Hewlett Packard Enterprise

Business white paper

Local, remote, and centrally unified key management

HPE Enterprise Secure Key Manager solutions

Table of contents

Key management for encryption applications creates manageability risks when security controls and operational concerns are not fully realized. Various approaches to managing keys are discussed with the impact toward supporting enterprise policy.

Overview

When deploying encryption applications, the long-term maintenance and protection of the encryption keys need to be a critical consideration. Cryptography is a well-proven method for protecting data and, as such, is often mandated in regulatory compliance rules as reliable controls over sensitive data, using well-established algorithms and methods.

However too often, not as much attention is placed on the social engineering and safeguarding of maintaining reliable access to keys. If you lose access to keys, you by extension lose access to the data that can no longer be decrypted. With this in mind, it's important to consider various approaches when deploying encryption with secure key management that ensure an appropriate level of assurance for long-term key access and recovery that is reliable and effective, throughout the information lifecycle of use.

Key management deployment architectures

Whether through manual procedures or automated, a complete encryption and secure key management system includes the encryption endpoints (devices, applications, etc.), key generation and archiving system, key backup, policy-based controls, logging and audit facilities, and best-practice procedures for reliable operations. Based on this scope required for maintaining reliable ongoing operations, key management deployments need to match the organizational structure, security assurance levels for risk tolerance, and operational ease that impacts ongoing time and cost.

This white paper discusses enterprise secure key management in context of local, remote, and centrally unified options when deploying encryption applications. Careful consideration of each approach, in light of an organization's security, regulatory compliance, and operational policies and procedures, should be made to determine an appropriate fit.

Local key management

Key management that is distributed in an organization where keys coexist within an individual encryption application or device is a local-level solution. When highly dispersed organizations are responsible for only a few keys and applications, and no system-wide policy needs to be enforced, this can be a simple approach. Typically, local users are responsible for their own ad hoc key management procedures, where other administrators or auditors across an organization do not need access to controls or activity logging.

Managing a key lifecycle locally will typically include manual operations to generate keys, distribute or import them to applications, and archive or vault keys for long-term recovery—and as necessary, delete those keys. All of these operations tend to take place at a specific data center where no outside support is required or expected. This creates higher risk, if local teams do not maintain ongoing expertise or systematic procedures for managing controls over time. When local keys are managed ad hoc, reliable key protection and recovery become a greater risk.

Although local key management can have advantages in its perceived simplicity, without the need for central operational overhead, it is weak on dependability. In the event that access to a local key is lost or mishandled, no central backup or audit trail can assist in the recovery process.

> "Organizations must develop a business-led data-centric security strategy that will lead to the appropriate selection of either multiple siloed KM solutions or a single Enterprise Key Manager (EKM). As EKM products continue to mature and improve, clients will be better-able to implement a consistent, enterprise-class strategy—thereby protecting data, and achieving legal and regulatory compliance, while limiting risk in a demonstrable way, and reducing operational and capital costs."
>
> – Hype Cycle for Data Security, Gartner, 2015

Figure 1: Local key management over a local network where keys are stored with the encrypted storage.

Fundamentally risky if no redundancy or automation exist

Local key management has potential to improve security if there are no needs for control and audit of keys as part of broader enterprise security policy management. That is, it avoids wide access exposure that, through negligence or malicious intent, could compromise keys or logs that are administered locally. Essentially, maintaining a local key management practice can minimize external risks to undermine local encryption and key management lifecycle operations.

However, deploying the entire key management system in one location without benefit of geographically dispersed backup or centralized controls can add higher risk to operational continuity. For example, placing the encrypted data, the key archive, and a key backup in the same proximity is risky in the event a site is attacked or disaster hits. Moreover, encrypted data is easier to attack when keys are co-located with the targeted applications—the analogy being locking your front door, but placing keys under a doormat, or leaving keys in the car ignition instead of your pocket.

Figure 2: When keys are co-located along with the encrypted data, easy access creates more risk.

