UTIMACO KeyBRIDGE UKM

Product Master Deck

Priyank Kumar
Principal Product Manager

Jason Way
SVP Payment Technologies

September 2020

Creating Trust in
the Digital Society

utimaco®

About us

HQ Location
Campbell, USA

UTIMACO is a global **platform solution leader** of trusted Cybersecurity and Compliance solutions.

We are driven to take a leading market position by providing uncompromised Cyber Security solutions fulfilling the highest standards.

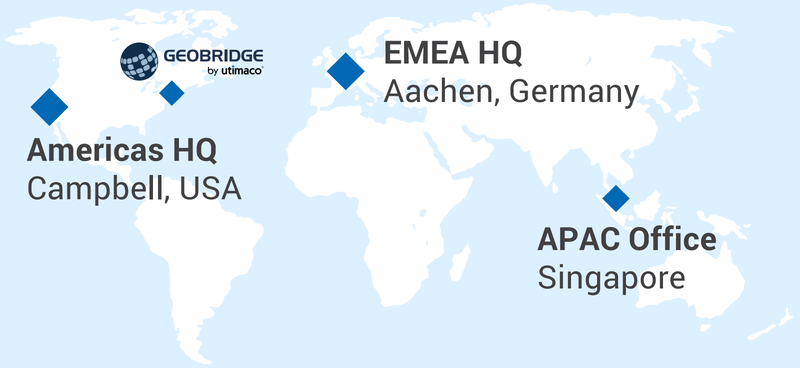
With responsibility for global customers and citizens we create innovative solutions to protect data, identities and communication networks.

HQ Location
Aachen, Germany

Revenue FY 19/20

Founded **1964**
Private company

UTIMACO is an international provider of
cyber security & compliance solutions
with headquarters in



330 highly skilled experts

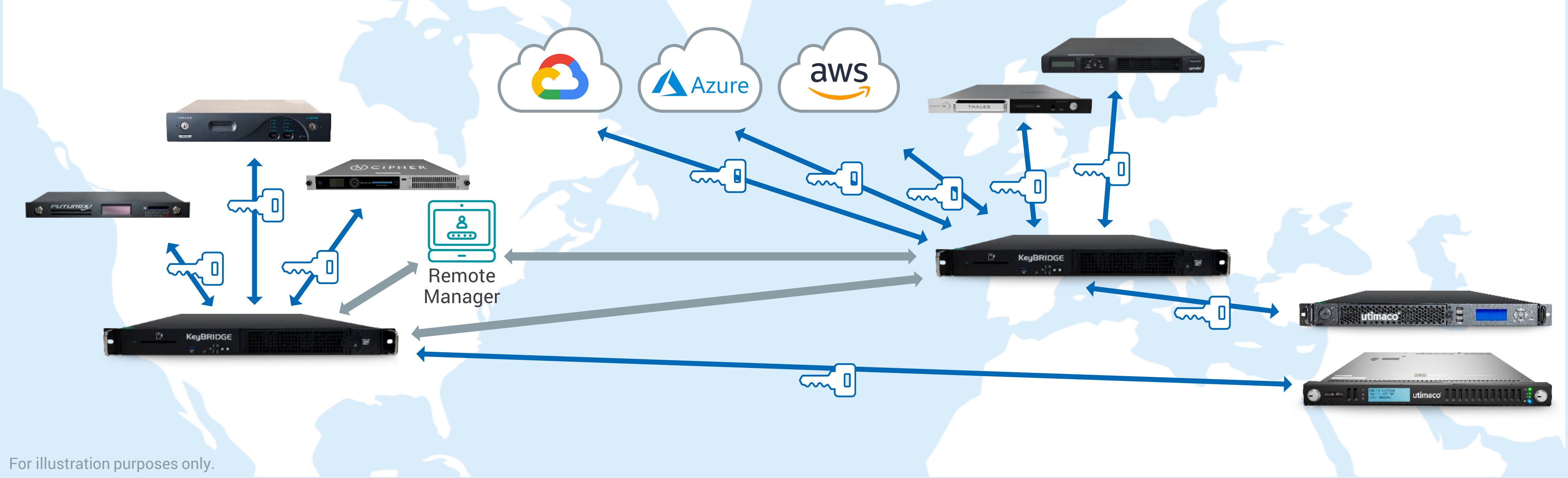
50+ years in IT and
35+ years in IT-Security

