SPECTRA

SPECTRALOGIC.COM

WHITE PAPER

Encryption: Managing Keys and Data

JANUARY 2006

Encryption: Managing Keys and Data

CONTENTS

Executive Summary

The business case for encrypting backed up data is clear-cut. The urgency to provide encryption continues to escalate as regulations and laws mandate encryption to protect personal, financial, and sensitive corporate data.

With the advances in technology and cryptography, it turns out that encryption itself isn't hard—for example, the AES-256 encryption algorithm has already been implemented in hardware and put into wide use. Instead, the difficult aspects of stored data encryption involve key management: creating keys, protecting keys, and linking keys to encrypted data all while maintaining security.

Key management itself can be conceptually distilled to a standard set of processes:

- Setting up security authorizations so that the creation of and access to key data is limited to only select administrators.
- Protecting the encryption key, so that the cleartext (unencrypted) version is never displayed publicly.
- Associating the key with the data it encrypts, while protecting the key value itself.
- Storing the key in a remote location, so that the encrypted data does not reside in the same physical location as the data encrypted using the key.
- Decrypting and restoring data in a manner that is practical yet secure.
- Deleting encrypted data.

Key Management: The Basics

Encryption of stored data implements symmetric, or private-key, encryption. That is, every key is private; and after the key is created, it must be protected and stored. Private key encryption differs from e-commerce-related encryption, where typically a Public Key Infrastructure (PKI) is used, with a public key that is freely available, along with a private key, that may be required for only a single transaction or session. Security on spinning disk is similarly simpler; for example, keys only have to be retained until the data is encrypted with a new key. When a new key is used to encrypt data, data formerly encrypted with a previous key is encrypted using the new key—so there is no need for the old key. Protocols that protect transmitted data, such as SSL, use instant, temporary key creation, then deletion. Again—no need to preserve keys over a long period.

Private key encryption permits a different type of data protection and security in that a single, possibly never-revealed key is used to both encrypt and decrypt data. The price of this encryption method is that you must protect the key so the data, which has been encrypted using that key, can't be decrypted by unauthorized users. You also need to recover the right key for each encrypted data set, or your data cannot be decrypted. If you lose the key, consider the data deleted—at least, most regulatory bodies accept key deletion as data deletion.

With private key encryption, the life cycle of an encryption key includes four stages:

- Key Creation and Use
- Key Escrow
- Key Use in Data Decryption
- Key Deletion

A key management system, central to any encryption system, needs to handle every phase of the key's life cycle. The Spectra BlueScale Encryption key management system is used to illustrate how key management requirements across the key's life cycle can be translated into specific features.

Phase I: Key Creation and Use

Creating, using, and storing a key locally constitute the first phase of the key's life cycle. A few tasks fall to administrators; these simply cannot be logically provided by key management software. The first: identify and track the library users with encryption privileges and make sure that their passwords are accessible in case of a disaster or emergency.

In creating keys, the key management system needs to protect the keys by:

- **Allowing only authorized users to create the key**. Additionally, a secure system may require multiple users to login prior to permitting key creation. Spectra Logic's BlueScale Encryption Professional Edition requires multiple authorized users to access the system prior to key creation. All versions of BlueScale Encryption provide a special category of user—an encryption administrator—so that standard library administrators, operators, and even super users are barred from the encryption function.
- **Creating secure keys that are difficult or practically impossible to break**. Two elements go into creating secure keys: length and the use of true random numbers to generate the keys. BlueScale Encryption implements AES-256, using the longest possible key length of 256 bits. BlueScale Encryption also uses a hardware-based true random number generator (TRNG) to seed encryption keys. Generating random numbers without bias is difficult. Hardware-based random number generation is much more accurate in generating truly random numbers than any other method, including software-based random number generators.
- **Hiding the key's true value**. The BlueScale system protects keys in multiple layers. First—and foremost from a user perspective—the system lets the key creator assign a key nickname, or moniker. Users always reference the key's moniker, rather than the key's real value (the 256-bit key). Further, the key's value is encrypted. The encryption method is based on a pass-phrase supplied by the encryption user. This is used to a create one-way hash of the key value, which is then encrypted. Decrypting the key from this state, then, requires an authorized user and a key-specific pass-phrase. (Some systems store keys in cleartext in databases, or give users the option of not encrypting the key. This weakens the encryption implementation altogether.)

Phase II: Key Escrow

Key escrow, also called key storage, is a critically important aspect of key management. Remote storage in a location other than that storing the encrypted data is important to the integrity of the encrypted data. It is also important to ensure that the key is available for data decryption. Off-site key storage makes sense in the same way that off-site tape storage makes sense: in the case of a disaster, a data center may be destroyed or rendered unusable, but the data on tape, and the key to decrypt the data, can be pulled together to restore data and if necessary, to rebuild the business. To escrow keys, an administrator needs to identify a remote storage site or a trusted third-party escrow service, then make sure that copies of the keys are stored at this site or by this service.

