TCG Storage Specifications and Key Management

December 2009

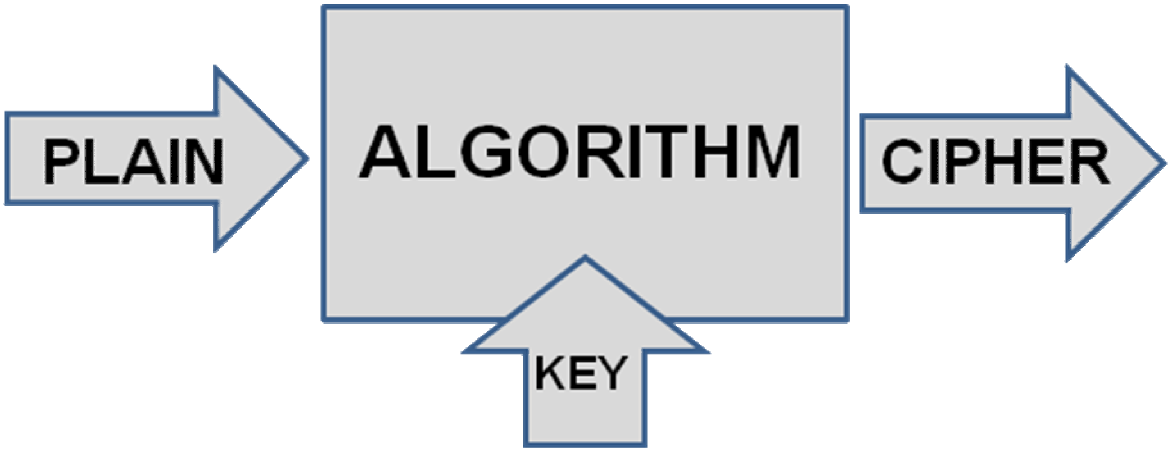
Trusted Computing Group
3855 SW 153rd Drive, Beaverton, OR 97006
Tel (503) 619-0562 Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

"Key management is the hardest part of cryptography and often the Achilles' heel of an otherwise secure system." – Bruce Schneier, Preface to *Applied Cryptography*, Second Edition.

The Trusted Computing Group has published specifications for trusted storage. Storage manufacturers have announced and shipped products designed to those specifications, including self-encrypting drives (SED), both hard (rotating) drives and solid state drives, for laptops and data centers. Not only is cryptographic key management simplified and available for SEDs today, but recent work on key management holds great promise for unifying and standardizing key management for SEDs and other cryptographic systems across the enterprise.

Cryptography 101

Cryptography is the science of secret writing. Good security practice for cryptography dictates that the algorithm (i.e., the mechanics) of a cryptographic system be openly known by all parties, published, and even standardized. In other words, there are no secrets in the way the system works. The only secret is the key – a parameter selected by the user or using system -that governs the specific operation of the system:



Once the secret key is selected, PLAIN text is fed into the known ALGORITHM, whose specifications are governed by the KEY, and CIPHER (encrypted) output is produced. The CIPHER can be stored or transmitted. Recovery of the PLAIN from the CIPHER consists of putting the CIPHER through the ALGORITHM in “reverse” order, governed by the KEY, and producing PLAIN. The key for the U.S. Advanced Encryption Standard (AES) is a binary string of three possible lengths: 128, 192, or 256.

Cryptography comes in two flavors:

- **Symmetric:** Encrypt and decrypt keys are the same.
- **Public key:** encrypt and decrypt keys are different.

