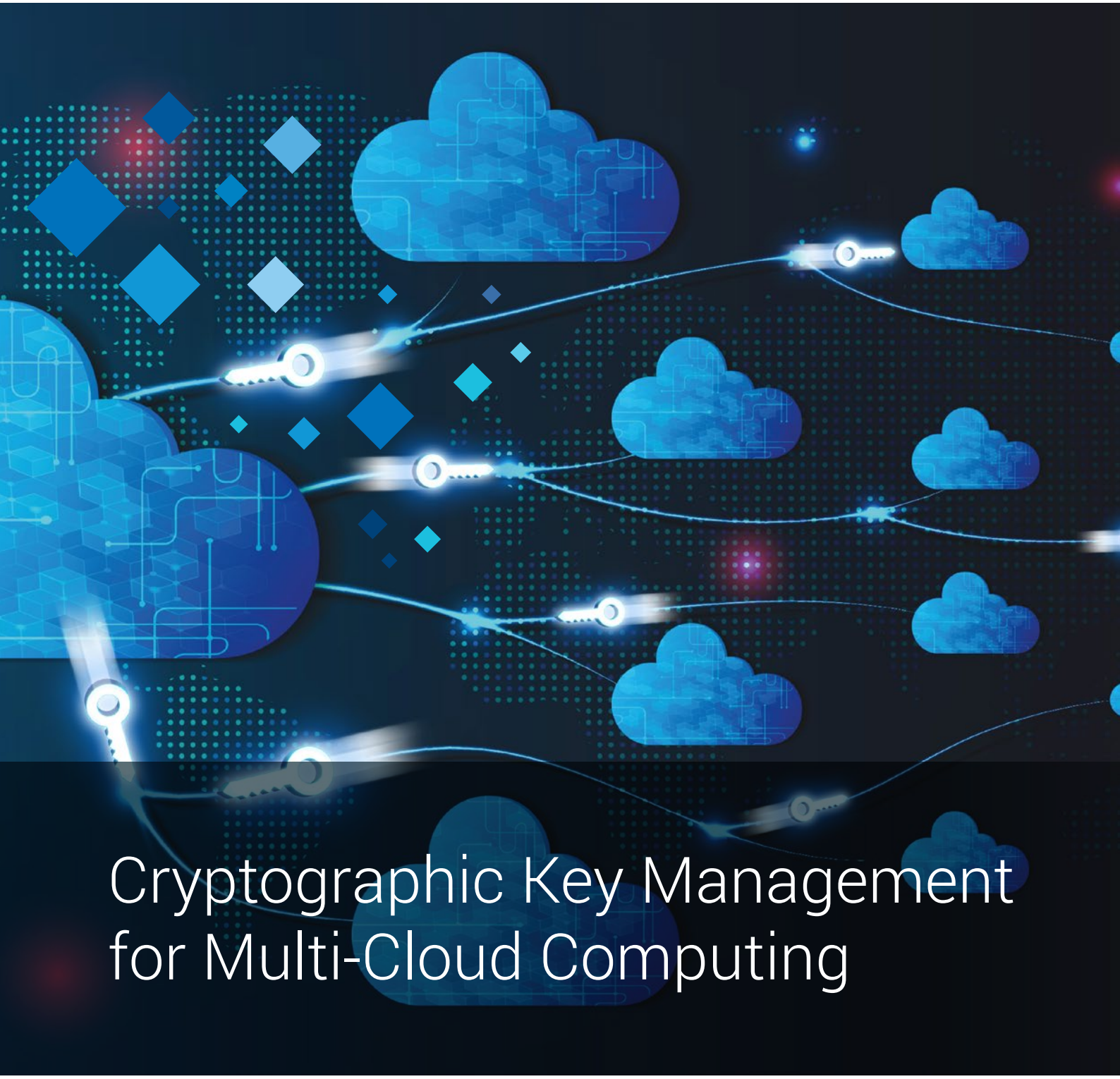
Solution Leaflet



Cryptographic Key Management for Multi-Cloud Computing

Creating Trust in the Digital Society

utimaco® 40 YEARS

Moving to the cloud is a modern-day necessity

Being dependent on an on-premises infrastructure is costly, and requires considerable effort to maintain. The cloud offers countless benefits for organizations such as storing, accessing, and maintaining data, without having to own their own data centers. As cloud storage poses as a comfortable solution in many ways, entire infrastructures are being moved to the cloud.

