are discussed in ISO/IEC 27040: Internet SCSI (iSCSI) and Fibre Channel over TCP/IP (FCIP).

Both iSCSI and FCIP benefit by controlling traffic between initiators and targets on the network. This can be accomplished by filtering the source and destination IP addresses and protocols which may be done either at the target or at intervening switches, reducing the volume of traffic that the target has to deal with while also reducing the number of attack vectors.

IP SANs typically use various information services to locate resources on the network. These may include Internet Storage Name Server (iSNS), Service Location Protocol (SLP), Domain Name Server (DNS), and others. ISO/IEC 27040 recommends that these services should be used with appropriate security controls to avoid attacks or collection of information about data storage resources. RFC 3723 recommends specific security requirements for a conforming implementation. While RFC 2608 *Service Location Protocol, Version 2* provides general guidance on security for SLP, RFC 3723 recommends suing SLPv2 with IPsec. Likewise, IETF RFC 4171 *Internet Storage Name Service (iSNS)* provides general guidance on security for iSNS, but RFC 3723 provides more specific recommendations including using iSNS with IPsec to avoid indirect attacks. Methods of managing network information services must also be protected.

From a practical standpoint, various devices have resource constraints that may make very secure solutions difficult to scale or even impractical. This is especially true for iSCSI networks where implementations may range from large servers to small embedded systems. Since Fibre Channel systems are typically used in data centers, resource constraints are usually lessened. As a result, implementing a secure IP SAN requires careful evaluation of all parts of the network.

2.1.1.1 Internet SCSI (iSCSI)

IETF RFC 3720 *Internet Small Computer Systems Interface (iSCSI)* describes a SCSI transport protocol that works on top of TCP/IP. Extensions to this protocol have been developed that provide for remote direct memory access (RDMA) by using the SCSI RDMA Protocol (SRP) or iSCSI Extensions for RDMA (iSER). ISO/IEC 27040 does not discuss security issues related to these RDMA protocols. All of the iSCSI security requirements as described in IETF RFC 3720 apply.

The iSCSI protocol provides some access protection through the use of CHAP authentication (see IETF RFC 1334 *PPP Challenge Handshake Authentication Protocol (CHAP)*). Bidirectional CHAP (e.g., initiators authenticate targets and visa-versa) should be used with random challenges.

To control access to an IP SAN, SCSI interfaces should not be connected to general purpose IP networks. From both a performance and security perspective, physically isolated iSCSI IP networks provide the best control. It this is not possible, virtual area networks (VLANs) should be used to segregate the IP SAN from other network traffic.

2.1.1.2 Fibre Channel over TCP/IP (FCIP)

IETF RFC 3821 *Fibre Channel Over TCP/IP (FCIP)* describes a pure encapsulation protocol that allows interconnection of Fibre Channel storage area networks through IP-based networks to form a unified storage area network in a single Fibre Channel fabric. IETF RFC 3821 and ISO/IEC 27040 rely on the use of IPsec to provide confidentiality and authentication.

2.1.1.3 IP Security Protocol (IPsec)

ISO/IEC 27040 and IETF RFC *3723 Securing Block Storage Protocols over IP* require the use of IPsec to secure the communication channel to protect sensitive or high value data for both iSCSI and FCIP. ISO/IEC 27040 recommends the use of IPsec Version 3 along with Internet Key Exchange (IKE) version 2. IPsec version 3 is described by a suite of IETF documents:

- RFC 4301 *Security Architecture for the Internet Protocol*
- RFC 4302 *IP Authentication Header*
- RFC 4303 *IP Encapsulating Security Payload (ESP)*
- RFC 4306 *Internet Key Exchange (IKEv2) Protocol*

In addition, IETF RFC 3723 *Securing Block Storage Protocols over IP* places the following requirements on the IPsec suite used with iSCSI and Fibre Channel over TCP/IP (FCIP) protocols:

- Confidentiality: ESP with 3DES in CBC mode as described in IETF RFC 2451 *The ESP CBC-Mode Cipher Algorithms* must be supported, although AES in Counter mode as described in IETF RFC 3686 *Using Advanced Encryption Standard (AES) Counter Mode* should be supported. The use of AES encryption in new implementations is highly recommended (see NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*).
- Authentication and Integrity: HMAC-SHA1 described in IETF RFC 2404 *The Use of HMAC-SHA-1-96 within ESP and AH* must be supported. AES in CBC MAC mode with XCBC extensions described in RFC 3566 *The AES-XCBC-MAC-96 Algorithm and Its Use with IPsec* should be supported. The use of AES encryption in new implementations is highly recommended. DES in CBC mode should not be used.
- IPsec Modes: ESP in tunnel mode per IETF RFC 2406 *IP Encapsulating Security Payload (ESP)* must be supported. IPsec with ESP in transport mode may be supported.

2.1.2 Fibre Channel (FC) SAN

As with IP SANs, FC SANs can leverage an assortment of security capabilities, including protocols to authenticate Fibre Channel entities, set up session keys, negotiate parameters to ensure frame-by-frame integrity and confidentiality, and define and distribute policies across a Fibre Channel fabric. Many of these mechanisms can be complex to understand and challenging to configure properly. Recognizing this situation, SNIA has developed a separate whitepaper, *SNIA Storage Security: Fibre Channel Security*, which covers FC security in more depth.

