KeyBRIDGE eKMS™ (Enterprise Key Management System) Solution

GEOBRIDGE recognized that the need for reliable data protection is increasing and the number of keys used to protect that data also has increased. Expanding upon the KeyBRIDGE 3100 platform, the KeyBRIDGE Enterprise Key Management System (eKMS) was designed to help customers solve a growing enterprise problem: consistent, centralized key lifecycle management.

Customers are able to generate, import and export keys quickly and efficiently. KeyBRIDGE’s centralized key management can do all of this and tracks all of the key details in a single location.

HSM Management

KeyBRIDGE eKMS solution enables organizations to securely manage and store all keys and sensitive data for the entire enterprise in a single, centralized location. By integrating HSMs from manufacturers including Thales, SafeNet, Utimaco and HP Atalla, customers can perform key management functions through a single, easy-to-use interface.
The KeyBRIDGE interface allowing customers to add/connect additional HSMs, as well as view and manage existing HSMs within their environment. Multiple HSMs from any manufacturer can be linked to KeyBRIDGE as well as logical endpoint applications needing to utilize keys or materials for use on specific HSMs.

Beneficial and Effective Audit Logging

The platform logs every user action regardless of status (pass or fail) is. Each record in the system audit log will contain the following information:

- A unique audit record ID
- Date and timestamp
- User IDs
- Function performed
- Relationship
- POS Terminal Details (injection only)
- Key Serial Number - KSI & DID portion only (injection only)
- Status: Pass or Failure
- Additional discretionary data (function specific)
PCI Compliant Architecture

The KeyBRIDGE eKMS protects all keys by utilizing a 256 Bit advanced encryption standard (AES) System Master Key (SMK). The AES SMK strength allows for the compliant interoperability of nearly any system that needs to connect and establish key encryption keys in order to transport keys among diverse systems. Leveraging a graphical interface, built in compliance-based controls and both the TR-31 and Thales® compatible key block formats.

Additional features

- 256-Bit AES Encryption
- Backup / Restore Capabilities
- Full Audit Visibility
- Enforcement of dual control, split knowledge.
- Role-based access
- Automated
- Key format interoperability.
- Stores keys as TR-31 bundle
- User-Definable Key Attributes
- Certificate Management
- Connection Profiles with TLS 1.2 Mutual Authentication
- Tokenization (TokenBRIDGE)

Support Going Above and Beyond

GEOBRIDGE customers are our most vital asset, and so we believe Support begins from initial KeyBRIDGE implementation and continues with ongoing maintenance of the appliance. The GEOBRIDGE team provides white glove support while working with customers around the globe to provide exceptional technical support for all of our products and services.
System components:

- KeyBRIDGE eKMS appliance: the appliance connects to the HSMs using TCP/IP. There can be multiple HSMs of each type Security Officers/Key Custodians: these are trusted individuals whose role is to manage the system; these responsibilities include:
  
  - System installation and configuration
  - System Master Key (SMK) management
  - User management
  - HSM management
  - Key management

- HSMs: eKMS can currently connect to Thales payShield and nShield HSMs, Atalla Network Security Processor (NSP), Safenet Luna EFT and Utimaco CryptoServer LAN.

**HSM-specific functions:**

- PayShield 9000:
  - Record Local Master Key (LMK) check values (up to 10 per HSM).
  - Establish a per-LMK transport key to enable translating keys in the inventory to a HSM's LMK.
  - Export an inventory key to a LMK.

- nShield Connect:
  - Connect KeyBRIDGE to a Security World.
  - Create a symmetric transport key between the eKMS and the Security World.
  - Export inventory keys from the platform to the nShield Security World wrapped under the transport key.
- **Atalla NSP**
  - Record Master File Key (MFK) check values (up to 10 per HSM).
  - Establish a per-MFK transport key to enable translating keys in the inventory to a HSM's LMK (manual process per MFK).
  - Export an inventory key to a MFK.

- **Safenet Luna Electric Fund Transfer (EFT)**
  - Establish a transport key to enable translating keys in the inventory to a HSM's Domain Master Key (KM) (manual process).
  - Export an inventory key to the Domain Master Key (MK).

- **Utimaco CryptoServer LAN**
  - Create a symmetric transport key between the eKMS and the CryptoServer.
  - Export inventory keys from the eKMS to the CryptoServer wrapped with the transport key.
payShield 9000 Support Details

Establishing the transport key between eKMS and a payShield follows this process:

1. Once the HSM is connected to KeyBRIDGE, KeyBRIDGE creates and shares a triple-length TDES or 256-bit AES Key Encryption Key (KEK)/Zone Master Key (ZMK) with the HSM, one per LMK. KeyBRIDGE connects to the 9000 console port on each HSM, and can support up to 16 with an external multiport adapter.

2. Users generate keys through the eKMS GUI, which are stored in the inventory.

3. To export inventory keys under LMK encryption, the solution passes the KEK/ZMK encrypted key to the HSM for LMK encryption.