While local key management could potentially be easier to implement over centralized approaches, economies of scale will be limited as applications expand, as each local key management solution requires its own resources and procedures to maintain reliably within unique silos. As local approaches tend to require manual administration, the keys are at higher risk of abuse or loss as organizations evolve over time, especially when administrators change roles, compared with maintenance by a centralized team of security experts.

As local-level encryption and secure key management applications begin to scale over time, organizations will find the cost and management simplicity originally assumed now becoming more complex, making audit and consistent controls unreliable. Organizations with limited IT resources that are oversubscribed will need to solve new operational risks.

Pros

- May improve security through obscurity and isolation from a broader organization that could add access control risks
- Can be cost effective if kept simple with a limited number of applications that are easy to manage with only a few keys

Cons

- Co-located keys with the encrypted data provides easier access if systems are stolen or compromised
- Often implemented via manual procedures over key lifecycles—prone to error, neglect, and misuse
- Places “all eggs in a basket” for key archives and data without benefit of remote backups or audit logs
- May lack local security skills, creates higher risk as IT teams are multi-tasked or leave the organization
- Less reliable audits with unclear user privileges and a lack of central log consolidation, driving up audit costs and remediation expenses, long term
- Data mobility hurdles—media moved between locations requires key management to be moved also
- Does not benefit from a single, central policy-enforced, auditing efficiencies or unified controls for achieving economies and scalability

Remote key management

Key management where application encryption takes place in one physical location, while keys are managed and protected in another, allows for remote operations, which can help lower risks. As illustrated in the local approach, there is vulnerability from co-locating keys with encrypted data if a site is compromised, due to attack, misuse, or disaster.

Remote administration enables encryption keys to be controlled without management being co-located with the application, such as a console UI via secure IP networks. This is ideal for dark data centers or hosted services that are not easily accessible and/or widely distributed locations where applications need to deploy across a regionally dispersed environment.

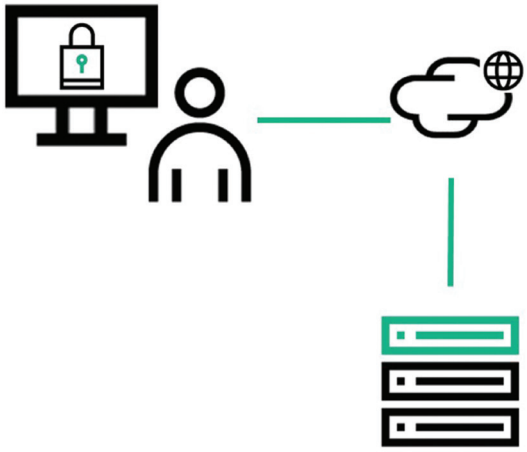

Figure 3: Remote key management separates encryption key management from the encrypted data.

Provides higher assurance security by separating keys from the encrypted data

While remote management doesn't necessarily introduce automation, it does address local attack threat vectors and key availability risks through remote key protection, backups, and logging flexibility. The ability to manage controls remotely can improve response time during manual key administration, in the event encrypted devices are compromised in high-risk locations. For example, a stolen storage device that requests a key at boot-up could have the key remotely located and destroyed, along with audit log verification, to demonstrate compliance with data privacy regulations for revoking access to data. Maintaining remote controls can also enable a quicker path to safe harbor, where a breach won't require reporting if proof of access control can be demonstrated.

As a current high-profile example of remote and secure key management success, the concept of "bring your own encryption key" is being employed with cloud service providers, enabling tenants to take advantage of co-located encryption applications, without worry of keys being compromised within a shared environment. Cloud users maintain control of their keys and can revoke them for application use at any time, while also being free to migrate applications between various data centers. In this way, the economies of cloud flexibility and scalability are enabled at a lower risk.

While application keys are no longer co-located with data locally, encryption controls are still managed in silos, without the need to co-locate all enterprise keys centrally. Although economies of scale are not improved, this approach can have similar simplicity as local methods, while also suffering from a similar dependence on manual procedures.

