Product Brochure

KeyBRIDGE UKM – Universal Key Management

Unifying Your Existing HSM Key Management Landscape

Creating Trust in
the **Digital Society**

40 utimaco® YEARS

The Key Management Needs and Challenges of the Digital Landscape

Recent trends in enterprise cyber breaches have further increased the cybersecurity regulations levied not only by the Payment Card Industry (PCI) in the Banking and Financial Services market but in other verticals as well to include Automotive and Healthcare. Demand for data and privacy continues to increase across the globe with the new wave of regional regulations taking hold whether it is the General Data Protection Regulation GDPR in the EU, the California Consumer Privacy Act CCPA in North America, or the Personal Data Protection Act PDPA in Asia.

If organizations fail to meet these legal, audit, or mandated industry requirements, they can face sanctions or fines. And, if sensitive data is breached at scale, they can expect adverse publicity, loss of customer confidence, and loss of shareholder value.

Now more than ever, individuals and enterprises need data to be protected and all assets whether physical or digital, must be delivered with confidentiality and integrity. Encryption can be simple when there is no requirement to share information. However, when encrypted information must be shared in real-time, the generation and distribution of cryptographic keys can be a daunting task. However, these fundamental cybersecurity services are necessary to deliver ubiquitous and agile “Trust in the Digital Society“.

This trust is only possible with properly implemented cryptographic key management principles. This discipline is extremely complex and compounded by the sheer volume of keys that will be required to secure all aspects of the digital landscape across multiple verticals in this ever-connecting and “always on” digital world. The need for confidentiality, integrity, availability and ultimately, the need for cryptographic keys will expand exponentially. Independent HSM domains, disparate applications, non-interoperable equipment, incompatible tools, and manual processes will quickly translate to added complexity, overwhelming compliance costs and corporate and consumer risk. The need for automated, compliant, versatile, centralized, and easy-to-use key management solutions will continue to grow.

Valuable data that enterprises need to secure:

- Payment card holder data
- Electronic health records
- Personally identifiable information
- Source code
- Intellectual property
- Digital identities
- Payment transactions
- Digital communications
- Confidential business records

UTIMACO's KeyBRIDGE UKM

The key management and cybersecurity experts at UTIMACO have integrated years of experience from the highly regulated Banking and Financial Services market into a universal key management platform that can deliver automated, compliant, versatile, and easy-to-use key management capabilities to any market. UTIMACO's KeyBRIDGE Universal Key Management (UKM) platform is designed to solve all your general purpose and payment related key management challenges from a single, centralized "pane of glass".

Integrate your existing HSMs and cryptographic keys under one single **"pane of glass"**.

Centralized

A "single pane of glass" and comprehensive platform for key generation, import/export, translation, encryption, digital signature, secrets management and audit reporting.

Compliant

FIPS 140-2, level 3 and PCI PTS HSM compliant hardware security provides the root of trust for a comprehensive key management architecture designed to PCI PIN standards.

Interoperable

KeyBRIDGE UKM unifies your multi-vendor HSM fleet into a single, central key management architecture by integrating support for 3rd party HSMs to include Thales, Luna, and nCipher.

Versatile

A versatile platform to satisfy large and small enterprises on-premise, from lights-out data centers or integrated into hybrid cloud operational models via ByoK or Key Management As-A-Service.

Solution Benefits

Centralized and Secure Key Storage

The top challenges that centralized key management are facing is proprietary formats, naming conventions, and unique interfaces that are utilized by each individual HSM or application. UKM enables organizations to securely manage and store enterprise keys and sensitive data in a single, centralized location. When integrating HSMs from UTIMACO and other manufacturers, customers can perform key management functions through one user-friendly interface. Customers can add and connect additional HSMs as well as to view and manage HSMs in their environment through this interface.

