Solution Leaflet

Securing Workloads in the Cloud Using an External Key Manager

Creating Trust in the Digital Society

utimaco®

The dilemma when moving to the cloud

Organizations that want to move their data to the cloud are often faced with a dilemma. Using cloudified resources like virtual machine instances, databases, etc. gives customers the scalability, flexibility, and security they need. The key material can also be stored where the data is located for convenience reasons. However, there are customers with special security needs or compliance requirements for whom, this generation and placement of cryptographic keys is not suitable. There is a special solution for these users and their encryption keys, and it's called BYOK – Bring Your Own Key – where the customers can bring their own key and inject it into the cloud instances instead of using one provided by their CSP.

The traditional BYOK scenario

With the BYOK concept, organizations can maintain control of the cryptographic keys used in the cloud to keep their data secure. With the right key manager like ESKM by their side, organizations can create their own keys using a FIPS approved algorithm, and send the keys in real time to the cloud.

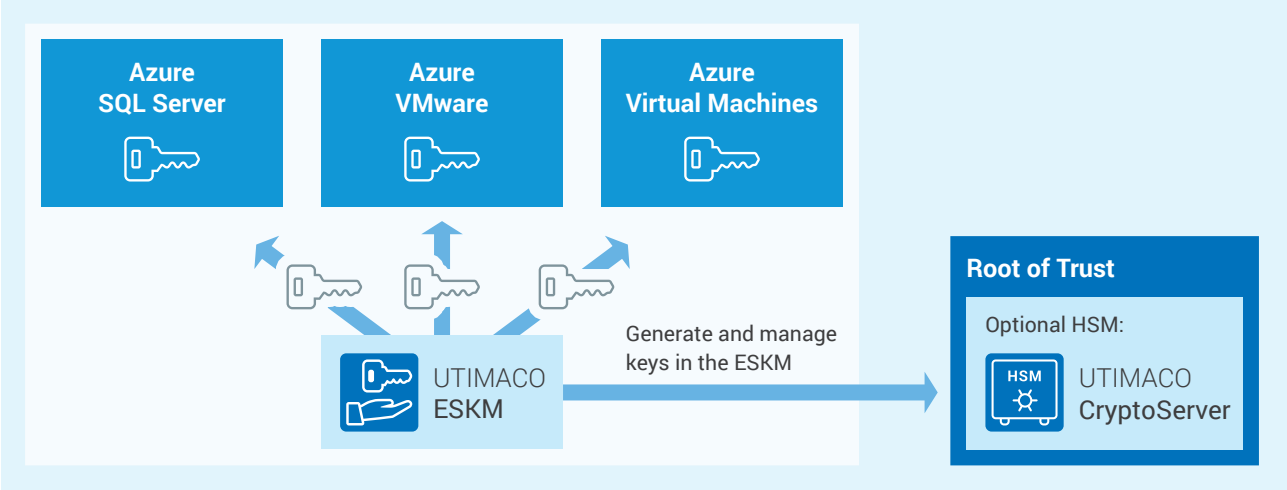

Figure 1: A typical multi-cloud BYOK scenario

Benefits of BYOK

1. Serve a unique key to multiple CSPs
2. Manage both ESKM-created, and CSP-created keys in the ESKM
3. Create keys using FIPS approved, Random Number Generator, backed by an HSM

Using an external key manager like ESKM helps control key access

Some organizations require more control, and for such customers, the BYOK concept can be enhanced further by using an external key manager. This way, the encryption keys stay with the organization and not with the CSP. And when the CSP needs a key, they will provide a reason for the key access request.

Depending on the reason, the organization can decide if it's legitimate enough to hand the key for. Reasons such as query optimization may not qualify to give the key for, whereas maintaining the database or report generation could be a qualifier.