Pros

- Provides the lowered-risk advantage of not co-locating keys, backups, and encrypted data in the same location, which makes the system more vulnerable to compromise
- Similar to local key management, remote management may improve security through isolation if keys are still managed in discrete application silos
- Cost effective when kept simple—similar to local approaches, but managed over secured networks from virtually any location where security expertise is maintained
- Easier to control and audit without having to physically attend to each distributed system or applications, which can be time consuming and costly
- Improves data mobility—if encryption devices move, key management systems can remain in their same place, operationally

Cons

- Manual procedures don't improve security, if still not part of a systematic key management approach
- No economies of scale if keys and logs continue to be managed only within a silo for individual encryption applications

Centralized key management

The idea of a centralized, unified—or commonly, an enterprise secure key management—system is often a misunderstood definition. Not every administrative aspect needs to occur in a single, centralized location; rather, the term refers to an ability to centrally coordinate operations across an entire key lifecycle by maintaining a single pane of glass for controls. Coordinating encrypted applications in a systematic approach creates a more reliable set of procedures to ensure what authorized devices can access keys and who can administer key lifecycle policies, comprehensively.

A centralized approach reduces the risk of keys being compromised locally along with encrypted data by relying on higher-assurance, automated management systems. As a best practice, a hardware-based tamper-evident key vault and policy/logging tools are deployed in clusters, redundantly for high availability, spread across multiple geographic locations, to create replicated backups for keys, policies, and configuration data.

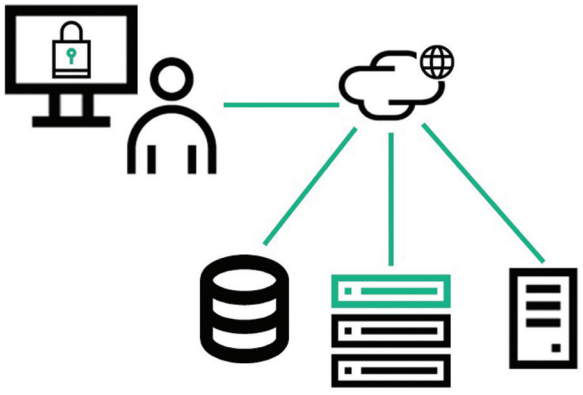

Figure 4: Central key management over wide area networks enables a single set of reliable controls and auditing over keys.

Higher assurance key protection combined with reliable security automation

As mentioned with local and remote key management, a higher risk is assumed if relying upon manual procedures to manage keys. Whereas, a centralized solution runs the risk of creating toxic combinations of access controls if users are over-privileged to manage enterprise keys, or applications are not properly authorized to store and retrieve keys.

Realizing these critical concerns, centralized and secure key management systems are designed to coordinate enterprise-wide environments of encryption applications, keys, and administrative users, using automated controls that follow security best practices. Unlike distributed key management systems that may operate locally, centralized key management can achieve better economies with the high-assurance security of hardened appliances that enforce policies with reliability, while ensuring that activity logging is tracked consistently for auditing purposes, and alerts and reporting are more efficiently distributed and escalated when necessary.

Pros

- Similar to remote administration, economies of scale achieved by enforcing controls across large estates of mixed applications from any location, with the added benefit of centralized management economies
- Coordinated partitioning of applications, keys, and users to improve on the benefit of local management
- Automation and consistency of key lifecycle procedures universally enforced to remove the risk of manual administration practices and errors
- Typically managed over secured networks from any location to serve global encryption deployments
- Easier to control and audit with a “single pane of glass” view to enforce controls and accelerate auditing
- Improves data mobility—key management system remains centrally coordinated with high availability
- Economies of scale and reusability as more applications take advantage of a single, universal system

Cons

- Key management appliances carry higher upfront costs for a single application, but do enable future reusability to improve total cost of ownership (TCO)/return on investment (ROI) over time with consistent policy and removing redundancies.
- If access controls are not managed properly, toxic combinations of users are over-privileged to compromise the system—best practices can minimize risks.