2.2 Data at Rest Encryption

2.2.1 SNIA Position on Encryption

The Storage Networking Industry Association (SNIA) security position on encrypting data, especially primary data, considers encryption to be a measure of last resort. That said, SNIA strongly recommends that appropriate encryption be used when *sensitive data* leaves the direct control of the organization owning or having responsibility for these data. In this context, sensitive data are data that have legal and/or regulatory requirements for confidentiality protection as well as data that require protection as part of the organization's *due care* (for example, trade secrets, intellectual property, etc.).

SNIA refers to data that leaves the control of the custodian organization as *externalized data*. When these externalized data are also sensitive data, SNIA recommends the following:

- Data stored on removable media (like backup tapes), which potentially leaves the control of the organization, must be protected while at rest.[5]
- Data stored in third party data centers must be protected both in motion and at rest within these "untrusted" data centers.
- Data transferred between "trusted" data centers (controlled by the organization) must be protected.

2.2.2 Point of Encryption

Typically at-rest encryption is dependent on the placement of a single encryption/decryption mechanism within the data flow path, which is known as the point of encryption. The placement of the point of encryption is critical because it defines where in the storage ecosystem that the plaintext data must be routed to be turned into ciphertext, and conversely, it represents the point in the storage ecosystem that the ciphertext must traverse before it can become usable plaintext data. The points of encryption also identify where in the storage ecosystem the data is present in its plaintext form and where it is present in ciphertext.

[5] Note that data residing on tape that is moving between data centers is considered to be at-rest.

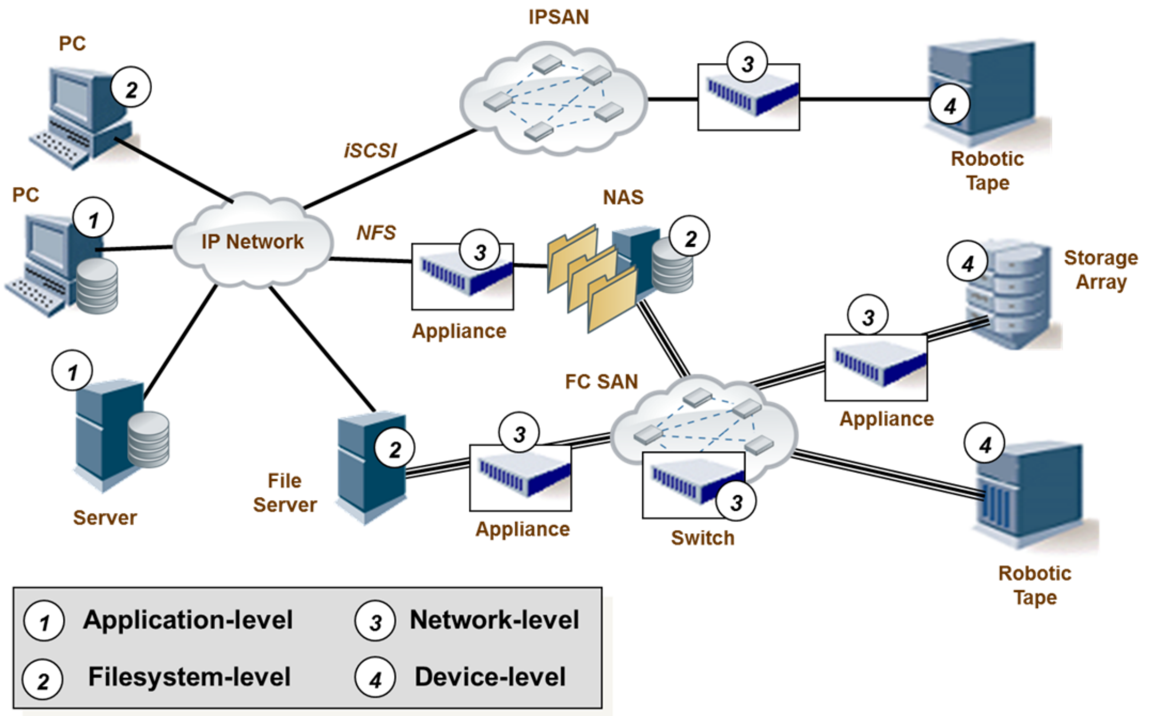


Figure 1. Point of Encryption Options in Storage Ecosystems

The general position of security professionals on the use of encryption is that it should be applied as close to the source of data (the generating application) as possible. Doing so maximizes the protection (data in motion and data at rest protection), and it allows characteristics or attributes of the data to be factored into the protection. Unfortunately, this general guidance often proves impractical because of other factors in the environment (e.g., the generating application may not offer encryption capability).

Architecturally, there may be multiple viable point of encryption options. In such situations, the following factors and impacts should be considered as part of the selection process:

- *Usability* — user experiences a change in the interface, process and/or storage mechanism, which may hamper its acceptance.
- *Availability* — the degree to which the overall availability of the system/solution will be restricted, diminished or eliminated.
- *Infrastructure* — the degree to which networking, systems and storage infrastructure (for example, moving LUNs) must be changed.
- *Performance/Throughput* — negative impact compared to existing (low=10 percent, moderate=20 percent, significant=35 percent, extreme=50 percent+)
- *Scalability* — the degree to which the overall scalability of the existing system will be restricted, diminished or eliminated.
- *In Motion Confidentiality* — characterization of confidentiality protection from the user system/application to the storage device or media.