Manage Your Own Key (MYOK)

The UKM platform manages and distributes cryptographic keys and keying materials across a broad spectrum of use cases. The platform offers full support of AES, DES, RSA and ECC algorithms. All keys within KeyBRIDGE are protected under an AES-256 bit System Master Key (SMK), for immediate use or distribution as a cryptogram or broken down into components.
In addition, UKM ensures that each organization is in full control of its own universal key inventory and not at the mercy of a single solution, manufacturer or an employee who is no longer available.

Detailed Key Inventory

Perform automated backups to USB, SFTP or network file share locations to ensure that the inventory and history of each key is protected and preserved. Restore processes if needed takes less than 5 minutes. As UKM provides support for secure key component and cryptogram handling, any number of secure mailer formats can be used for printing and tracking.

PCI Compliant Architecture

The KeyBRIDGE UKM 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. The KeyBRIDGE UKM leverages a graphical user interface, built-in compliance-based controls with support for the interoperable TR-31 key blocks as well as other third party proprietary Key Block formats for transport and internal storage.

Interoperability

UKM 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 implemented on all the systems that must be managed, UTIMACO integrated and adapted the proprietary techniques in order to create a truly centralized key management system with seamless integration for any third-party device. Enterprises can use UKM as the cryptographic key management anchor so that their key imports, exports and translations can be centrally managed and tracked for use with any third-party endpoint.

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

Beneficial and Effective Audit Logging

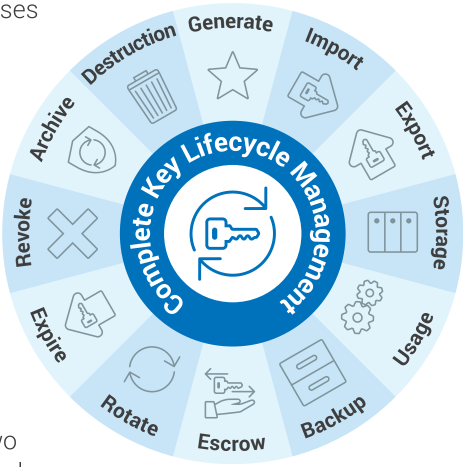
The platform logs every user action regardless of status (pass or fail). Each record in the system audit log will contain the following information:

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

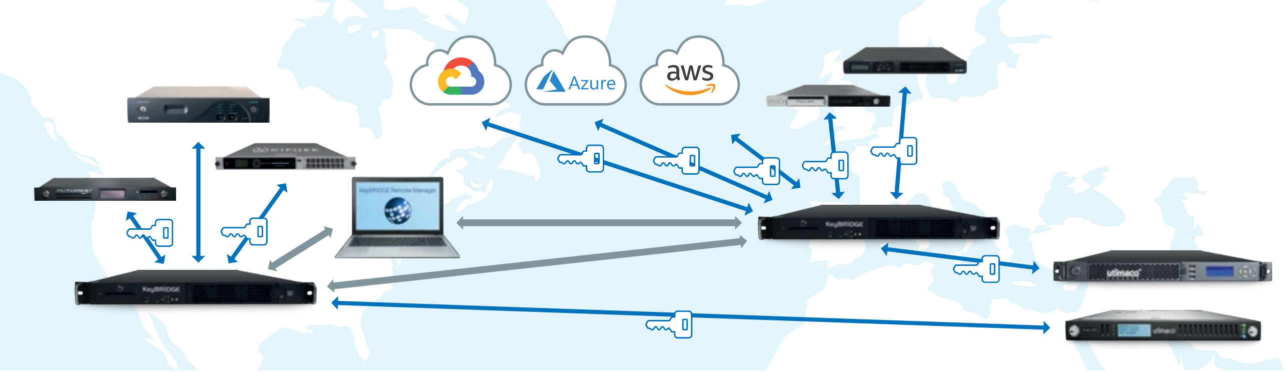
Global Key Management Platform

Due to acquisitions, dual-vendor strategy, and different use cases, enterprises can have more than one HSM to manage. Different HSMs require different sets of keys – and different ways to manage them. KeyBRIDGE UKM assists in the operation of pushing the keys across all different HSMs, regardless of the vendor. No keys are visible in clear text, and all sensitive operations happen within the FIPS 140-2 Level 3 protection zone. Enterprises can now freely create, rotate, export, delete, and move keys locally or in the cloud, and the remote manager UI (the laptop in the picture below) gives insight and helps manage all these operations.