Best practices—adopting a flexible strategic approach

In real world practice, local, remote, and centralized key management can coexist within larger enterprise environments driven by the needs of diverse applications deployed across multiple data centers. While a centralized solution may apply globally, there may also be scenarios where localized solutions require isolation for mandated reasons (e.g., government regulations or weak geographic connectivity); application sensitivity level; or organizational structure where resources, operations, and expertise are best to remain in a center of excellence.

In an enterprise-class, centralized and secure key management solution, a cluster of key management servers may be distributed globally while synchronizing keys and configuration data for failover. Administrators can connect to appliances from anywhere globally to enforce policies with a single set of controls to manage and a single point for auditing security and performance of the distributed system.

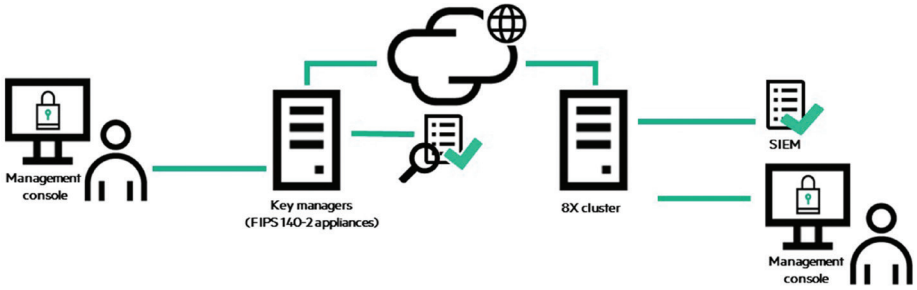

Figure 5: Clustering key management enables endpoints to connect to local key servers, a primary data center, and/or disaster recovery locations, depending on high availability needs and global distribution of encryption applications.

Considerations for deploying a centralized enterprise key management system

Enterprise secure key management solutions that offer the flexibility of local, remote, and centralized controls over keys will include a number of defining characteristics. It's important to consider the aspects that will help match the right solution to an application environment for best long-term reusability and ROI—relative to cost, administrative flexibility, and security assurance levels provided:

- **Hardware or software assurance:** Key management servers deployed as appliances, virtual appliances, or software will protect keys to varying degrees of reliability. FIPS 140-2 is the standard to measure security assurance levels. A hardened hardware-based appliance solution will be validated to level 2 or above for tamper evidence and response capabilities.
- **Standards-based or proprietary:** The OASIS Key Management Interoperability Protocol (KMIP) standard allows servers and encrypted applications to communicate for key operations. Ideally, key managers can fully support current KMIP specifications to enable the widest application range, increasing ROI under a single system.
- **Policy model:** Key lifecycle controls should follow NIST SP800-57 recommendations as a best practice. This includes key management systems enforcing user and application access policies depending on the state in a lifecycle of a particular key or set of keys, along with a complete, tamper-proof audit trail for control attestation.
- **Partitioning and user separation:** To avoid applications and users having over-privileged access to keys or controls, centralized key management systems need to be able to group applications according to enterprise policy, and to offer flexibility when defining user roles to specific responsibilities.
- **High availability:** For business continuity, key managers need to offer clustering and backup capabilities for key vaults, and configurations for failover and disaster recovery. At a minimum, two key management servers replicating data over a geographically dispersed network, and/or a server with automated backups, are required.

- **Scalability:** As applications scale and new applications are enrolled to a central key management system, keys, application connectivity, and administrators need to scale with the system. An enterprise-class key manager can elegantly handle thousands of endpoint applications and millions of keys for greater economies.
- **Logging:** Auditors require a single pane of glass view into operations, and IT needs to monitor performance and availability. Activity logging with a single view helps accelerate audits across a globally distributed environment. Integration with enterprise systems via SNMP, syslog, email alerts, and similar methods help ensure IT visibility.
- **Enterprise integration:** As key management is one part of a wider security strategy, a balance is needed between maintaining secure controls and wider exposure to enterprise IT systems for ease of use. External authentication and authorization such as Lightweight Directory Access Protocol (LDAP), or security information and event management (SIEM) for monitoring, helps coordinate with enterprise policy and procedures.