KeyBRIDGE UKM 4100

Executive Summary

- PCI-PIN Certified Policy based Key Life Cycle Management incl. Distribution Control
- Unify your existing HSM key management landscape
- Remote HSM Operation & Management

Unify the lifecycle management of keys in your organization



For illustration purposes only.

The Market & Why?

Let’s Understand the Market First!

- Dual HSM vendor
- Multiple Use cases
- Internal Organization
- M&A

- Key management requirements grow due to compliance obligations

- Increased risk on policies and audit requirements

PCI Security Standards Council®

Accredited Standards Committee X9 Inc.
Financial Industry Standards

Challenges Faced By A Business

Organizations that require heterogeneous HSM

Cost effective way to **manage the "different current HSM Landscape"** and **"ensuring consistency / compliance"**

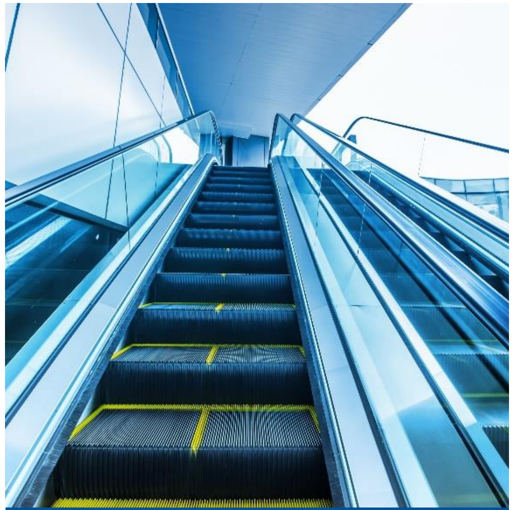
Reduce expensive PCI DSS errors as an enterprise grows and expands that leads to an increase in repositories and systems

