Guidelines for Media Sanitization

HPE Enterprise Secure Key Manager

Modern storage environments are rapidly evolving. Data may pass through multiple organizations, systems, and storage media in its lifetime. The pervasive nature of data propagation is only increasing as the Internet and data storage systems move towards a distributed cloud-based architecture. As a result, the efficient and effective management of information from inception through disposition is the responsibility of all those who have handled the data.

How HPE Enterprise Secure Key Manager helps customers meet requirements

Easily redeploy servers and disks
Managing the costly and time-consuming sanitization and destruction services for servers and disks, as well as redeployment of hardware assets from sensitive areas to more operational areas has traditionally been difficult. Today, with HPE Enterprise Secure Key Manager (ESKM), companies can quickly shred the encryption key, rewrite the disk, and immediately redeploy assets as required.

The ability to eliminate these costly and time-consuming key management procedures required by mandates and best practices to keep sensitive data safe, brings immediate return on investment (ROI) and helps increase the total cost of ownership (TCO) of data center infrastructures. This simple use case can save companies thousands of dollars and often the overall savings actually can pay for the cost of the HPE ESKM secure key management appliance.

Media sanitization/Destruction cost avoidance

Example of annual media destruction costs avoided
HPE Security—Data Security key management solutions render sensitive information useless to unauthorized users, thereby eliminating dependence on costly media sanitization and destruction services.

References

Guidelines for Media Sanitization—NIST
Special Publication 800-88 Revision 1
**nvlpubs.nist.gov/nistpubs/
SpecialPublications/NIST.SP.
800-88r1.pdf**

Optimizing IT Technology Refresh
Policies
**archstoneconsulting.com/services/
it-strategy-opeations/white-papers/
optimizing-it-technology.jsp**

Media Sanitization/Destruction Costs
**hytecdrivesecure.com/Pricing.aspx
dx.doi.org/10.6028/NIST.SP.800-88r1**

Annual media destruction costs avoided:

Total disk drives owned by the organization	**200,000**
Percent of drives containing sensitive information	10%
Drives subject to sanitization/destruction	20,000*
IT refresh cycle (years)	5
Drives sanitized/destroyed annually	4,000
Cost of operation per drive	**$70 USD**
Annual media sanitization/destruction costs	**$280,000 USD**

Assuming a modest growth factor of five percent, the total three-year projected organizational cost of media destruction amounts to **$882,700**.

Annual media sanitization costs avoided:

Total disk drives owned by the organization	**200,000**
Percent of drives containing sensitive information	10%
Drives subject to sanitization/destruction	20,000
IT refresh cycle (years)	5
Drives sanitized/destroyed annually	4,000
Cost of operation per drive	**$45 USD**
Annual media sanitization/destruction costs	**$180,000 USD**

Assuming a modest growth factor of five percent, the total 3 year projected organizational cost of media sanitization amount to **$567,450**.

Note*

The above calculations use an example of 200,000 drives as a baseline for reference assumption. This drive calculation will vary by actual customer installation. For a more personalized ROI estimate, please contact your HPE sales representative or contact us at **esp-value-management@hpe.com**.

The efficient and effective management of information from inception through disposition is the responsibility of all those who have handled the data.

NIST SP 800-88

Meet NIST SP 800-88 Media Sanitization Standards

Based on the results of categorization, system owners should refer to NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, which specifies, "Organizations must sanitize information system digital media using approved equipment, techniques, and procedures. The organization tracks, documents, and verifies media sanitization and destruction actions and periodically tests sanitization equipment/procedures to ensure correct performance. The organization sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media."

Per the **NIST SP 800-88 Media Sanitization Standards—Appendix D**, here are summary guidelines:

- **Make/Model/Version/Media type:**

  – The product and versions the statement applies to, and the type of media the device uses (i.e., magnetic, solid-state drive (SSD), hybrid, and others). Many devices store the target data in several different media, e.g., a dynamic random access memory (DRAM) cache in addition to rotating platters. It is important to identify the storage locations and how each is sanitized.

- **Key generation:**

  – Identify whether a Deterministic Random Bit Generator (DRBG), such as one of those listed in SP 800-90 [28] was used, and whether it was validated.

- **Media encryption:**

  – Identify the algorithm, key strength, mode of operation, and any applicable validation(s).

- **Key level and wrapping:**

  – Identify if the Media Encryption Key (MEK) (either wrapped with another value or not wrapped) is directly sanitized, or if a key that wraps the MEK (a key encryption key [KEK]) is sanitized. A description of the wrapping techniques only applies where a KEK (and not the MEK) is sanitized. Wrapping details, when provided, should include the algorithm used, strength, and (if applicable) mode of operation.

- **Data areas addressed:**

  – Describe which areas are encrypted and which areas are not encrypted. For any unencrypted areas, describe how sanitization is performed.

- **Key lifecycle management:**

  – Identify the product key(s) on a device may have multiple wrapping activities (wrapping, unwrapping, and rewrapping) throughout the device's lifecycle. Identify how the key(s) being sanitized are handled during wrapping activities that are not directly part of the Cryptographic Erase operation. For example, a user may have received a Self-Encrypting Drive (SED) that was always encrypting, and simply turned on the authentication interface. Identify how the previous instance of the MEK was sanitized when it was wrapped with the user's authentication credentials.

- **Key sanitization technique:**

  – Describe the media-dependent sanitization method for the key being sanitized. Some examples might include one or more inverted overwrite passes if the media is magnetic, a block erase for an SSD, or other media-specific techniques for other types of media.

- **Key escrow or backup:**

  – Identify whether the device supports key escrow or backup. Identify whether the device supports discovery of whether any key(s) at or below the level of the key escrowed has/have ever been escrowed from or injected into the device. If the MEK is directly sanitized and only a KEK can be escrowed, clearly identify that fact.

- **Error condition handling:**

  – Identify how the device handles error conditions that prevent the Cryptographic Erase operation from fully completing. For example, if the location where the key was stored cannot be sanitized, does the Cryptographic Erase operation report success or failure to the user?

- **Interface clarity:**

  – Identify which interface commands support the features described in the statement. If the device supports the use of multiple MEKs, identify whether all MEKs are changed using the interface commands available and any additional commands or actions necessary to ensure all MEKs are changed. Note that under certain conditions, not all MEKs have to be cleared (e.g., partial sanitization of target data).

Learn more at
hpe.com/software/ESKM

Hewlett Packard Enterprise