Conclusions

As enterprises mature in complexity by adopting encryption across a greater portion of their critical IT infrastructure, the need to move beyond local key management towards an enterprise strategy becomes more apparent. Achieving economies of scale with a single pane of glass view into controls and auditing can help accelerate policy enforcement and control attestation.

Centralized and secure key management enables enterprises to locate keys and their administration within a security center of excellence, while not compromising the integrity of a distributed application environment. The best of all worlds can be achieved with an enterprise strategy that coordinates applications, keys, and users with a reliable set of controls.

As more applications start to embed encryption capabilities natively, and connectivity standards such as KMIP become more widely adopted, enterprises will benefit from an enterprise secure key management system that automates security best practices and achieves greater ROI as additional applications are enrolled into a unified key management system.

HPE Data Security Technologies

HPE Enterprise Secure Key Manager

Our HPE enterprise data protection vision includes protecting sensitive data wherever it lives and moves in the enterprise, from servers to storage and cloud services. It includes HPE Enterprise Secure Key Manager (ESKM), a complete solution for generating and managing keys by unifying and automating encryption controls. With it, you can securely serve, control, and audit access to encryption keys while enjoying enterprise-class security, scalability, reliability, and high availability that maintains business continuity.

Standard HPE ESKM capabilities include high availability clustering and failover, identity and access management for administrators and encryption devices, secure backup and recovery, a local certificate authority, and a secure audit logging facility for policy compliance validation. Together with HPE Secure Encryption for protecting data-at-rest, ESKM will help you meet the highest government and industry standards for security, interoperability, and auditability.

Reliable security across the global enterprise

ESKM scales easily to support large enterprise deployment of HPE Secure Encryption across multiple geographically distributed data centers, tens of thousands of encryption clients, and millions of keys.

The HPE data encryption and key management portfolio uses ESKM to manage encryption for servers and storage including:

- HPE Smart Array Controllers for HPE ProLiant servers
- HPE NonStop Volume Level Encryption (VLE) for disk, virtual tape, and tape storage
- HPE Storage solutions including all StoreEver encrypting tape libraries, the HPE XP7 Storage Array, and HPE 3PAR

With certified compliance and support for the OASIS KMIP standard, ESKM also supports non-HPE storage, server, and partner solutions that comply with the KMIP standard. This allows you to access the broad HPE data security portfolio, while supporting heterogeneous infrastructure and avoiding vendor lock-in.

Benefits beyond security

When you encrypt data and adopt the HPE ESKM unified key management approach with strong access controls that deliver reliable security, you ensure continuous and appropriate availability to keys while supporting audit and compliance requirements. You reduce administrative costs, human error, exposure to policy compliance failures, and the risk of data breaches and business interruptions. And you can also minimize dependence on costly media sanitization and destruction services.

Don't wait another minute to take full advantage of the encryption capabilities of your servers and storage. Contact your authorized HPE sales representative or visit our website to find out more about our complete line of data security solutions.

About HPE Security—Data Security

HPE Security—Data Security drives leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of expertise, we protect the world's largest brands and neutralize breach impact by securing sensitive data-at-rest, in-use, and in-motion. Our solutions provide advanced encryption, tokenization, and key management that protect sensitive data across enterprise applications, data processing infrastructure, cloud, payments ecosystems, mission-critical transactions, storage, and Big Data platforms. HPE Security—Data Security solves one of the industry's biggest challenges: simplifying the protection of sensitive data in even the most complex use cases.

Learn more at
hpe.com/software/ESKM

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-3732ENW, January 2016