The “strength” of the cryptographic system depends on two things:

- The **ALGORITHM** produces “random-looking” **CIPHER** from any **PLAIN**
- The difficulty of guessing or re-producing the **KEY**

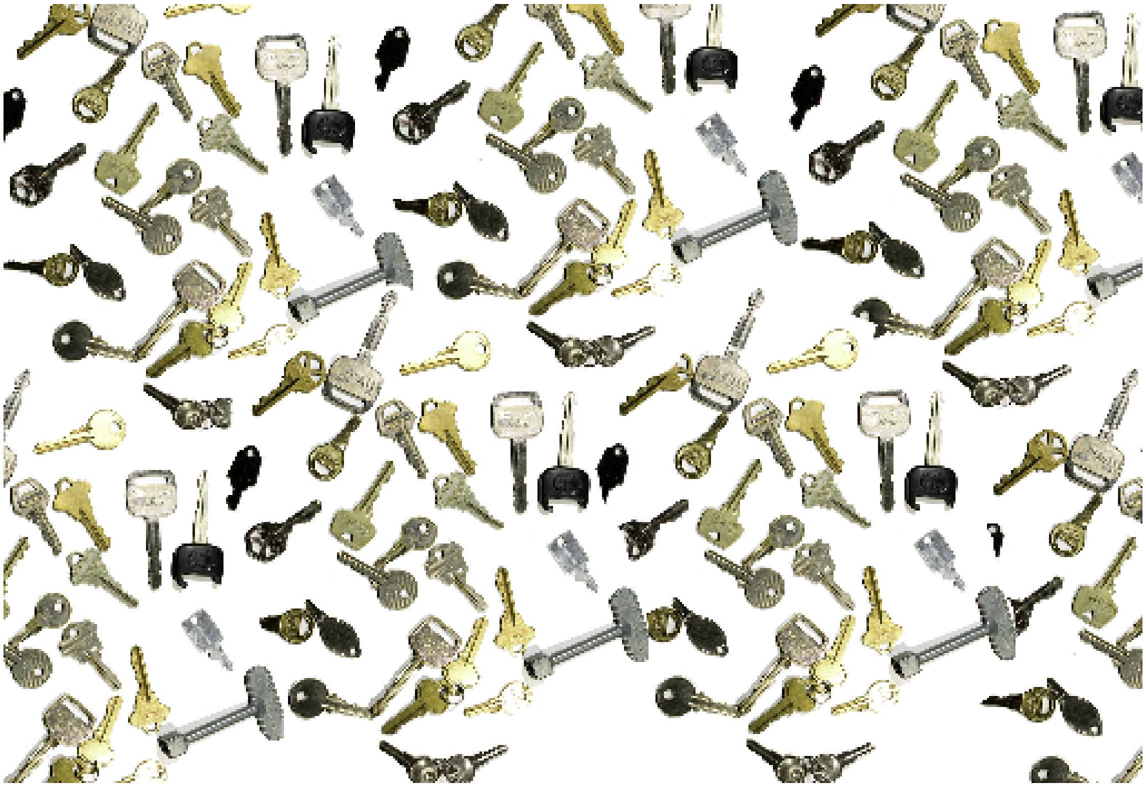
ALGORITHM strength is determined through exhaustive analysis and mathematical proof. KEY strength is usually determined by selecting the KEY at random from a large key space (= all possible keys). For example, there are 2128 possible 128-bit AES keys, which is about

340,000,000,000,000,000,000,000,000,000,000,000,000

“Exhaustive search” (or brute force attack) over the key space requires an attacker to test all possible keys, looking for the one key that converts the captured CIPHER into meaningful PLAIN. Very large key spaces make exhaustive search difficult, at least with present or anticipated computing machinery.