- *Business Continuity/Disaster Recovery* — the degree to which the overall business continuity/disaster recovery will be restricted, diminished or eliminated.
- *Proof of encryption* — characterization of the proof of encryption aspects (functionality, integration into existing infrastructure, evidence).
- *Environmentals* — characterization of the environmental aspects (power, cooling, space).

When each of these factors is compared and contrasted for the four point of encryption categories (see Table 1), there is no clear winner. In other words, each organization's unique requirements (for example, on compliance), data sensitivity and existing infrastructure have to be carefully considered to arrive at an acceptable solution.

IMPACT	APPLICATION	FILESYSTEM	NETWORK	DEVICE
Usability	Low	Low-Moderate	None	None
Availability	Can be significant	Can be significant	Low-Moderate (Redundancy)	Low-Moderate
Infrastructure	Can be significant	Can be significant	Low-Moderate	Low
Performance/ Throughput	Can be severe	Can be significant	Low	Low-Moderate
Scalability	Can be significant	Can be significant	Can be moderate	Minimal
In Motion Confidentiality	Excellent	Low-Moderate (NAS); Excellent (Host)	Low-Moderate	None
Business Continuity/Disaster Recovery	Can be extremely complicated	Can be complicated	Can be extremely complicated	Can be extremely complicated
Proof of Encryption	Can be complicated	Relatively easy	Low-Moderate	Can be complicated
Environmentals	Low-Moderate	Low-Moderate	Can be significant	Low

Table 1. Factors Influencing Encryption

That being said, some organizations are looking to encryption at the network level (to a lesser degree) and device level as a safety net. The primary objective is to ensure that storage media (tapes and disks), used in conjunction with sensitive data, are encrypted. If these protected media are mishandled (lost, incomplete, transferred to unauthorized parties, etc.) or returned to a vendor or supplier, the organization is often able to avoid the cost and/or embarrassment associated with a security incident.

2.2.3 Data at Rest Recommendations

While ISO/IEC 27040 recognized that data is best encrypted as close as possible to the origin of that data, it also recognizes that encryption used near the point of storage provides an effective mechanism to combat situations where control of the media is lost (e.g., storage media recycled, discarded, etc.). In these cases, technologies such as self-encrypting drives (SED), controller-based encryption, and tape encryption may be especially useful. However, these technologies require careful planning to provide the following:

- Selection of the point and type of encryption
- Identification, location, and verification of encryption (audit)
- Key management

The appropriate encryption algorithms should be employed to assure data confidentiality. These include AES block chaining encryption methods such as XTS-AES for drives and Galois/Counter mode (GCM) for tape, among others. In any event, key management is a very important part of securing data at rest and is further discussed in Section 3 of this document.

For all types of encryption, the following controls are recommended:

- Storage based encryption should not be the primary form of encryption. Assuring data confidentiality and integrity extends beyond data at rest encryption.
- The point of encryption depends on any required data reduction operations.
- Data retention requirements should be accommodated when deploying encryption.
- The strength of the encryption should be a minimum of 112 bits, with 128 as the recommended minimum.
- Cryptographic modules should be validated using recognized criteria.
- Multiple encryption steps may be used. For example, encryption at the application layer that is then stored on a self-encrypting drive.
- Encryption activities must generate appropriate audit log entries (e.g., activation, re-keying, verification, etc.).

For high-value data, encryption should be end to end, including data at rest and data in motion encryption. For more information, see ISO/IEC 27040, Section 7.5 *Data confidentiality and integrity*.

3 Key Management

3.1 Importance of proper key management

Proper key management for encrypted data, both at rest and in motion, is crucial to the confidentiality and availability of that data. While key management of data in motion is important, keys used in this situation are usually ephemeral and generated through automated key exchange methods (e.g., IKEv2). Further, the amount of data secured with a single key is usually small. Keys for the protection of data at rest require greater care, since the lifespan of the encrypted data may be long and the amount of data secured by a single key may be substantially greater than those used for data in motion. In addition to ISO/IEC 27040, NIST Special Publication 800-57, *Recommendation for Key Management – Parts 1-3*, provide a great deal of detailed information and recommendations for key management.

The lifecycle of keys and keying material is an important consideration of any key management scheme. Key management considerations include the generation of keys, secure distribution of the keys, activation and deactivation of keys. Additionally, procedures must be put into place governing how keys are archived, destroyed at the end of their useful life and how key compromises should be handled. A simple key lifecycle system is shown in Figure 2.

