The role of key management

Protect your data with HP ESKM
The role of key management in critical data protection and business continuity architecture

Today IT organizations in large enterprises face many challenges to security and business continuity. 24x7 business applications and services require continuous availability, data protection, and regulatory compliance, but there are changing internal and external threats to consider in designing a robust architecture that combines high availability (HA) and high security elements.

Then and now:
The evolution of Cyber Crime

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Breaches</th>
<th>Cost</th>
<th>Time to Fix</th>
<th>Daily Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>1.1</td>
<td>$3.8 million</td>
<td>14 days</td>
<td>avg. $1,264 per day</td>
</tr>
<tr>
<td>2013</td>
<td>2.0</td>
<td>$11.6 million</td>
<td>32 days</td>
<td>avg. $32,368 per day</td>
</tr>
</tbody>
</table>


Encryption and key management essentials for high availability and disaster recovery

In the modern security landscape, we have seen an evolution in the nature and motivation of attacks faced by enterprises. There has been a shift from the simple denial of service and defacement attacks of a decade ago, toward sophisticated, persistent penetration of enterprise networks with theft of sensitive data on a massive scale. Retailers have been a particular target, with theft and monetization of customer and cardholder information as their financial motive. Government organizations and technology companies have also been under increasing attack, with theft of personal information, confidential records, and intellectual property by both criminals and state-sponsored attackers as their motive.
What is accelerating this alarming trend is the development of a criminal market ecosystem where participants specialize in different parts of the attack lifecycle and buy and sell tools, botnet capacity, and data to each other. Payment card fraud is an extremely profitable business for the attackers, allowing continuous investment and improvement in their malicious technologies.

Enterprise IT is also changing with emergence of mobile access to systems by both consumers and employees, the adoption of cloud services, and with the extended enterprise including supply chain and other service providers inside the organization’s networks. The traditional enterprise perimeter is gone.

Enterprises also see a tremendous increase in regulatory and compliance pressures. If they fail to meet legal, audit, or mandated industry requirements, they can face sanctions or fines. If sensitive data is breached at scale, they can expect adverse publicity, loss of customer confidence, and loss of shareholder value.

HP’s approach to enterprise security is providing customers the tools to defend themselves in this hostile environment and to disrupt the adversary criminal ecosystem. This includes educating users and improving systems to avoid security errors; blocking adversary access into enterprise networks and systems; detecting and removing adversaries quickly if they gain access; securing the sensitive information assets wherever they live and move; and lastly helping organizations adopt plans to mitigate and reduce damages when a breach occurs. Today, organizations must assume they will be breached at some point and plan appropriately to respond.

HP Atalla’s focus for the past 35 years has been protecting the financial services, banking, and retail industries and their customers from fraud and attacks using strong cryptography and key management.
HP Atalla products protect hundreds of millions of card payments transactions daily worldwide. It is a trusted security partner in the financial services and retail industries, and its products meet the highest government and industry standards for security and interoperability.

HP Atalla today has a portfolio of four information protection solutions:

- **Atalla Network Security Processors (NSPs)** for payment security
- **HP ESKM** for managing cryptographic keys for HP storage and server encryption solutions
- **Atalla Cloud Encryption (CE)** protecting sensitive information in cloud storage and application processing by providing customer control of encryption keys
- **Atalla Information Protection and Control (IPC)**, which provides classification and lifecycle protection for unstructured sensitive data wherever it moves in the enterprise

Data encryption is a technology increasingly used in enterprises to protect sensitive data at rest and in motion. However, encryption itself is not sufficient without the proper management of encryption keys: if keys are exposed, that negates the value of performing encryption; if a key is lost, the corresponding data can be lost forever; if keys are stored or sent with the encrypted data, the security is dramatically reduced; and finally if keys are accessed without controls or logging, the enterprise can still face audit failures. So use of information protection in the enterprise depends both on strong encryption controls and strong key management technologies.

HP’s enterprise data protection vision includes protecting sensitive data wherever it lives and moves in the enterprise, from servers to storage and cloud services. It also includes generating and managing encryption keys securely with enterprise-grade security, scalability, reliability, HA, and auditability. Finally, HP data encryption and key management solutions are designed to meet the highest government and industry standards for security, interoperability, and audit.

HP’s unified solution for enterprise key management is HP’s ESKM. ESKM is deployed wherever customers use encrypted storage or communications to protect their sensitive information. Sensitive data types include payment cardholder data (CHD), electronic health records (EHR), personally identifiable information (PII), intellectual property (IP), confidential business records, service provider hosted data, and defense and classified information. Sensitive information can reside in tape libraries/media, in enterprise disk arrays, on storage area networks, in server attached storage and HP NonStop servers, and in private and public cloud services.