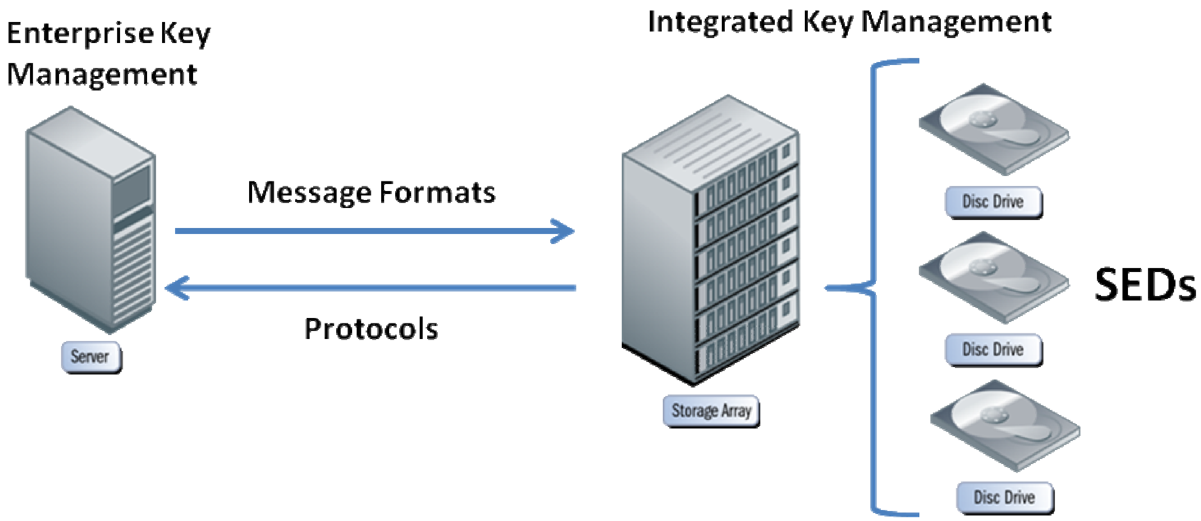
Key Management

With good ALGORITHM strength, the security of any cryptographic system depends on how well the key is protected from an adversary during its lifetime. Such key management can include generation, exchange, storage, safeguarding, use, vetting, replacement and finally, destruction of a key. Since a large enterprise is typically employing cryptography in a number of situations, many keys may require management at the same time. There are a number of publications 1, 3, 4, 5 detailing best practices for security in general and key management in particular. In the mind of the security manager, the challenging landscape may appear like the following graphic:



(Keys! Keys! Keys! courtesy of Walt Hubis: www.hubis.com)

Key management comes in two basic flavors: integrated and enterprise 11. An integrated system has the key management built into the system. For example, self-encrypting drives (SED) have ‘local’ key management built right into the drive. Similarly, a RAID system containing multiple SEDs may provide the key management for all the SEDs from within the RAID controller. Enterprise key management means that a consolidated, central key management server provides service to multiple cryptographic systems. For example:



Multiple storage arrays may interface their local, integrated key management into a central enterprise key management server. This key management server serves the life cycle functions to its clients: the distributed cryptographic systems. The language between the key management server and clients consists of protocols composed of messages exchanged between the server and client. For example, the client may request a new key and the server will respond with a newly-generated key. All such messages are themselves securely authenticated and protected. A central key management server provides consistent enterprise-wide security policy execution, including archiving and scheduled updates of keys. Today, nearly all such enterprise key management systems are proprietary. The "holy grail" of key management would be a standardized and widely-adopted system. Before reviewing the status of standardization, consider key management in the context of the Trusted Computing Group (TCG) Storage Specifications (www.trustedcomputinggroup.org).

TCG Storage Specifications

The Storage Work Group of the Trusted Computing Group has published a Core Specification and several context-specific subsets of the Core Specification, called Security Subsystem Classes (SSC). SSCs are published for optical, workstation/laptop, and enterprise/data center storage devices (e.g., drives). Each SSC defines how to build security directly into storage, including self-encryption. The Specifications also support integrated key management for the self-encrypting drive (SED) function. With self-encryption, the cryptographic key for the AES algorithm is generated in the factory by an on-board random process. The storage system is thus 'born' as a cryptographic device: encrypting everything written to storage and decrypting everything read from storage. Since the cryptography is self-contained, the key never leaves the drive, eliminating the need to do key management for the on-board cryptographic key. For re-use, end-of-life, or safe off-site transport of drives, deleting and replacing the key causes the encrypted data on the storage system to be unreadable,. This is called "instant erase". With the new key, the storage system can be re-formatted and re-used; however, the old data is gone.