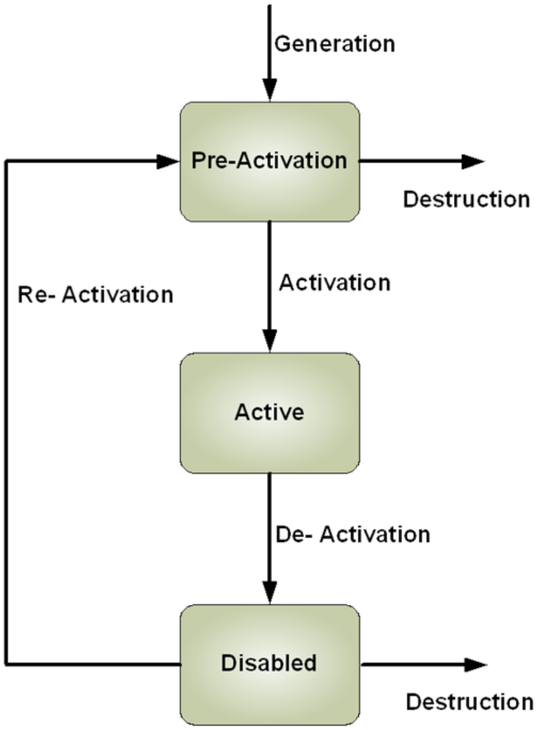


Figure 2: Simple Key Lifecycle

There are significant complexities associated with various aspects of key lifecycle management issues that are well beyond the scope of this whitepaper. NIST Document SP 800-57 Part 1-Rev. 3 *Recommendations for Key Management: Part 1: General (Revision 3)* provides recommendations on key lifecycles. The OASIS *Key Management Interoperability Protocol (KMIP) Specification Version 1.2* illustrates an industry standard key lifecycle model.

3.2 KMIP Considerations

Key management is one of the more challenging cryptography elements to implement correctly. Use of KMIP by storage clients is an effective way to "outsource" many of the more problematic elements (e.g., random key generation). When using KMIP or considering its use, it is important to consider the following:

- *Availability of Key Materials* — When a storage system is dependent on an external key management server for its data encryption keys and/or key wrapping keys, it means the data on the storage system cannot be accessed until these keys are available; it may be impossible to perform operations on the ciphertext (e.g., replication, backups, etc.). Consequently, it is important to build in redundant access to multiple key management servers. In addition, the storage system should block attempted user or host access to the data until the appropriate keys are available.

- *Secure Transport* — Encryption keys are considered sensitive information and must be protected at all times, especially when they are transmitted. The KMIP Specification requires this protection, but defers the details to the KMIP Profiles; these profiles specify the use of TLS in the *Basic Authentication Suite* and the *TLS 1.2 Authentication Suite*. KMIP Servers are required to support TLS 1.0, but may support TLS 1.1 and TLS 1.2; no such requirements are imposed on KMIP Clients. The Basic Authentication Suite mandates the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite and the TLS 1.2 Authentication Suite mandates the TLS_RSA_WITH_AES_ 128_CBC_SHA256 and TLS_RSA_WITH_AES_256_CBC_SHA256 cipher suites.[6]

  NOTE: The *SNIA TLS Specification for Storage Security* (ISO/IEC 20648) requires the TLS_RSA_WITH_AES_128_CBC_SHA and TLS_RSA_WITH_AES_128_CBC_SHA256 cipher suites.

- *Audit Security* — When a storage system is dependent on the interactions with a KMIP Server, logging of the KMIP transactions can be critical to identifying the root cause of problems. As such, all KMIP client-to-server operations need to be logged with sufficient details that a problem can be diagnosed; keys must never be exposed in the logs. In addition, many organizations need to retain records that serve as proof-of-encryption and disaster recovery/business continuity evidence. Some of the KMIP operations play a role in these activities, which means the appropriate event entries need to be captured in the audit logs.

[6] The mandatory cipher suites for TLS vary by the version of TLS and can differ from those required by KMIP. TLS version 1.0 (see IETF RFC 2246) requires TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA, TLS version 1.1 (see IETF RFC 4346) requires TLS_RSA_WITH_3DES_EDE_CBC_SHA, and TLS version 1.2 (see IETF RFC 5246) requires TLS_RSA_WITH_AES_128_CBC_SHA.

- *KMIP Server Compatibility* — An important motivation for using KMIP-based key management is that conforming KMIP Clients can use key management servers from a variety of vendors (e.g., Cryptsoft, HP, IBM, Quintessence Labs, Thales e-Security, Townsend Security, Gemalto, and Vormetric). KMIP Client implementations must be carefully designed to avoid accidentally constraining compatibility (and possibly conformance) due to incorrect interpretations of the KMIP Specification. As an explicit example, the KMIP data type "text string" does not have a maximum length associated with it (nor does it permit null termination); when a "text string" is used for the "Unique Identifier" or "Certificate Issuer Distinguished Name," which are determined by the KMIP Server, the KMIP Client must be prepared to handle both short and lengthy (over 256 characters) strings.
- *Verification of KMIP Conformance* — It is not uncommon for an organization to deploy key management servers from multiple vendors or to change from one vendor to another. As such inter-operability between KMIP Clients and KMIP Servers can be important and it may be necessary to demonstrate this inter-operability as a requisite to deploying in an organization's environment. The Storage Security Industry Forum (SSIF) of the Storage Networking Industry Association (SNIA) has established a KMIP Conformance Test Program that enables vendors with KMIP implementations in their products to test those products for protocol compliance against test tools and other products at the SNIA Technology Center in Colorado Springs, Colorado. This program provides independent verification from a trusted third-party that a given KMIP implementation conforms to the KMIP standard. This verification can give customers confidence that assessed products will interoperate with other similarly-tested KMIP products. Test fees are dependent on the type of product (Client or Server) and the number of profiles that the product is verified against, and whether the company is a member of the SSIF.