To be compliant with **BYOK keys** in the cloud to manage and monitor the keys

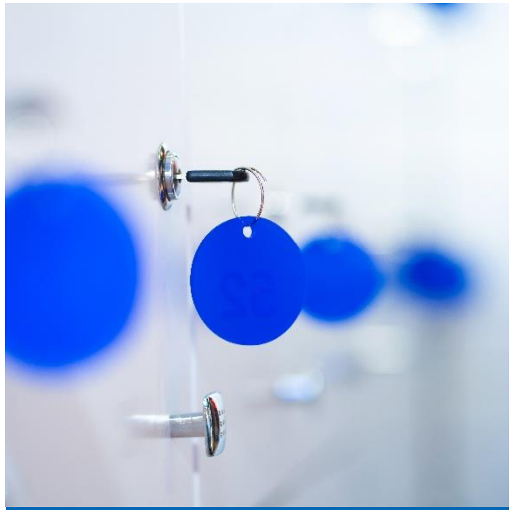
Utimaco UKM Solution

Value Proposition

A **single pane** of **glass** to manage all your HSM keys



Automate and reduce key management manual errors



Monitor all your keys with an **Audit trail**

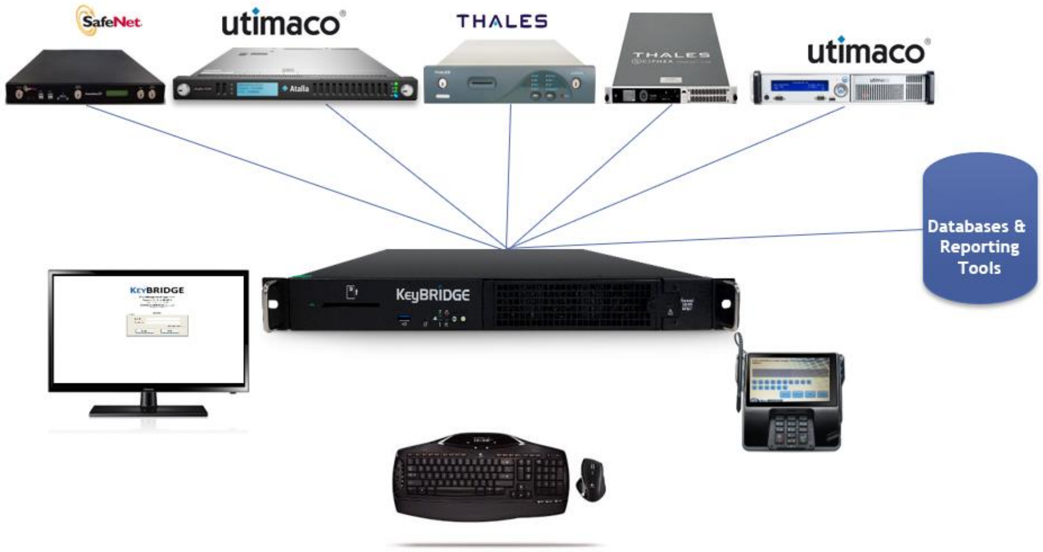
Remotely Access the UKM solution; limiting expensive onsite visits and cost/risk associated

Key Management – Common Interface for all HSMs

Common Interface for conducting Key Management Activities with a Heterogenous HSM Environment.

- **Import** via parts, blobs, cryptograms, or key blocks
- **Export** via parts, blobs, cryptograms, or key blocks
- **Generate** keys using FIPS certified RNG
- **Rotate** individual keys or entire inventory