If the user is further concerned about loss or theft of the storage system, the user can optionally introduce an authentication key during initialization of the storage system. The authentication key is understood by the storage system and is used to lock the storage system, which is unlocked for use by presentation of the authentication key. Thus, the (optional) authentication key requires external key management. An SED configured with authentication key(s) provides protection against loss or theft (or snooping), since it is locked to unauthorized users and all on-board data is encrypted; plus, end-of-life, re-purposing, sending out for repair or replacement are all supported by "instant erase".

The TCG Storage Work Group has published a Key Management Application Note on how to locally manage the authentication keys for SEDs by exploiting the standard interface defined in the TCG Storage

Specifications. This local, integrated, authentication key management has been tied into enterprise key management servers for centralized key management. Key management products designed to these Specifications are available today for both laptops and data centers. The information technology community would further benefit from having a standard for enterprise key management applicable to all cryptographic systems, instead of the current state: a multitude of proprietary systems.

For laptop SEDs, many workstation security software vendors are providing local SED management systems with sophisticated capabilities and user-friendly interfaces. Such vendors are further tying this local key management support to centralized servers to support automation and other key management life cycle services across an enterprise of end-user laptops.

Data center storage system vendors are also providing local (eg, RAID controller-based) but automated SED key management that is tied back to centralized servers.

Complete systems are available today for both SED laptops and data centers in the enterprise.

Key Management Standards

Recall that key management must deal with the full life-cycle of keys: generation, exchange, storage, safeguarding, use, vetting, replacement and finally, destruction of a key. In addition to numerous integrated key management systems, subsets of the full enterprise key management life-cycle have been defined, built, and occasionally standardized over the years. The subset may be based on: life-cycle phase, applicable industry, grammar/syntax used, or other aspects. Recent work includes IEEE 1619.3 (in process) 6, W3C XKMS 9, and the OASIS EKMI TC 8. Classical work includes ISO X9 10, applicable to the financial industry. Since the on-board, integrated key management for SEDs has been defined and published by the TCG, SED developers, integrators, and especially users are interested in how emerging enterprise key management systems will “harmonize” (that is, interface) with the on-board key management.

A promising exercise in this regard is the work of the **OASIS Key Management Interoperability Protocol (KMIP) Technical Committee 2** (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip). KMIP was initiated by four important vendors in the key management community: IBM, HP, RSA, and Thales/nCipher. Since its inception, KMIP has been joined by a number of other key management providers. KMIP is focused on the Message Formats and Protocols (as shown above). The output of KMIP promises to provide the long-sought goal of a standardized, enterprise key management system.

To quote from the draft KMIP specification (note: ‘normative’ means part of the formal specification, from a conformance perspective):

“In addition to the normative definitions for managed objects, operations and attributes, this specification also includes normative definitions for the following aspects of the protocol:

- The expected behavior of the server and client as a result of operations
- Message contents and formats
- Authentication profiles for clients and servers
- Message encoding (including enumerations)
- Error handling”

As to schedule, Bob Griffin of RSA and co-chair of the KMIP Technical Committee, says:

“We hope to make the draft V1.0 KMIP spec and other documents available for 60-day public review in October. Depending on the results of that review, we would be able to have an approved OASIS standard in early January 2010. Included materials: KMIP Specification (normative), KMIP Usage Guide (illustrative), KMIP

Use Cases (illustrative) and KMIP Profiles (illustrative). I would also expect a number of supporting materials, such as an updated white paper and presentation materials. The normative conformance statement will be in the KMIP Specification. I anticipate that we will have a separate KMIP Profiles document that encourages interoperability through detailing essential KMIP elements that must be supported for particular domains of use (eg, creation of symmetric keys by the server)."