When customers encrypt data and adopt a unified key management approach with ESKM, they store and serve keys with strong access controls and security. They ensure continuous availability to keys, and they support their internal and external audit and compliance requirements. Customers adopting a unified key management architecture reduce their costs for administration, reduce the possibility of human error, reduce their exposure to audit and compliance failures, and reduce the risk of data breaches and business interruptions. Lastly, they can eliminate dependence on costly media sanitization and destruction services.
For strong security, ESKM complies with National Institute of Standards & Technology (NIST) cryptography and key management guidance, has been validated to Federal Information Processing Standards (FIPS) 140-2 Level 2, and is delivered as a hardened security appliance. ESKM supports Secure Sockets Layer (SSL) protected communications, uses mutual certificate authentication, and provides a built-in Certificate Authority to provide strong certificate-based authentication for access to keys. ESKM provides a HA service through symmetric HA clustering from two through eight nodes, and a replicated key database for redundancy and failover. ESKM is highly scalable for large organizations, supporting thousands of enrolled keys using clients and millions of encryption keys. ESKM is interoperable; it supports HP’s broad server and storage portfolio as well as the OASIS Key Management Interoperability Protocol (KMIP) standard for client/server interoperability. Lastly, ESKM is easy to manage: all settings, client enrollments, and cryptographic keys are automatically replicated across the HA cluster; hand-off administration for daily operations is provided using scheduled backups, log rotation, and audit logging of all administrator and client activities.

To ensure the highest level of reliability, availability, and disaster recovery (DR), ESKM supports multiple layers of protection and recovery for mission-critical encryption keys. As a preconfigured server appliance, ESKM demonstrates reliable hardware and software, with millions of customer unit hours with zero failures, and never resulting in loss of customer keys or data. Each ESKM unit includes mirrored disk drives, redundant cooling, dual power supplies, and easy mechanisms for installation of software patches or rollbacks. ESKM clusters up to eight nodes that can be physically distributed across data centers and geographically for fault isolation. Clients can perform round-robin access to the ESKM cluster members and failover to any available ESKM nodes. Finally, ESKM enables robust DR strategies. ESKM performs automatic encrypted backups on a schedule set by the administrators. Backups can be directed to external remote file storage and to physical media. ESKM supports full “bare metal” DR of a customer environment if ever necessary using new hardware and restore of encrypted backup of the prior configuration.
ESKM for HP NonStop’s Volume Level Encryption

ESKM provides key management and HA for HP NonStop’s Volume Level Encryption (VLE) for disk and tape storage protection. ESKM also supports BackBox Virtual Tape for NonStop servers. HP NonStop customers expect the highest levels of availability and recoverability, and ESKM meets those requirements. With VLE, ESKM is often deployed in clusters of four nodes, two co-located in primary NonStop data center and the other two in a mirror or DR data center. In NonStop VLE, the NonStop storage Cluster I/O Modules (CLIMs) are clients of ESKM and access key generation and retrieval services. NonStop VLE and ESKM are fully integrated for ease of deployment and administration. ESKM supports mixed client environments. VLE customers leverage other HP data encryption solutions and maintains a shared, unified key management infrastructure.

Best practices for data encryption and ESKM deployments

1. Consolidate key management solutions and replace any legacy key management systems with ESKM; however, isolate encryption and key management development and test environments from production environments.

2. Always configure ESKM in clusters of two or more nodes for production environments; when possible, extend clusters across different data centers and geographic sites for the greatest fault isolation and resilience.

3. Schedule regular ESKM backups to internal, external, and offsite storage. Since ESKM backups are already encrypted, no special security measures are required.

4. Train, enroll, and utilize at least two high access security administrators at all times to avoid human single points of failure. Assign the least necessary privileges to any other administrators.

Note
HP, as a matter of policy, has no backdoor access to ESKM, nor the ability to recover lost customer passwords or keys.

5. Always configure ESKM for the highest security settings: FIPS mode operation, SSL, and mutual server client certificate authentication. Use ESKM’s IP whitelisting controls to limit ESKM access to only intended client and administrator IP addresses.

The HP data encryption and key management portfolio using ESKM now supports storage encryption for HP ProLiant servers using HP Smart Array controllers, NonStop VLE for disk and tape storage, and HP Storage solutions including all encrypting tape libraries, the new HP XP7 Storage Array, and HP 3PAR. With support for the OASIS KMIP standard, ESKM 4.0 also supports non-HP storage, server, and partner solutions that comply with the KMIP standard. This allows customers to access HP’s broad data security portfolio, while supporting heterogeneous IT infrastructures, and avoiding concerns of vendor lock-in.

In summary, HA and high security work together very well for HP NonStop customers.

Learn more at hp.com/go/ESKM