3.3 Key management recommendations

Key management is the foundation for the secure generation, distribution, and destruction of keys. Accordingly, ISO/IEC 27040 provides considerable guidance on key use and management.

- Use keys randomly selected from the entire key space.
- Avoid the use of weak keys and check for them, especially when they are user selected. In general, user selected keys should not be used directly as a data encryption key. Further, keys should be difficult enough to be not guessable by an attacker. See NIST SP-800-132 *Recommendation for Password-Based Key Derivation Part 1: Storage Applications* for recommended guidelines.
- Limit the time frame of the use of a key to 2 years, the maximum cryptoperiod recommended by NIST. In certain circumstances, this time period may be considerably shorter.
- Limit the maximum amount of data protected by a key.

- Enforce strict access controls for key generation, change, and distribution. Most key management systems using KMIP implement the necessary controls.
- Use a centralized, interoperable key management infrastructure.
- Key management should be fully automated.
- OASIS KMIP-compliant servers and clients should be used to manage keys.

The OASIS Key Management Interoperability Protocol provides a common protocol that has broad industry acceptance. The OASIS Key Management Interoperability Protocol Specification defines a protocol used for the communication between clients and servers to perform management operations on objects (typically encryption keys) stored and maintained by a key management system. The SNIA Storage Security Industry Forum (SSIF) provides a Key Management Interoperability Protocol (KMIP) Conformance Test Program. See http://www.snia.org/forums/SSIF/kmip for more details.

4 Other Key Management and Encryptions Issues

ISO/IEC 27040 recommends procedures and infrastructures for end users of secure storage systems, especially in large and/or virtualized systems:

- Understand and obey governmental regulations related to encryption and key management.
- Understand and comply with key escrow requirements.
- Have a key compromise recovery plan.
- Have a key backup plan in place.
- Distribute keys securely to devices that access or process the same data.

4.1 Cryptographic Erase

As described in the *SNIA Storage Security: Sanitization* whitepaper, ISO 27040:2015 and NIST Special Publication 800-88R2, when cryptographic erase is used as a data sanitization method, effective and verifiable destruction of all copies of the applicable data encryption/key wrapping keys must be assured. Sound key management processes make it possible to reliably locate all copies (both active and archived) of the relevant keys and destroy them in a verifiable and auditable fashion.

It should be noted that inadvertent loss of the cryptographic keys can produce the same result as performing a cryptographic erase of the data.

4.2 Interactions with data reduction techniques

Data at rest encryption impacts system topology since various forms of data reduction, including deduplication and compression require ordering when combined with data encryption. Typically, data must be reduced before any encryption is performed and likewise expanded after any decryption.

4.3 Import/Export controls

It is important to understand and comply with government regulations for both the import and export of encryption technologies between various countries. Frequently, such regulations prohibit the import of a strong encryption method into a country. Likewise, strong encryption technologies where both the clear text data and the cypher text data can be viewed are considered general purpose encryption devices that usually face export restrictions. These issues are complicated by differing trade agreements that have been constructed with different governments, and usually apply to both data encryption and key management equipment.

Additionally, key escrow may be required either by governmental or corporate requirements. This is an arrangement where keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. Note that key escrow may be required for both data in motion and data at rest.

As an example, a great deal of practical information about United States regulations related to the export of encrypting technologies and equipment can be found at the US Department of Commerce's Bureau of Industry and security website: https://www.bis.doc.gov/index.php/policy-guidance/encryption.

4.4 Recovery plan

Recovery of encrypted data requires both the encrypted data and the keys needed to decrypt that data. As a result, keys need to be distributed to allow redundancy, but must be exchanged in a secure fashion to avoid compromise or corruption of the key. Unintended alteration of the key will also cause a loss of access to the data, so the key management system must provide redundancy and disaster recovery mechanisms for the keys. Recovery plans must also be available in the event that a key is compromised.

4.5 Compliance

Compliance aspects of storage and key management systems that would be of concern in an audit include accountability, traceability, detection and monitoring, sanitization, privacy, and legal requirements. While many of these processes may be in place for the overall computing infrastructure, it is important to extend audit logging to the storage layer. This means maintaining a secure audit log for such events as data encryption, decryption, or destruction of data, and the creation, deletion, and use of keys. Sufficient information must be collected so that the source and a specific individual of such changes can be identified.

5 Summary

Management of data that is secured through the use of encryption is a complex effort, involving all parts of a data system infrastructure. The needs of the data path for adequate protection of the data vary greatly from data in motion to data at rest. The needs of key management systems to secure and protect the keys reflect that complexity.

Not all data needs to be secured. In most instances, only a small part of the data being transferred requires the protection encryption can provide. Carefully reviewing the data to ascertain the confidentially priorities of the data and the flow of that data can result in simplification of the encryption system, while avoiding a costly brute-force approach.

ISO/IEC 27040 has provided clear guidance for these and other areas related to secure storage. It is unique in that it is provide international guidance, pulling together the best practices of international security and storage security communities.