Translate Keys among proprietary formats

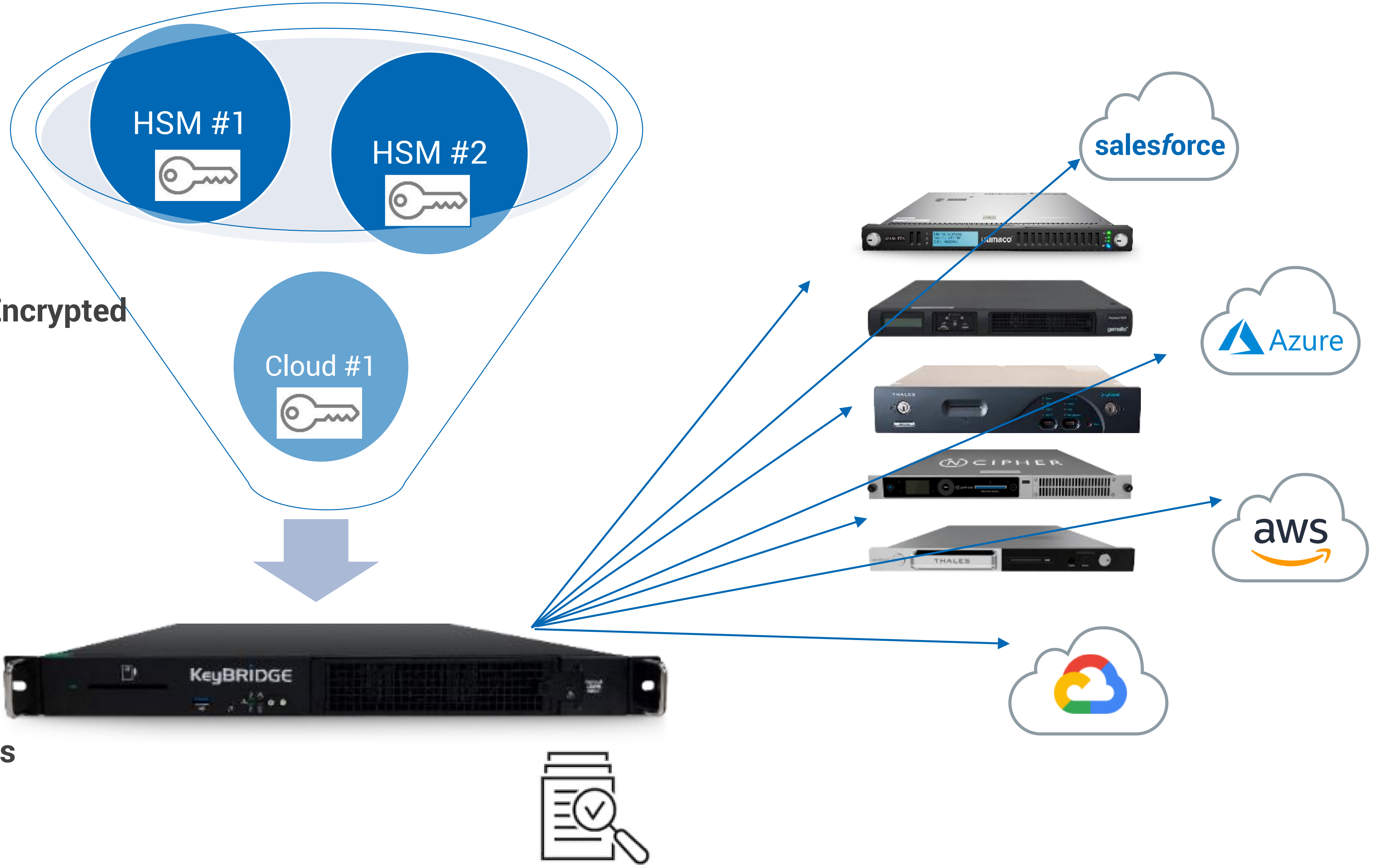


Centralized Key Management for Heterogenous Environment

- **Generate Keys**

  Or

- **Consume Keys Encrypted by 3rd Party**
- **Categorize Keys**
- **Translate Keys**
- **Distribute Keys**
- **Record All Details**



Key Management – Architecture (symmetric & asymmetric key Inventory)