KeyBRIDGE can be managed remotely in one of two ways – via the Remote Manager user interface or the API for Remote Centralized Key management (ARCK). This allows two KeyBRIDGE appliances to be installed in “dark” data centers to deliver high availability (HA) service to two different regions of a global fleet while being managed remotely from a single Remote Manager location.



Unify the lifecycle management of keys in your organization



Role Based Access Controls

When it comes to security on the KeyBRIDGE platform, one of the most important aspects is Access Controls. The KeyBRIDGE solution enforces the concepts of dual control and split knowledge, with extensive audit logging to capture each action that is performed. All activities can be reliably traced to at least two unique personnel. Additionally, the KeyBRIDGE architecture is rooted in role-based access to ensure appropriate controls and restrictions are in place to protect sensitive functions. The assigned role will dictate the access and capabilities of a given user. Each role has specified privileges to allow access based on the need to know of the user. The four user roles in KeyBRIDGE are:

Manager

Key Custodian

Supervisor

Operator

API Key Request Processing

KeyBRIDGE features the ARCK API, (API for Remote Centralized Key management). This is a simple JSON Schema RESTful API that allows for new schemas to be included for support in rapid fashion. Basic key generate, import, export, and delete operations, along with a suite of administrative and audit functions are all available as GET and POST commands.

Internal Certificate Management

KeyBRIDGE includes features for the centralized management of X.509 and PKCS #7 certificates for payload signing and TLS session management. KeyBRIDGE supports the import of multiple Certificate Authority (CA) and Sub-CA certificates as well as CA-signed certificates, so submitted client certificates can be fully validated. KeyBRIDGE uses TLS for session security for API requests. A unique certificate must be designated for TLS authentication in order for incoming requests via the API to be accepted.

Secure Secret Data Storage

The solution enables secure storage of secret data (up to 128 characters), such as HSM master key components, passwords, PINs, safe combinations, access codes, and derivation data. Virtually any piece of information that is frequently stored in physical safes can be securely stored and tracked within KeyBRIDGE. Each secret is owned by a designated Key Custodian Group. Retrieval of the secure data requires dual control access from two key custodians assigned to the group to which the secret data is associated.

Digital Signature Capability

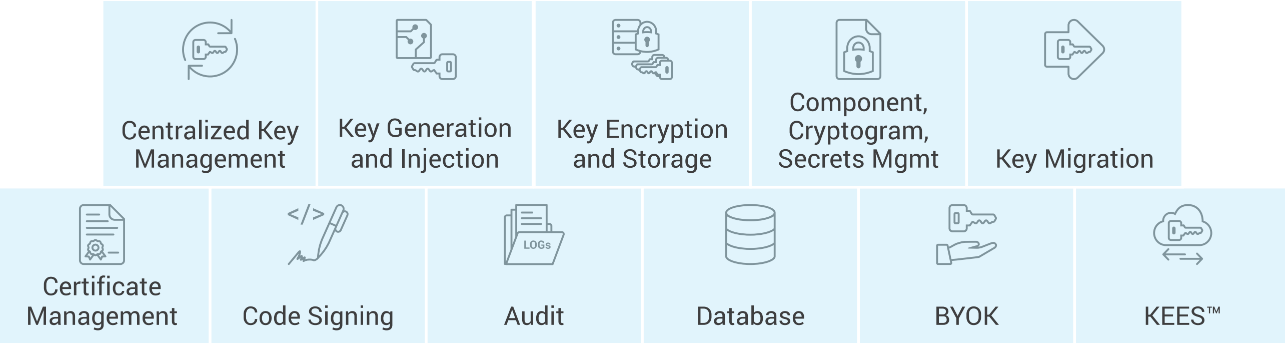
KeyBRIDGE's new digital signing capability expands the operational breadth of the portfolio to new opportunities requiring computation and verification of digital signatures and MACs.