Key management software that permits and protects key escrowing includes features that let users:

- **Copy the key**. The copy can be sent to a third-party or off-site. The BlueScale key management system lets you copy an encrypted version of the key to a USB device. Alternately, you can e-mail the encrypted key to a trusted party.
- **Protect the copied key**. BlueScale Encryption lets only authorized users export or copy keys. Further, the key is encrypted using a pass-phrase that the encryption administrator assigns to the key. To access the e-mailed or stored key, the pass-phrase is required. Best practices recommend that you send the pass-phrase using a different method from that used to send the key. Keep the two processes separate. For example, you can e-mail the key and use the telephone to convey the pass-phrase, or send the USB device using surface mail, then e-mail the pass-phrase.
- **Supplement security with advanced methods of key protection**. BlueScale Encryption professional edition lets you split a single key across multiple USB devices, with a password required for each USB device to which the key is written. The key can then be restored with M-of-N shares—that is, not all parts, or shares, (N) need to be present to restore a key; instead, you only need a subset (M) of the key parts to restore the data. This is more secure than requiring only a single pass-phrase.

Administrator key-escrow tasks that cannot be logically provided by encryption key management software include:

- Identifying an off-site key storage location or service, then using it.
- Tracking every copy of the key that is created.
- Storing the pass-phrase used to encrypt the key.

Phase III: Key Use in Decrypting Data

Data decryption and recovery depends on pulling together the right tapes, the right key or keys, and the right hardware to support the decryption.

- To decrypt data, you need to be able to associate the encrypted data with the key used to encrypt it. The encryption key management system needs to support these associations securely, without revealing the key's value. BlueScale Encryption handles this by writing encryption moniker information with data as the data is encrypted, so that when a tape with encrypted data is then loaded into a library, the BlueScale software checks to see if the matching key—revealed only by its moniker—is available on the library. If the key is not available, the encryption software tells you the moniker of the key that is required to decrypt the data.

- The most reliable key management and encryption systems provide multiple methods to choose from in decrypting data. In optimal cases, you'll decrypt and restore data using a system, such as an appliance or library, similar to the one used to encrypt and store the data. However, make sure an alternate method is available. For example, BlueScale Encryption supports two decryption methods. The most straightforward method involves decrypting data using a Spectra library with BlueScale Encryption. The graphical display makes it easy to import the key, then decrypt and restore the data.

  BlueScale Encryption also supports a software-only method of data decryption. This solution requires a Red Hat(R) Linux server, a copy of Endura™ Decryption Utility (EDU) software, and drives that can read data from the encrypted tape, and send the decrypted data to another tape so that the data can be restored using the appropriate backup software application. Although not as straightforward as using the Spectra library, this method lets you decrypt and restore data rapidly, regardless of your environment and with only a minimum of readily available equipment.

Phase IV: Deleting Keys

Encrypted data is considered deleted once all copies of its key are destroyed. The key management software needs to provide a feature that deletes specific encryption keys. Note that data deletion may be mandated by law, such as HIPAA, and that this method of data deletion is the by far the simplest and most cost-effective method of deleting data.

The role of the administrator in this process: make sure every copy of a key is identified.

The key management software must provide a feature that lets you delete a key. The BlueScale key management software option is easy to use. If the key is on the library, delete it using the key management software. If the key is on a USB device, delete the key from the device. The data is then considered deleted, as well. Even though data encrypted using the key may still be stored, the data is inaccessible.

Conclusion

Encrypting data is easy. Tracking and managing the keys used to encrypt and decrypt data is the real challenge. Make sure that any encryption solution you choose provides comprehensive key management features, including those reviewed here. The taxonomy presented in this white paper applies particularly to systems implementing the encryption of secondary storage, where keys may need to be retained for long periods.

Managing a key across its life cycle requires a balance between security and ease of data decryption and restoration. You'll have to identify the right level of security for your data and your site. Regardless, the key management system needs to let you easily create and use keys, escrow keys, access keys when you need to decrypt data, and destroy keys at the end of the key life cycle.

References

Denning, Dorothy E. and Dennis K. Branstad, "A Taxonomy for Key Escrow Encryption Systems," *Communications of the ACM*, Vol. 39, No. 3, March 1996.

Spectra Logic Corporation
1700 N 55th Street
Boulder Colorado 80303 USA
800.833.1132
303.449.6400

Spectra Logic Europe Limited
Magdalen Centre
Robert Robinson Avenue
Oxford Science Park
Oxford UK OX44 7 RW
+44 (0) 870.112.2150