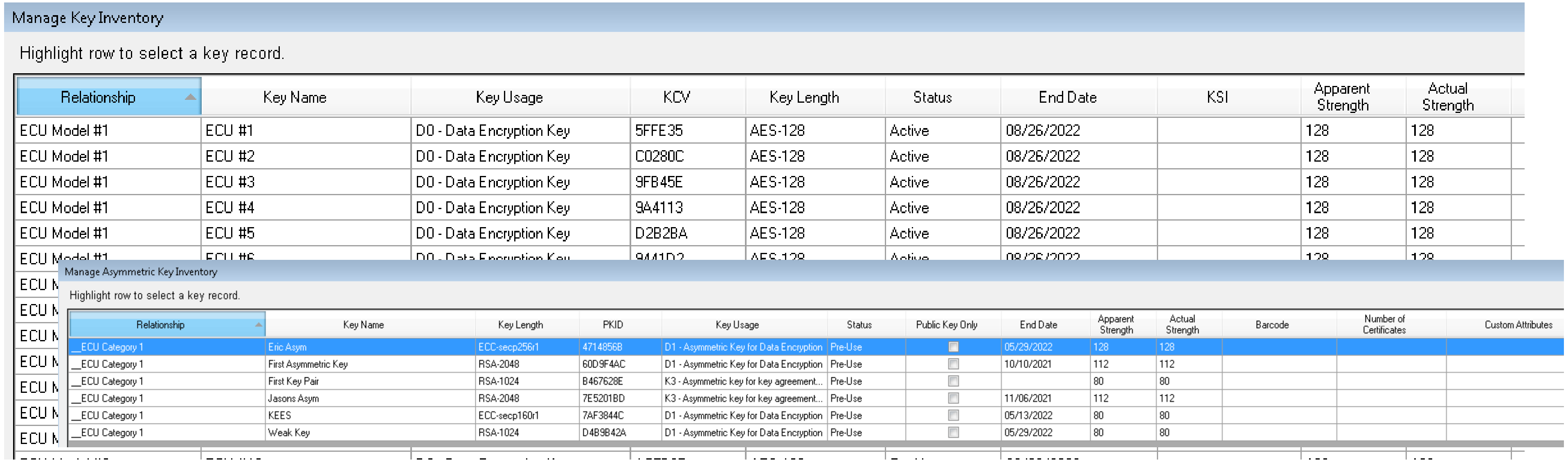
All Working Level Keys
TDES
AES
RSA
ECC

With Full Lifecycle History, Common & Custom Meta-Data, Accessible via RBACs

- **Single Centralized View of Full Inventory**
  - **Filterable with multiple criteria**
  - **Customize Quick-View Access for Primary info**
  - **Enabling Drill-Down for detailed meta-data view**

Customize

- Relationships
- Key Names
- Attributes



Manage Key Inventory

Highlight row to select a key record.

Relationship	Key Name	Key Usage	KCV	Key Length	Status	End Date	KSI	Apparent Strength	Actual Strength
ECU Model #1	ECU #1	D0 - Data Encryption Key	5FFE35	AES-128	Active	08/26/2022		128	128
ECU Model #1	ECU #2	D0 - Data Encryption Key	C0280C	AES-128	Active	08/26/2022		128	128
ECU Model #1	ECU #3	D0 - Data Encryption Key	9FB45E	AES-128	Active	08/26/2022		128	128
ECU Model #1	ECU #4	D0 - Data Encryption Key	9A4113	AES-128	Active	08/26/2022		128	128
ECU Model #1	ECU #5	D0 - Data Encryption Key	D2B2BA	AES-128	Active	08/26/2022		128	128
ECU Model #1	ECU #6	D0 - Data Encryption Key	9441D2	AES-128	Active	08/26/2022		128	128
ECU M									
ECU M									
ECU M									
ECU M									
ECU M									
ECU M									
ECU M									

Manage Asymmetric Key Inventory

Highlight row to select a key record.