6 Acknowledgments

6.1 About the Authors

Walt Hubis is the owner of Hubis Technical Associates. He provides expertise related to storage interface and storage security standards organizations with a focus on protocols and software interfaces and how innovative and disruptive computer storage technologies impact these standards. Walt has over twenty-five years of experience in storage systems engineering in both development and managerial positions and has authored several key patents in RAID and other storage related technologies. He is the vice-chair of the SNIA SSSI Initiative and has served as the Chair of the Trusted Computing Group Key Management Services Subgroup, Chair of the IEEE SISWG P1619.3 Key Management subcommittee, and Secretary of the IEEE Security in Storage work group (SISWG). Walt holds a Bachelor of Science degree in Electrical Engineering.

Eric Hibbard is the CTO Security and Privacy in Hitachi Data Systems where he is responsible for product security strategies and oversees the integration of security and privacy measures in products and services. Mr. Hibbard is a senior security and IS auditor professional with 30+ years of experience in enterprise-class ICT, working for government (DoD, DoE, and NASA), academia (University of CA), and industry. He is actively involved in a wide range of technologies and represents Hitachi and HDS in several standards development organizations (ISO/IEC, ITU-T, INCITS) and industry associations (SNIA, TCG, DMTF, ODCA, IIC, ISACA, ISSA). He currently serves as the International Representative for INCITS/CS1 Cyber Security, Chair of the IEEE Information Assurance Standards Committee, Co-Chair of the Cloud Security Alliance International Standardization Council, Co-Chair of the ABA Electronic Discover & Digital Evidence (EDDE) Committee, Co-Chair of the ABA IoT Committee, Vice Chair of the ABA Cloud Computing Committee, Chair of the SNIA Security TWG, and Vice Chair of the IEEE Security in Storage WG (SISWG). In addition, he is currently the Editor of ISO/IEC 27050 (Electronic discovery) and ISO/IEC 20648 (TLS for Storage Systems) draft standards as well as the recently published ISO/IEC 27040:2015 (Storage security) and Rec. ITU-T Y.3500 | ISO/IEC 17788:2014 (Cloud computing - Overview and vocabulary). Mr. Hibbard currently holds the (ISC)2 CISSP certification with the ISSAP, ISSMP, and ISSEP concentrations and the CCSP certification as well as the ISACA CISA certification. His educational background includes a B.S. in Computer Science and a Certificate of Proficiency in Data Communications.

6.2 Reviewers and Contributors

The Security TWG wishes to thank the following for their contributions to this whitepaper:

Richard Austin, CISSP	HP
Dr. Alan Yoder	Huawei Technologies Co. Ltd.
Mark Carlson	Toshiba America Information Systems, Inc.
Gary Sutphin	Individual
Roger Cummings	Antesignanus Inc.

7 For More Information

Additional information on SNIA security activities, including the Security TWG, can be found at http://www.snia.org/security.

Suggestion for revision should be directed to http://www.snia.org/feedback/.

The ISO/IEC 27040 standard can be purchased at http://www.iso.org.

Appendix A. Overview of ISO/IEC 27040

The International Organization for Standardization (ISO), in conjunction with the International Electrotechnical Commission (IEC), under Subcommittee 27 (SC 27) of the Joint Technical Committee 1 (JTC 1) is nearing completions of a standard to address storage security. This is noteworthy since a major element of SC27's program of work (see Appendix B) includes International Standards for information security management systems (ISMS), often referred to as the ISO/IEC 27000-series, including ISO/IEC 27001 (criteria used for ISMS certification of organizations).

The full title of the new SC27 storage security standard is ISO/IEC 27040:2014, *Information technology — Security techniques — Storage security*. The purpose of ISO/IEC 27040 is to provide security guidance for storage systems and ecosystems as well as for protection of data in these systems; it supports the general concepts specified in ISO/IEC 27001. It is relevant to managers and staff concerned with data storage and information security risk management within an organization and, where appropriate, external parties supporting such activities.

The standard provides relevant terminology, including the following important definitions:

- ***Storage security*** - application of physical, technical and administrative controls to protect storage systems and infrastructure as well as the data stored within them

  Note 1 to entry: Storage security is focused on protecting data (and its storage infrastructure) against unauthorized disclosure, modification, or destruction while assuring its availability to authorized users.

  Note 2 to entry: These controls may be preventive, detective, corrective, deterrent, recovery, or compensatory in nature.

- ***Data breach*** - compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed

Since data breaches are a major area of concern (common types are addressed in this standard), this definition plays a pivotal role throughout the standard. Historically, the storage industry was only worried about unauthorized disclosure/access, but his new definition, which is aligned with the new EU General Data Protection Rules, adds destruction, loss, and alteration. This potentially means that individuals involved with storage could now be a party to a data breach due to an action that causes data loss or corruption (e.g., from a failed microcode updated).