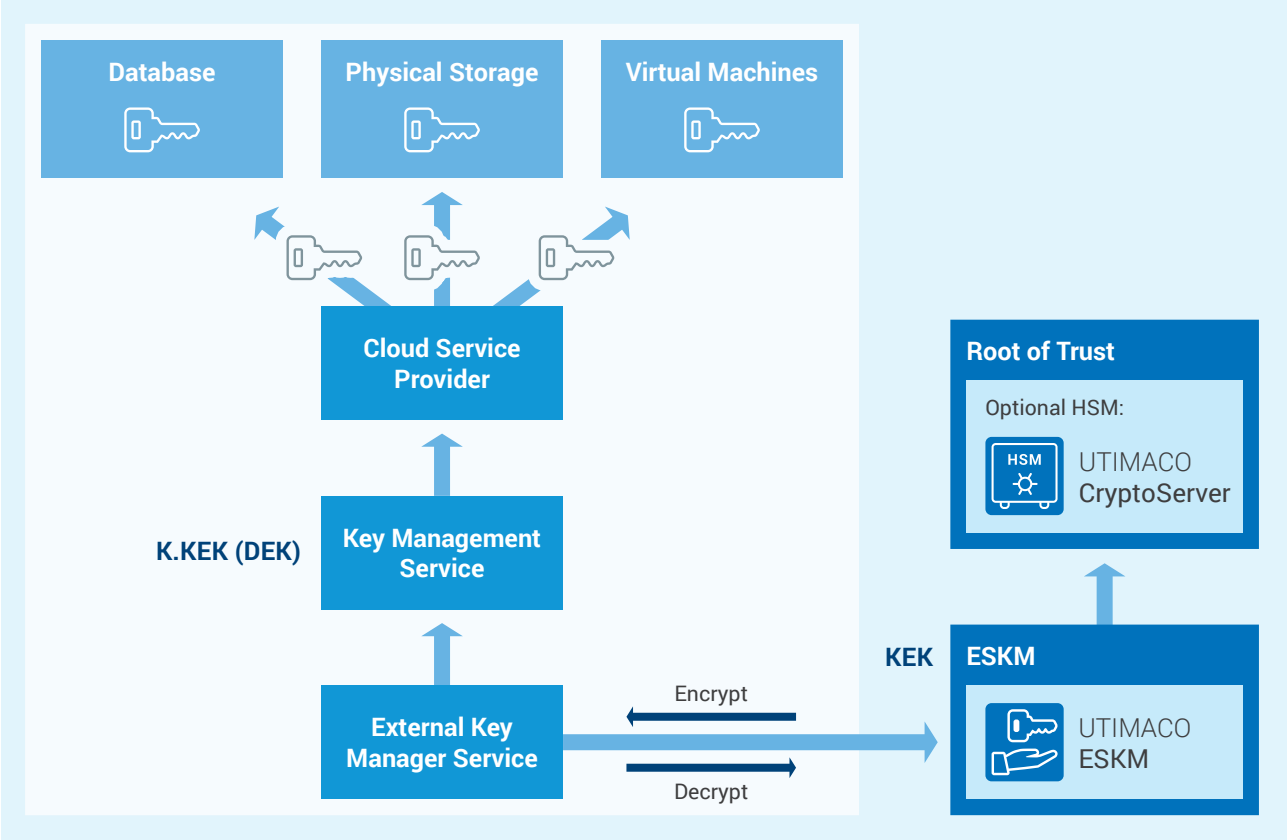

Figure 2: Using an External Key Manager

EKMS is a feature that enables customers to encrypt their data in several Cloud services using encryption keys stored in a third-party key management system outside of the CSP's infrastructure. EKMS keeps the encrypted data in the Cloud separate from the encryption keys stored outside the cloud. With enhanced key permissions, customers can have control over access to their data in the Cloud by requiring a reason for every encryption key request.

Some of the CSPs like Google and AWS are already implementing support for EKMS to protect their customer's data without holding the keys. ESKM, a multi-cloud key manager is integrated with Google and AWS and implements EKMS allowing the customer to protect their workloads on-prem and in cloud.

With EKMS, Enterprises encrypt their own data, retain control of their encryption keys, and do not give the control away to the CSP.

Benefits of an External Key Manager

1. Serve a unique key to multiple CSPs
2. Manage both ESKM-created, and CSP-created keys in the ESKM
3. Create keys using FIPS approved, Random Number Generator, backed by an HSM

Plus, the following:

4. The CSP doesn't have access to your keys
5. You can justify the rationale behind the key access request
6. Data Sovereignty

Other ESKM benefits

Full key control and data sovereignty

- Cryptographic keys remain under your control in a secure, FIPS validated environment
- Key Control and Management through a single pane of glass
- Reliable policy controls
- Centralized administration and audit trails to assist in control attestation

Meets highest security requirements

- Hardware-based security
- Designed for NIST SP 800-131A and FIPS 140-2 Levels 1, Level 2, and Level 3
- Meets enhanced compliance requirements such as PCI DSS, HIPAA, and GDPR

High availability and capacity

- Capacity to manage millions of keys, thousands of clients, and thousands of hardware or virtual appliances

Integrated, flexible, and easy to use

- Easy deployment and simple licensing
- Comprehensive monitoring, recovery, scheduled backups, and log rotations, restore functionality
- Web browser GUI and Command Line Interface
- Support for partner applications and pre-qualified solutions through the first industry-certified Key Management Interoperability Protocol (KMIP)
- Simplified RESTful API interface for key CRUD (Create, Read, Update, Delete) operations and crypto functions

Multi Cloud ready

- Works with the most common cloud service providers such as Microsoft Azure, AWS, Google Cloud, and more
- Flexible migration from one cloud provider to another possible
- No vendor-lock-in
- Keys remain under your sovereignty
- Possibility to use the same keys across multiple cloud service providers

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

…people, devices and digital identities
against natural disaster, terrorism and cyber crime.

…financial transactions, data at rest and in motion
against theft and sabotage.

We protect …

…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

Creating Trust in
the **Digital Society**

utimaco®