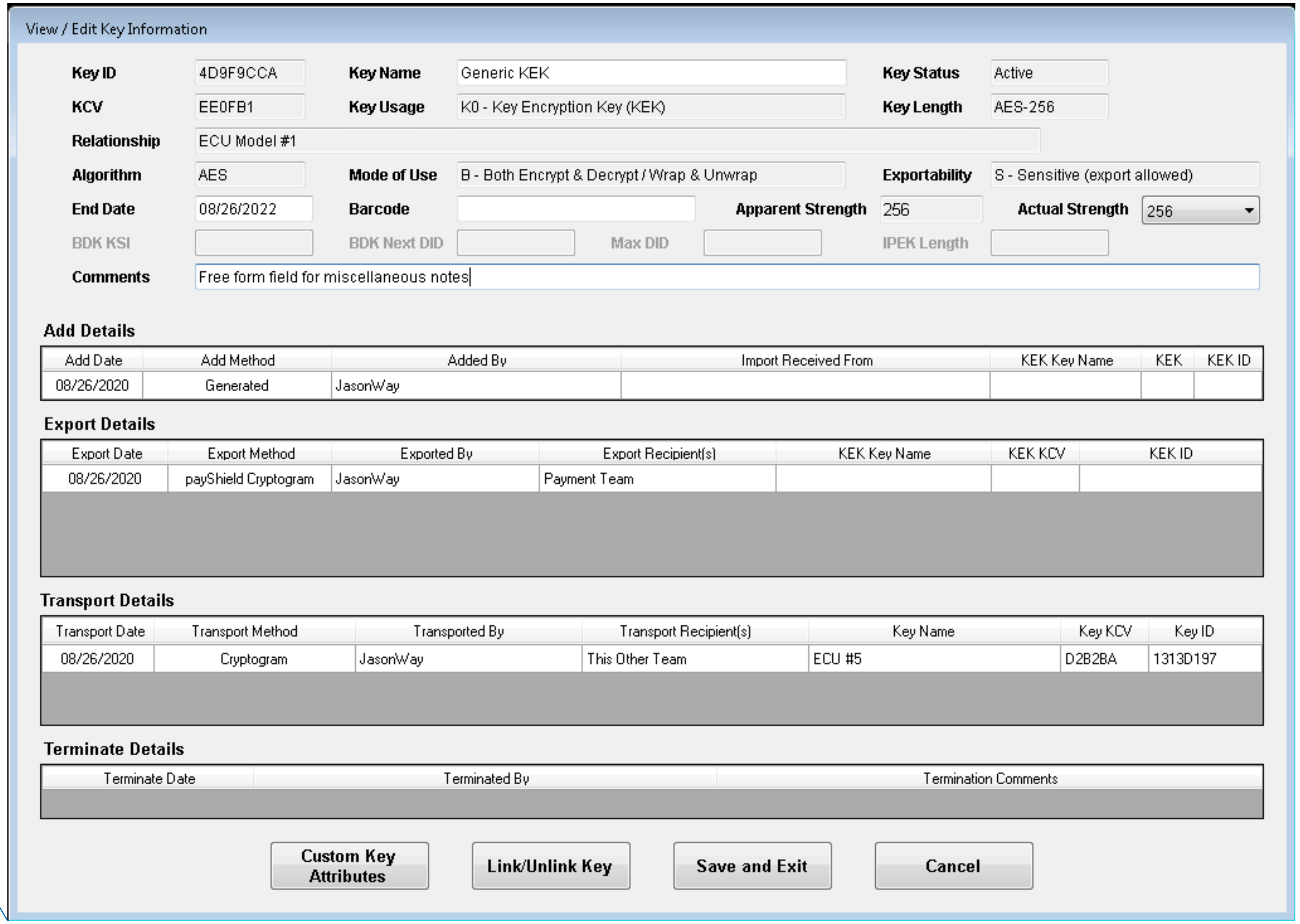
Relationship	Key Name	Key Length	PKID	Key Usage	Status	Public Key Only	End Date	Apparent Strength	Actual Strength	Barcode	Number of Certificates	Custom Attributes
__ECU Category 1	Eric Asym	ECC-secp256r1	4714856B	D1 - Asymmetric Key for Data Encryption	Pre-Use	□	05/29/2022	128	128			
__ECU Category 1	First Asymmetric Key	RSA-2048	60D9F4AC	D1 - Asymmetric Key for Data Encryption	Pre-Use	□	10/10/2021	112	112			
__ECU Category 1	First Key Pair	RSA-1024	B467628E	K3 - Asymmetric key for key agreement...	Pre-Use	□		80	80			
__ECU Category 1	Jasons Asym	RSA-2048	7E5201BD	K3 - Asymmetric key for key agreement...	Pre-Use	□	11/06/2021	112	112			
__ECU Category 1	KEES	ECC-secp160r1	7AF3844C	D1 - Asymmetric Key for Data Encryption	Pre-Use	□	05/13/2022	80	80			
__ECU Category 1	Weak Key	RSA-1024	D4B9B42A	D1 - Asymmetric Key for Data Encryption	Pre-Use	□	05/29/2022	80	80			

Key Management - Architecture

All Working Level Keys
TDES
AES
RSA
ECC

With Full Lifecycle History, Common & Custom Meta-Data, Accessible via RBACs

Drill Down – Meta Data View



View / Edit Key Information

Key ID	4D9F9CCA	**Key Name**	Generic KEK	**Key Status**	Active		
KCV	EE0FB1	**Key Usage**	K0 - Key Encryption Key (KEK)	**Key Length**	AES-256		
Relationship	ECU Model #1						
Algorithm	AES	**Mode of Use**	B - Both Encrypt & Decrypt / Wrap & Unwrap	**Exportability**	S - Sensitive (export allowed)		
End Date	08/26/2022	**Barcode**		**Apparent Strength**	256	**Actual Strength**	256
BDK KSI		BDK Next DID		Max DID		IPEK Length	
Comments	Free form field for miscellaneous notes						