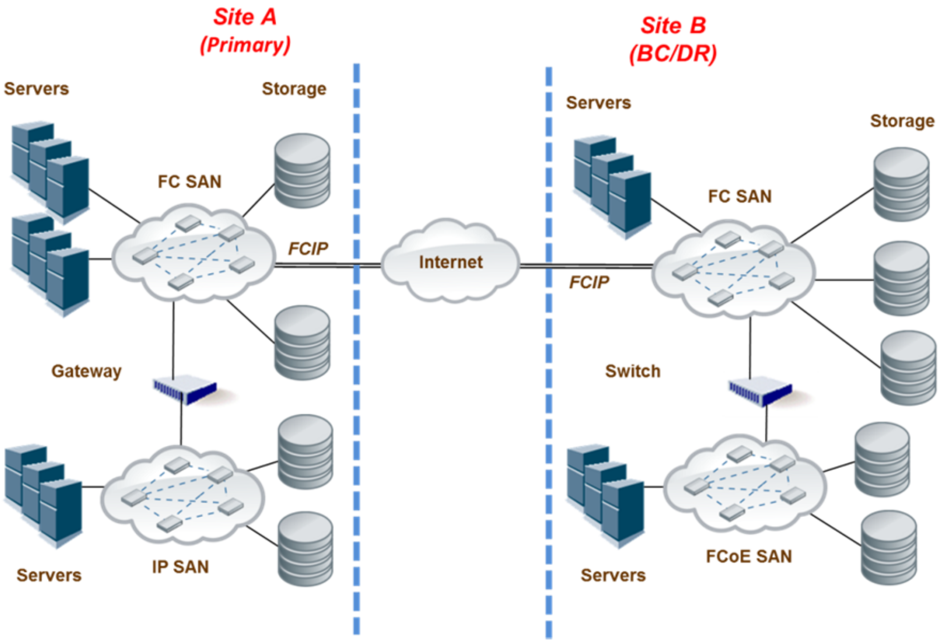
ISO/IEC 27040 approaches storage security guidance from two angles: 1) supporting controls and 2) design and implementation of storage security. Both are addressed in sufficient detail that storage professional with limited security knowledge and security/audit professionals with little storage background can leverage the materials.

Storage Security - Supporting Controls

The supporting controls clause in ISO/IEC 27040 identifies the controls (measures) that support storage security architectures, their related technical controls, and other controls (technical and non-technical) that are applicable beyond storage. Each of the following is addressed:

- Direct Attached Storage (DAS)
- Storage networking (multiple flavors of SAN and NAS)
- Storage management
- Block-based storage (Fibre Channel and IP)
- File-based storage (NFS, SMB/CIFS, pNFS)
- Object-based storage (cloud, OSD, CAS)
- Storage security services (sanitization, data confidentiality, and data reductions)

No storage technology is recommended over another. Instead, the guidance is provided in a manner that makes it clear as to what is needed/expected from a security perspective when particular storage technologies are selected or deployed. The standard also considers complex scenarios as shown in the figure.



(Source: ISO/IEC 27040:2014, Figure 2; developed by SNIA Security TWG)

Storage Security - Design and Implementation

Designing and implementing storage solutions requires adherence to core security principles. ISO/IEC 27040 addresses these design principles from a storage security perspective and leverages the supporting controls to counter storage security threats and vulnerabilities. The basic premise is that design failures can lead to significant problems (i.e., data breaches).

The materials in this clause cover the following:

- Storage security design principles (defense in depth, security domains, design resilience, and secure initialization)
- Data reliability, availability, and resilience (including backups and replication as well as disaster recovery and business continuity)
- Data retention (long-term and short/medium-term retention)
- Data confidentiality and integrity
- Virtualization (storage virtualization and storage for virtualized systems)
- Design and implementation considerations (encryption and key management issues, alignment of storage and policy, compliance, secure multi-tenancy, secure autonomous data movement)

The secure multi-tenancy and secure autonomous data movement (similar to ILM security) are advanced issues and they are likely to have broader applicability (e.g., cloud computing).

Value-added Elements of ISO/IEC 27040

A significant effort was made to enhance the applicability and usability of ISO/IEC 27040, which lead to the incorporation of the following:

- ***Media Sanitization*** - The standard includes an annex that provides detailed information (similar to NIST SP 800-88r1) on ways to sanitize different types of storage media. The techniques span the use of overwriting approaches through cryptographic erasure (key shredding). This is the only International Standard providing detailed coverage of this topic and it is structured such that it can be referenced like the 1995 version of DoD 5220.22-M document, which is often used by vendors.
- ***Selecting Storage Security Controls*** - It was recognized that organizations would not be able to address the 330+ controls provided in ISO/IEC 27040. To avoid an all-or-nothing scenario, an annex was developed to help prioritize the selection and implementation of storage security controls, based on security criteria (i.e., confidentiality, integrity, availability) or data sensitivity (low or high). This annex can also be used as a checklist by auditors for storage systems and ecosystems.
- ***Important Security/Storage Concepts*** - Given the disparate target audiences (security, storage, and audit), it became clear that certain "tutorial" materials needed to be provided to ensure a common understanding of certain concepts. As such, these details are provided in an annex, which briefly covers topics such as authentication,

authorization and access control, Self-Encrypting Drives (SED), sanitization, logging, N_Port_ID Virtualization (NPIV), Fibre Channel security, and OASIS KMIP. The Fibre Channel materials are especially important because this is one of the few places FC-SP-2 and other FC security mechanisms are explained.

- ***Bibliography*** - Normally, the bibliography of a standard is of marginal value. In ISO/IEC 27040, however, this is not the case because it represents the go-to list for relevant storage security information. One might consider it the core source material for storage security.