As to the complementary work of the OASIS EKMI TC 8, Griffin observes that "EKMI is particularly focused on application-level XML services rather than the message-level marshalling of KMIP".

Walt Hubis, LSI/Engenio and one of the technical leads on both IEEE 1619.3 6 and KMIP, is working on the "harmonization" issues with respect to other standards activities, including IEEE 1619.3 and TCG. Hubis also wrote the Key Management Application Note from TCG Storage, so he is in a unique position to well-understand the nuances of such harmonization. Hubis notes that "we in IEEE 1619.3 are actively working on getting the changes into our draft specification to be compatible with the KMIP specification." As to harmonization with TCG, Hubis said: "We expect a similar time frame (to KMIP), perhaps lagging just a bit."

The bottom line is that KMIP is on track for early 2010, is supported by major key management providers, and is actively working to harmonize with several other key management initiatives, most importantly: TCG Storage and SEDs.

At least one vendor has already announced a product designed to the KMIP specifications.

Jorge Campello, Hitachi/HGST and chair of the TCG Storage Work Group stated that:

"Software vendors participate in TCG and in the Storage Work Group and have become very active in helping to shape the Storage WG specs. We envision that solutions for corporate and consumer PC client environments will continue to be provided by vendors that participate in and/or track the TCG Storage WG specs. We further believe that the enterprise-environment key management solutions will continue to be developed in these other standards bodies and we will continue to do liaison work to make sure there are no compatibility issues."

Jon Oltsik, Principal Analyst, Enterprise Strategy Group, and a recognized expert on security, cryptography, and key management, speculates that:

"As encryption technologies become more and more ubiquitous, data security and integrity will depend upon strong and scalable key management services across the enterprise. Unfortunately, today's key management systems are immature and proprietary and thus inappropriate for enterprise requirements. The industry desperately needs a set of key management standards soon; I am hopeful that the OASIS KMIP effort and the multitude of leading vendors participating will fill this void. If OASIS KMIP comes to fruition as I expect, it will encourage organizations to expand their use of cryptographic technologies and therefore have a profound impact on overall data security."

Since SEDs are superior to other options for storage encryption as protection for loss/theft and to support re-purposing, off-site shipment, and end-of-life scenarios, the I.T. security community and end users should begin integration of SEDs, both laptop and data center, into their enterprises now, in order to meet security best practices and to satisfy encryption safe harbor conditions in breach notification legislation. Evolving key management standards, most notably OASIS/KMIP, will help consolidate SED key management systems that exist and are operational today with other cryptographic systems in use in the enterprise.

Selected References

1. SNIA/SSIF Security Best Practices:

http://www.snia.org/forums/ssif/forums/ssif/programs/best_practices/

2. OASIS KMIP TC:

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

3. OASIS survey of KM:

http://xml.coverpages.org/keyManagement.html

4. "Best Practices for Key Management for Secure Storage." By Walt Hubis (LSI Corporation). A project of the SNIA Education Committee:

http://www.snia.org/images/tutorial_docs/Security/WaltHubis-Best_Practices_Secure_Storage.pdf

5. NIST SP 800-57: Recommendation for Key Management:

http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

6. IEEE 1619.3: Key Management:

http://siswg.net/

7. IETF: Provisioning of Symmetric Keys:

http://www.ietf.org/dyn/wg/charter/keyprov-charter.html

8. OASIS EKMI TC: Enterprise Key Management Infrastructure:

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ekmi

9. W3C XML Key Management (XKMS):

http://xml.coverpages.org/keyManagement.html#w3c

10. ANSI X9 Financial Industry:

http://xml.coverpages.org/keyManagement.html#ansi-X9

11. Enterprise KM (centralized) versus Integrated KM (.built-in key management system of a specific encryption solution):

http://www.scmagazineus.com/Enterprise-key-management-deciphered/article/126075/