4. The HSM returns the LMK-encrypted ciphertext or key block for eKMS to place in a dedicated application key table where it will be immediately available for PayShield system utilization.
nShield Connect Support Details

By integrating eKMS with nShield, the keys are enabled to send keys from eKMS to nShield for inclusion into the Security World, so applications can use them for processing, and to recover keys generated by applications and store them in eKMS.

System Diagram for nShield integration:

The overall process to establish a KEK for working key exchanges is shown above. A description of the process:

1. nShield creates a RSA wrapping key pair.
2. nShield sends the public key to eKMS.
3. eKMS generates an AES KEK, wraps it with the RSA key and sends it to the nShield.

At this point, both systems have a KEK with which to securely exchange additional working keys. Standard PKCS11 key exchange mechanisms can be used, since the HSM in eKMS and nShield both provide PKCS11 APIs to their respective applications.
Atalla Support Details

1. Key Administrators create a triple-length TDES KEK on the HSM and install the KEK cryptogram on the eKMS, one per MFK.

2. Users generate keys through the eKMS GUI, which are stored in the inventory.

3. To export inventory keys under LMK encryption, the eKMS passes the KEK encrypted key to the HSM for MFK encryption.

4. The HSM returns the MFK-encrypted ciphertext or key block for eKMS to place in a dedicated application key table where it will be immediately available for Atalla system utilization.
Safenet Support Details

1. Key Administrators create a triple-length TDES Bidirectional Interchange Key (KI) on the HSM and install the KI cryptogram on the KeyBRIDGE appliance.

2. Users generate keys through the KeyBRIDGE GUI.

3. To export inventory keys under Domain Master Key (KM) encryption, KeyBRIDGE passes the KI encrypted key to the HSM for KM encryption.

4. The HSM returns the KM-encrypted cipher text encrypted under the shared KI for eKMS to place in a dedicated application key table where it will be immediately available for Safenet system utilization.
Utimaco Support Details

The goal of integrating eKMS with the Utimaco is to enable sending keys from eKMS to the Utimaco, so applications can use them for processing, and to recover keys generated by applications and store them in eKMS.

System Diagram for Utimaco integration:

![System Diagram](image)

The overall process to establish a KEK for working key exchanges is shown above. A description of the process:

1. Utimaco creates a RSA wrapping key pair.
2. Utimaco sends the public key to eKMS.
3. eKMS generates an AES KEK, wraps it with the RSA key and sends it to the Utimaco.

At this point, both systems have a KEK with which to securely exchange additional working keys. Standard PKCS11 key exchange mechanisms can be used, since the HSM in eKMS and Utimaco both provide PKCS11 APIs to their respective applications.
Cryptographic Key Management

KeyBRIDGE eKMS is the most comprehensive centralized key management system in the market. The single greatest challenge to centralized key management is the utilization of proprietary formats, proprietary naming conventions, and unique interfaces that are utilized by each individual HSM or application. This causes enormous confusion and necessitates duplicate key ceremonies on multiple systems that possess either limited audit functionality or none at all. KeyBRIDGE eKMS is the only solution with the ability to align the proprietary key management techniques used throughout the cryptographic industry. Instead of waiting for an interoperable key management technique to be approved and finally implemented on all the systems that must be managed, GEOBRIDGE has worked cooperatively with each individual major HSM provider and adapted their proprietary techniques in order to create a truly centralized key management system with seamless integration for any third party device.

By utilizing KeyBRIDGE eKMS as the cryptographic key management anchor for the enterprise, key imports, exports, and translations can be centrally managed and tracked for use with any third party endpoint. Automated backups to USB or network file share locations ensure that the inventory and history of each key is protected and preserved. Restore processes can be completed in under five minutes. KeyBRIDGE eKMS provides support for secure key component and cryptogram handling. Any number of secure mailer formats can be utilized for print capabilities and tracking.
GEOBRIDGE has maintained support for dozens of technology manufacturers that realize the value of a centralized system that allows for them maintain their own proprietary key handling techniques thereby eliminating the need for new development and increased costs. GEOBRIDGE is continuing to add support for new technology manufacturers on a continual basis as a result of customer demand. So, if additional end-points require integration the GEOBRIDGE eKMS can easily accommodate additional key management requirements.

About GEOBRIDGE

In 1997, GEOBRIDGE emerged as one of the first information security solutions providers to support cryptography and payment applications for payment processors, financial institutions and retail organizations. Guided by the credo that information security solutions should support, rather than dictate, business requirements, GEOBRIDGE continues to find new mechanisms that leverage our customers’ security measures to better meet their business needs.

Today GEOBRIDGE is a leading information security solutions and compliance provider that supports a diverse global client base in retail, financial services, manufacturing and key injection facilities.

GEOBRIDGE brings together a team of highly skilled and highly experienced Network Security Architects, Application Developers, Cryptographic Key Management Experts and Project Management professionals who are fully invested in satisfying the security and compliance requirements of our customers.

Visit us at www.GEOBRIDGE.net.