Businesses survive by being agile and getting new products and solutions to market. Migrating to the cloud has become one of the most important elements of digital transformation for a successful, modern enterprise. But how do you find assurance that your data is secure in the cloud?

Multi-Cloud/Hybrid Cloud for Data Storage

To have an effective cloud strategy, organizations can choose to adopt a multi-cloud computing approach, where a mix of two or more public cloud services such as AWS, Microsoft Azure, Google Cloud, DigitalOcean, or others, can be used within one architecture at the same time. This means for example that you can use Microsoft Azure to serve your US customers, and AWS for your European customers. Or you can run different apps on different clouds - you can for instance use Google Cloud for data storage, Microsoft Azure for development and testing, and AWS for disaster recovery.

A multi-cloud deployment is a mix of multiple public clouds from different providers that are generally not connected. A hybrid cloud on the other hand, combines different types of cloud: a third-party public cloud with an on-premises private one with communication between these two.

Many business areas, including banks, the automotive industry, the manufacturing industry, as well as governments are increasingly leveraging a hybrid cloud strategy for the purpose of improving their service offerings and cost performance and to increase agility and time-to-market. In a hybrid cloud, companies can blend the best of local data centers and cloud infrastructures, including service mash-ups.

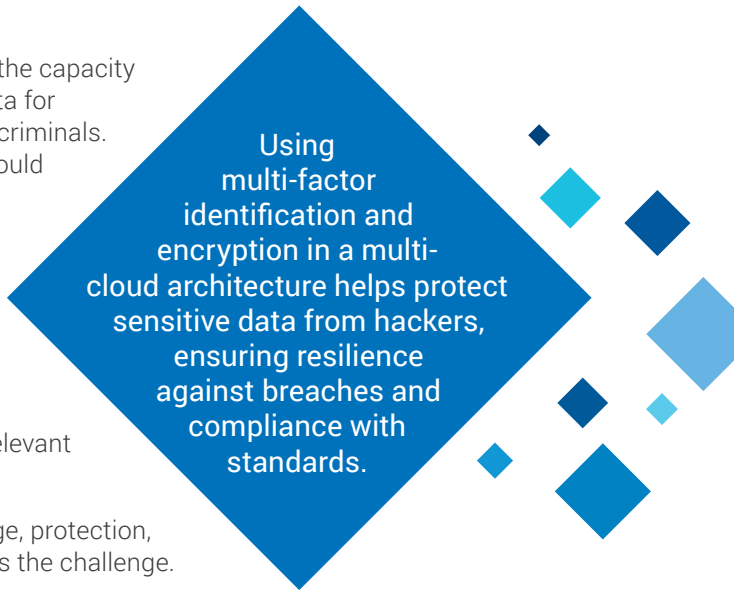
With all this increased complexity and convolution, how do you keep everything secure? Is there a simple way to protect your data at all times?

Multi-cloud security

While the exponential growth of cloud services has increased the capacity of data storage and expediated the processing of sensitive data for businesses, it has also turned the cloud into a haven for cybercriminals. Organizations moving to or using multi-cloud deployments should be aware of the potential security threats that exist and apply best practices in order to protect their cloud-based data.

Multi-factor identification and encryption can be used to prevent intruders from hacking their information. Organizations need to encrypt all the network connections to public cloud services within the multi-cloud architecture that involve sensitive data. Encryption of sensitive data brings resilience against data breaches as well as compliance with relevant standards and regulations.

The encryption aspect itself is not difficult to do. It's the storage, protection, and lifetime key management of the encryption keys that holds the challenge.