KeyBRIDGE digital signature functionality allows customers to digitally sign any file type, whether documents, code, applications, scripts, etc. Customers can maintain full access to their signing key(s) and signing use while using SHA2, ECDSA, and RSA signature algorithms.

Quantum Ready

KeyBRIDGE supports asymmetric and symmetric cryptography as each is used in a variety of industries. KeyBRIDGE is positioned for the future with its support for AES 256-bit keys and its ability to be firmware upgraded once quantum resistant asymmetric algorithms have been standardized.

UTIMACO
KeyBRIDGE UKM


Centralized Key Management
Key Generation and Injection
Key Encryption and Storage
Component, Cryptogram, Secrets Mgmt
Key Migration
Certificate Management
Code Signing
LOGs
Audit
Database
BYOK
KEES™

Key Management and the Cloud

KeyBRIDGE allows large enterprise customers with access to more resources, to centrally manage a global inventory of cryptographic keys. Small and middle-sized customers will continually reduce their footprint as the cost and complexity of key management compliance forces them to migrate completely to the cloud while the larger enterprises will likely diversify into a hybrid model making use of public and private cloud providers – Google, AWS, Salesforce, IBM, Microsoft, etc. KeyBRIDGE UKM supports any cloud-based model whether public, private or a hybrid whether it is via Bring Your Own Key (BYOK) interfaces or by allowing customers to always maintain custody over their keys throughout their key lifecycle. Customers that want to maintain some independence from the global, public cloud providers can consume PCI PIN compliant key management from UTIMACO's Key Escrow and exchange Services (KEES™) private cloud. Whether managed locally on-premise, consumed off-premise As-A-Service – UTIMACO's architecture is flexible and – the KeyBRIDGE architecture is flexible and versatile to meet your universal and dynamic key management demands now and in the future.

Special Application of Automotive/IoT Industry

The number of IoT or smart devices including smart vehicles, is increasing with connectivity and necessitates additional security to protect communications, devices, and data. Before data exchange or communication between devices, it is necessary that the device's identity be authenticated. This trusted communication and authentication is enabled through the trusted generation, injection, and management of cryptographic keys and certificates.

The KeyBRIDGE UKM can generate this cryptographic content from its FIPS 140-2 Level 3 approved HSM platform and be the single "pane of glass" to manage the entire lifecycle for the volume of keys and certificates that are deployed and used in the automotive/IoT ecosystem during manufacturing, operation, and service.

What are the benefits of using KeyBRIDGE UKM for the Automotive/IoT industry?

1

High assurance and trust from the FIPS 140-2 Level 3 security architecture

2

High availability and redundancy ensures production capacity is maintained

3

Complete key management lifecycle visibility from a centralized, automated platform

4

Compliance & auditability made easy with detailed activity logs

5

Remote access improves logistics and security

Compliance at the Highest Level

UTIMACO participates in the major national and international standards bodies. The KeyBRIDGE appliance and KEES™ KMaaS were designed with these compliance and security standards in mind.

Our customers can always look to us for guidance and be assured that KeyBRIDGE is compliant with the following standards:

- **ANSI X9.24-1-2017:**
  Retail Financial Services Symmetric Key Management
  Part 1: Using Symmetric Techniques
- **ANSI X9.24-2-2016:**
  Retail Financial Services Symmetric Key Management
  Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
- **ANSI X9.24-3-2017:**
  Retail Financial Services – Symmetric Key Management
  Part 3: Derived Unique Key per Transaction
- **ANSI X9.143-2021:**
  Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
- **ASC X9.TR-34-2019:**
  Interoperable Method for Distribution of Symmetric Keys Using Asymmetric Techniques
  Part 1: Using Factoring-Based Public Key Cryptography Unilateral Key Transport
- **ANSI X9.97-2009:**
  Financial services – Secure Cryptographic Devices (Retail)
  Part 1: Concepts, Requirements, and Evaluation Methods
- **ANSI X9.52-1998:**
  Triple Data Encryption Algorithm Modes of Operation
- **Payment Card Industry (PCI) PIN Security Requirements**
- **Payment Card Industry (PCI) PTS HSM:**
  Modular Security Requirements Version 3
- **FIPS FIPS 140-2, Level 3:**
  Security Requirements for Cryptographic Modules, Security Level 3 Certificates