Summary

As data breaches persist, organizations are scrambling to find additional ways to protect their systems and data. Storage security is often overlooked and may be pressed into service as a last line of defense. ISO/IEC 27040 provides the details that can help accomplish this.

ISO/IEC 27040 is a "guidance" standard (i.e., everything is specified as "should"). It is relatively easy to turn this guidance into requirements by specifying that some or all of the guidance *shall* be implemented, or in the case of materials directed towards a vendor (e.g., RFP), the vendor *shall provide* the capabilities/functionality necessary to implement the ISO/IEC 27040 guidance (some or all).

Appendix B. Overview of ISO/IEC JTC 1/SC27

The International Organization for Standardization (ISO) is the world's largest developer of voluntary International Standards and it is an independent, non-governmental organization made up of members from the national standards bodies of 164 countries and 3,368 technical bodies.[7] Since its founding in 1947, ISO has published over 19,500 International Standards covering almost all aspects of technology, business, and manufacturing (e.g., from food safety to computers, and agriculture to healthcare).

Founded in 1906, the International Electrotechnical Commission (IEC) is the world's leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies, collectively known as "electrotechnology."[8] "Over 10,000 experts from industry, commerce, government, test and research laboratories, academia and consumer groups participate in IEC Standardization work."

ISO and IEC are two of the three global sister organizations (International Telecommunication Union, or ITU, being the third) that develop International Standards for the world. When appropriate, some or all of these SDOs cooperate to ensure that International Standards fit together seamlessly and complement each other. "Joint committees [e.g., JTC 1] ensure that International Standards combine all relevant knowledge of experts working in related areas." All ISO/IEC International Standards are fully consensus-based and represent the needs of key stakeholders of every nation participating in ISO/IEC work. "Every member country, no matter how large or small, has one vote and a say in what goes into an [ISO or] IEC International Standard."

Subcommittee 27 (SC27)

Within JTC 1, SC27 has responsibility for the development of standards for the protection of information as well as information and communications technology (ICT). This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;

[7] *About ISO*, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, http://www.iso.org/iso/home/about.htm (last visited September 15, 2014).

[8] *About the IEC*, INTERNATIONAL ELECTROTECHNICAL COMMISSION, http://www.iec.ch/about/?ref=menu (last visited September 15, 2014).

- Conformance assessment, accreditation and auditing requirements in the area of information security;
- Security evaluation criteria and methodology.[9]

Since convening its first plenary session in April 1990, SC27 has published more than 120 standards and it currently has in excess of seventy-five active projects. To manage these projects and the on-going maintenance associated with the published standards, SC27 is organized into the following working groups (WGs)[10]:

- WG 1: Information security management systems (ISMS)
- WG 2: Cryptography and security mechanisms
- WG 3: Security evaluation, testing, and specification
- WG 4: Security controls and services
- WG 5: Identity management and privacy technologies
- SWG-M: Special working group on management items.
- SWG-T: Special working group on transversal items.

[9] International Organization for Standardization/ International Electrotechnical Commission [ISO/IEC], *SC 27 Business Plan October 2013—September 2014*, at 1.2, ISO/IEC JTC 1/SC 27 N12830 (Sept. 30, 2013).

[10] *ISO/IEC JTC 1/SC 27 IT Security techniques*, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, http://www.iso.org/iso/iso_technical_committee?commid=45306 (last visited May 15, 2014).

Bibliography

[01] ISO/IEC 27040:2015, *Information technology – Security techniques – Storage security*

[02] ISO/IEC 11770-1:2010, *Information technology -- Security techniques -- Key management -- Part 1: Framework*

[03] NIST Special Publication (SP) 800-57 Part 1-3, *Recommendation for Key Management*

[04] NIST Special Publication (SP) 800-88 (R2), *Guidelines for Media Sanitization*

[05] NIST Special Publication (SP) 800-111, *Guide to Storage Encryption Technologies for End User Devices*

[06] NIST Special Publication (SP) 800-132, *Recommendation for Password-Based Key Derivation Part 1: Storage Applications*

[07] Storage Networking Industry Association (SNIA), *Storage Security: Fibre Channel Security,* Draft

[08] Storage Networking Industry Association (SNIA), *Storage Security: Sanitization*

[09] IETF RFC 1334, *PPP Challenge Handshake Authentication Protocol (CHAP)*

[10] IETF RFC 2246, *The TLS Protocol Version 1.0*

[11] IETF RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*

[12] IETF RFC 2406, *IP Encapsulating Security Payload (ESP)*

[13] IETF RFC 2451, *The ESP CBC-Mode Cipher Algorithms*

[14] IETF RFC 3686, *Using Advanced Encryption Standard (AES) Counter Mode*

[15] IETF RFC 3720, *Internet Small Computer Systems Interface (iSCSI)*

[16] IETF RFC 3721, *Fibre Channel Over TCP/IP (FCIP)*

[17] IETF RFC 3723, *Securing Block Storage Protocols over IP*

[18] IETF RFC 4171, *Internet Storage Name Service (iSNS)*

[19] IETF RFC 4346, *The Transport Layer Security (TLS) Protocol Version 1.1*

[20] IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*

[21] OASIS *Key Management Interoperability Protocol Specification Version 1.2*