Key Management

There are many reasons that organizations have a need for centralized key management; to prevent against data breaches, to be compliant, to protect data at rest, and to manage a high volume of encryption keys used across different infrastructures. A key manager makes sure that the keys stay separate from the encrypted data that needs to be protected, and provides an audit trail so that you can know who accessed what data at what point of time.

A centralized and robust enterprise key management system is an effective and efficient way to secure keys and manage them during their entire lifecycle.

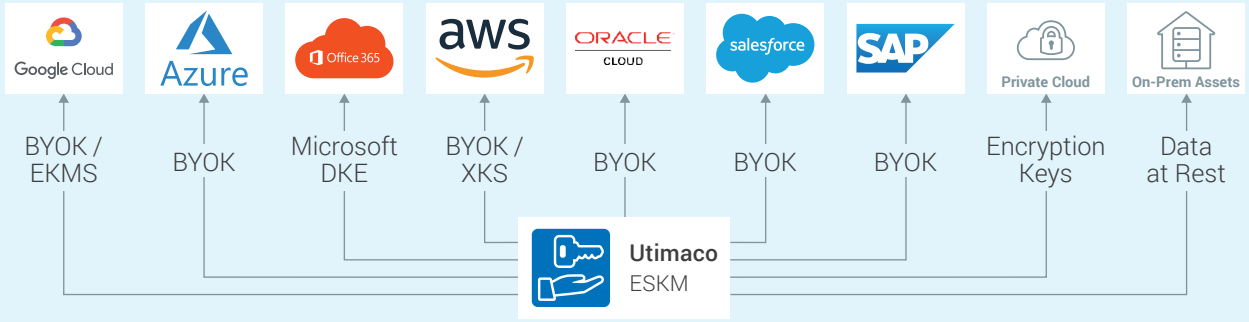
Operating a key manager on-premise is one thing, but what happens when you need to move data to the cloud? How do you know that your data will still be secure?

Multi-Cloud Key Management

Multi-cloud key management is about applying key management capabilities to environments where multiple different clouds are used. Utimaco's solution to multi-cloud key management, the ESKM, integrates seamlessly into private, hybrid, or multi-cloud environments. It enables organizations to centrally manage the lifecycle of all keys, from a single pane of glass, no matter if these keys are used on-premises, or in the cloud, or if multiple CSPs are being used.

ESKM is a Single Pane of Glass for all Key Management

- Protect on-prem and cloud workloads
- Single pane of glass
- Data Sovereignty
- Highly Available solution
- Simple integration
- Scalability (thousands of nodes, millions of keys)
- REST API for external integrations
- On-Prem and Cloud Deployments
- HSM Protected



Benefits of ESKM

- **Streamlines data and processes**
  ESKM enables unified enterprise key management with reliable policy controls, centralized administration, and audit trails to reduce operational costs and assist in control attestation.
- **Provides the highest level of security**
  Tamper-responsive with the ability to act in response to side-channel attacks with FIPS 140-2 Level 1, Level 2, Level 3 and Level 4 (physical) compliant architecture; certificate-based authentication and built-in CA.
- **Is compliance driven**
  Meets audit and compliance mandates with controls for PCI-DSS, HIPAA, EU data privacy laws and other regional privacy mandates.
- **Provides easy integration**
  Provides a simplified RESTful API interface for key CRUD operations (Create, Read, Update, Delete), and crypto operations (Encrypt, Decrypt, Sign, Verify), that results in flexibility and ease of use supporting key management and encryption.

Conclusion

Multi-cloud architecture provides an environment where businesses can build secure and powerful cloud environments outside the traditional infrastructure. Multi-cloud key management gives organizations the needed control and autonomy to operate their daily business activities. With independence from a specific cloud service provider, and uncompromisable protection of data privacy with regard to third parties, key management in the cloud is becoming more and more controllable and manageable.

Utimaco's ESKM is here to support you on your journey to create a highly secure, compliant, and integrated multi-cloud key management environment.

Visit us at utimaco.com to find out more!

Utimaco
Enterprise Secure
Key Manager – ESKM

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.

550+ 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

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®