Technical Details

Physical Dimensions

- **Height:**
  1.75 inches (4.4 cm)
- **Width:**
  17.2 inches (43.8 cm)
- **Depth:**
  21.3 inches (54.2 cm)

Connectivity

- **Communications Ethernet:**
  TCP/IP, TLS 1.2 (only)
- **LAN Connection:**
  10/100/1000BASE-T (RJ45) autosensing

Electrical Characteristics

- **Rated input voltage:**
  100 to 240 VAC
- **Rated input current:**
  5 A at 100 VAC; 3 A at 240 VAC
- **Rated input frequency:**
  50 Hz to 60 Hz
- **Rated input power:**
  300 W

Operating Environment

- **Temperature:**
  10°C to 35°C (50°F to 95°F)
- **Relative humidity:**
  5% to 80% Non-condensing

Certification/Compliance

- **Safety / Emissions:**
  UL62368-1+, CB62368-1/60950-1, CE/FCC,
  RCM #1 Australia

Cryptographic Algorithms

- **Asymmetric algorithms/lengths:**
  RSA: 1024, 2048, 3072, 4096 Bits
  ECC: NIST, SEC 2 and Brainpool elliptic curves,
  160 – 571 Bits
- **Symmetric algorithms/lengths:**
  DES, TripleDES
  AES 128, 192, 256 Bits
- **Hash Functions:**
  SHA1, SHA224, SHA256, SHA384, SHA512 Bits
- **Message Authentication:**
  CMAC
  HMAC

Related Solutions

UTIMACO
Atalla AT1000

The fastest payment HSM in the industry

UTIMACO
SecurityServer

Best in class general purpose HSM

About UTIMACO

UTIMACO is a global platform provider of trusted Cybersecurity and Compliance solutions and services with headquarters in Aachen (Germany) and Campbell, CA (USA).

UTIMACO develops on-premises and cloud-based hardware security modules, solutions for key management, data protection, and identity management as well as data intelligence solutions for regulated critical infrastructures and Public Warning Systems. UTIMACO is one of the world's leading manufacturers in its key market segments.

500+ employees around the globe create innovative solutions and services to protect data, identities and communication networks with responsibility for global customers and citizens. Customers and partners in many different industries value the reliability and long-term investment security of UTIMACO's high-security products and solutions.

Find out more on utimaco.com

Headquarters Aachen, Germany

Headquarters Campbell, USA

We protect …

…people, devices and digital identities

against natural disasters, terrorism and cybercrime.

…financial transactions, data at rest and in motion

against theft and sabotage.

…data and ideas

Digital economy and digital transformation processes against theft, abuse and manipulation.

…investments

with proven, future-proof technology, products and solutions that meet regulation and compliance standards.

Contact us

EMEA

UTIMACO IS GmbH

📍 Germanusstrasse 4
52080 Aachen,
Germany

☎ +49 241 1696 200

✉ info@utimaco.com

Americas

UTIMACO Inc.

📍 900 E Hamilton Ave., Suite 400
Campbell, CA 95008,
USA

☎ +1 844 UTIMACO

✉ info@utimaco.com

APAC

UTIMACO IS Pte Limited

📍 6 Temasek Boulevard
#23-04 Suntec Tower Four
Singapore 038986

☎ +65 6993 8918

✉ info@utimaco.com

For more information about UTIMACO® products, please visit:

utimaco.com

© UTIMACO IS GmbH 03/23 – Version 1.1
UTIMACO® is a trademark of UTIMACO GmbH. All other named trademarks are trademarks of the particular copyright holder. All rights reserved. Specifications are subject to change without notice.

Creating Trust in
the **Digital Society**