Hewlett Packard Enterprise

HPE Connected MX and HPE Enterprise Secure Key Manager Solution

Take control of data privacy for your endpoint backups with increased security

Maintaining privacy over data-at-rest is a critical part of an organization's data security strategy. While businesses have embraced the cloud for many IT needs, a high level of security assurance is expected for the privacy of backup data in the higher risk, co-located environments. HPE Connected MX with HPE Enterprise Secure Key Manager offers high assurance security for endpoint devices by protecting the keys used for encrypting backup data. The combined solution extends Connected MX to offer customers the option to manage their encryption keys and control authorized access to data backups.

Highly secure, industry standard-based architecture

HPE Connected MX is a secure cloud-based endpoint information management solution that enables organizations to continuously protect information generated by an increasingly mobile workforce and confidently deliver information accessibility while facilitating organizational visibility and control. The Connected MX architecture allows organizations to protect and control encryption keys securely using HPE Enterprise Secure Key Manager (ESKM)—an appliance that serves keys as an OASIS Key Management Interoperability Protocol (KMIP)-compliant solution. ESKM services Connected MX authorized requests for encryption keys from Federal Information Processing Standard (FIPS 140-2) validated hardware.

ESKM is a complete enterprise secure key management solution to secure cloud-hosted data against losses, mishandling, and attacks. KMIP-standardized interoperability can extend security controls beyond Connected MX to a wide range of HPE and third-party applications. ESKM enables endpoint protection and continuous access to business-critical applications that rely upon encryption keys—both locally and remotely managed, with a centralized enterprise secure key management approach and automated key replication between appliances across global enterprise encryption solutions.

ESKM appliances integrate seamlessly with Connected MX infrastructure to offer high-assurance hardware protection and availability of encryption keys. To support enterprise-managed keys, Connected MX integrates with the ESKM appliance that is deployed on your premises to encrypt and decrypt all data using the keys under your control.

Key benefits of HPE Connected MX and HPE ESKM

Reliable, secure data recovery with the assurance of encrypted endpoint backups

Enterprise control of key management, independent of hosted service providers

Flexibility of geographic location for key storage, ensuring data privacy regulation compliance

Economic value of managing backups in the cloud, without compromising access exposure

Leveraging analytics and intelligence for smarter backup and recovery, Connected MX and ESKM enable organizations to benefit from centralized real-time insights, auditing, reporting, and information compliance features. With a centrally managed repository bound by organizationally defined policies, the business can more effectively deliver end-user conveniences guided by a corporate strategy that centers on risk reduction and exposure.

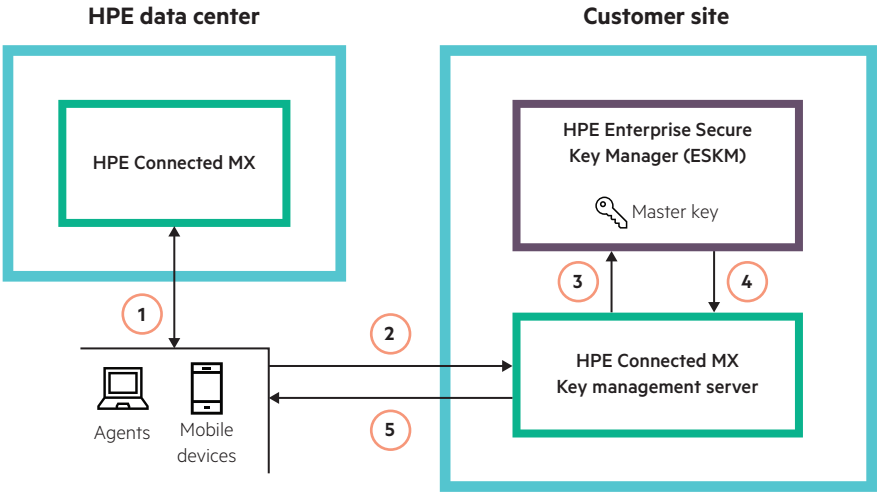

Figure 1: Architecture example: HPE Connected MX and HPE ESKM implementation

Architecture value

The Connected MX and ESKM integrated architecture offers superior value including:

- A best-of-breed solution for managing encryption keys within FIPS 140-2 validated hardware that enables reliable recovery of encrypted endpoint backups.
- Enterprise-managed encryption keys where access controls over backups limit data exposure.
- No noticeable performance impact to the Connected MX environment—key operations are automated by ESKM, where keys are vaulted securely over long-term data retention periods.
- Automatic key replication within an ESKM cluster enables high availability for business continuity in the event of a data center outage.
- Integration is predictable with pre-qualified, standards-based interoperability that takes the guesswork out of deployment and doesn't require custom development.

Dependable recovery—when you need it most

Disaster often hits at inopportune times and can even occur through attacks. Connected MX and ESKM help organizations to recover quickly from data loss events and thwart newer threats such as ransomware that can compromise access to data at the endpoint. Recovery features include:

- Continuous data protection that enables recovery of clean, recent backups
- Flexible data retention policies that can be tuned to most appropriately reduce risk
- Data restore from the old to the new endpoint during device upgrade
- Point-in-time data restore for accurate recovery prior to a data loss event or attack

Learn more at
hpe.com/software/connectedmx
hpe.com/software/eskm

Hewlett Packard Enterprise

4AA6-5791ENN, May 2016