Add Details

Add Date	Add Method	Added By	Import Received From	KEK Key Name	KEK	KEK ID
08/26/2020	Generated	JasonWay				

Export Details

Export Date	Export Method	Exported By	Export Recipient(s)	KEK Key Name	KEK KCV	KEK ID
08/26/2020	payShield Cryptogram	JasonWay	Payment Team			

Transport Details

Transport Date	Transport Method	Transported By	Transport Recipient(s)	Key Name	Key KCV	Key ID
08/26/2020	Cryptogram	JasonWay	This Other Team	ECU #5	D2B2BA	1313D197

Terminate Details

Terminate Date	Terminated By	Termination Comments

Lifecycle management of each individual key

Use Case: Universal Key Management

Customer profile

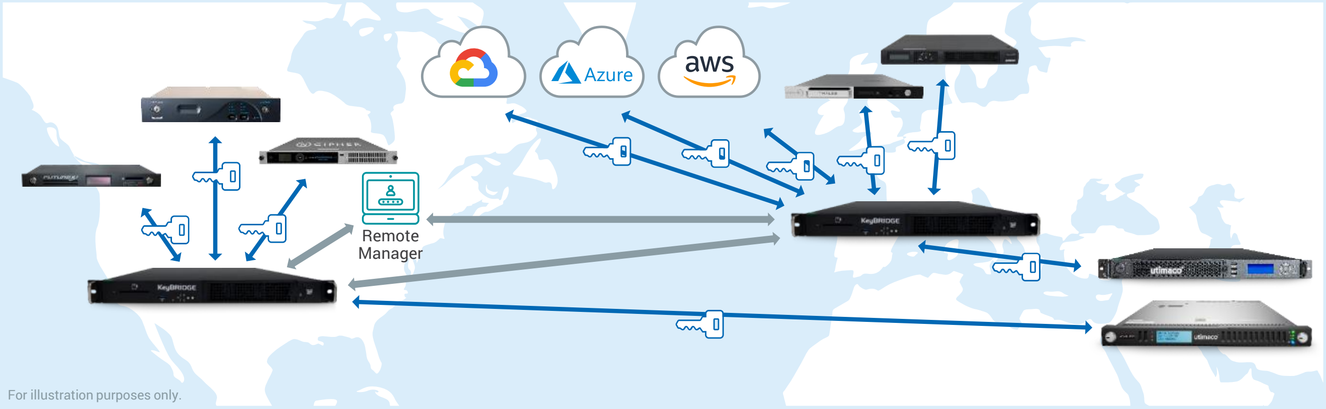
Merchant Acquirer with Heter
Environment

Business Challenge(s)

- **Unify** key inventory
  HSM key management landscape
- PCI-PIN Certified Policy based
  Key Life Cycle Management
  including **Distribution** Control
- Deploy Cloud – **BYOK** in production

Demonstrate Compliance for Audit

- Single Solution
- Streamline Written Policies/Procedures
- Single audit trail



For illustration purposes only.

UTIMACO KeyBRIDGE UKM

Manage and integrate existing HSM & Cloud Use Case under one umbrella

KeyBRIDGE Advanced Security Features

Physical Security

- Built-in **FIPS** & **PCI-HSM v3** certified HSM
- Built-in **smart card reader**
- **Secure Cryptographic Device** for Component entry

Logical Security

- **RBAC** enforced with dual control and split knowledge
- **Extensive audit logs** containing the complex workflows with mapping to all required data elements
- **Remote Centralized Key Management** built on JSON schema RESTFul API

Summary

- KeyBRIDGE UKM allows a business to simplify their **Audit requirement**

- Reduce **risk** & **liability** on the key custodian / officer

- KeyBRIDGE UKM built-in key management for both **GP HSM** and **Payment HSM** allows a business to have a **single pane of glass** / KB

Thank you

for your attention!

UTIMACO GmbH

Germanusstraße 4
52080 Aachen
Germany

Phone +49 241 1696-0
Web https://hsm.utimaco.com
E-Mail hsm@utimaco.com

utimaco®