

Implementing Data Sovereignty Strategies with Strong Cryptographic Protection

Achieving Highest Sovereignty Levels through Separation of Encrypted Data and Key Material

The Critical Question Every Organization Must Answer

Data Sovereignty is crucial for the security and disclosure of digital data as well as for legal and compliance reasons.

Organizations are forced to implement the right protection measures in order to be confident about the answer to the question:

Who can access our data?

If an organization fails to implement the right digital protection strategy, their data could be exposed to the risk of third-party access while being non-compliant to internal and external requirements.



Unlocking Data Sovereignty by Strong Cryptographic Protection

Implementing full Data Sovereignty requires the right combination of strong encryption and reliable key management capabilities.

This means ensuring:

- ♦ Strict separation of encrypted data and cryptographic keys
- ♦ Secure key storage outside of CSP environments
- ♦ Central key control and reliable access management
- ♦ Complete audit trails
- ♦ Compliance with security policies and regulatory requirements



The Challenge: Keeping Control Over Digital Information Across Distributed Environments

Data Sovereignty in digital environments is crucial for the security and disclosure of data as well as for legal and compliance reasons.

Today's organizations are becoming endpoints of a global network of digital environments and must face the challenge to effectively protect their sensitive digital information at every entry point from external access while keeping it accessible for their authorized users.

Data that is created within a nation's borders is governed by that nation's laws and regulatory frameworks. This also implies that this country has the authority over how the data is accessed, stored, and used. When it comes to the use of both public and private Cloud infrastructures, this introduces complexity for organizations because data may reside in servers outside the country of data origin or the organizations' location.

In order to benefit from the advantages that Cloud offers while staying fully aligned with local laws and compliance requirements, organizations must implement the right data protection measures.

Data Sovereignty: How Secure and Compliant Data Protection must be Designed

When organizations host data with global Cloud Service Providers (CSPs) like AWS, Azure, or Google, they often face a "sovereignty paradox" connected to foreign laws. In the case of the U.S. CLOUD Act a CSP based in the United States may be legally compelled to hand over that data, even if stored in a specific geographic region outside of the US territory.

By storing the keys used to encrypt your cloud-stored data, outside of the cloud, either in a key manager on-premises or a 3rd party managed service, your data and keys are fully protected. And with that full key protection, you are automatically leveling up the protection level of your digital data – up to full Data Sovereignty depending on the model deployed, including security and compliance and disclosure prevention. Without your keys, cloud providers do not have access to and cannot disclose your data even for lawful requests.

Utimaco's Key Management Solutions Enabling your Data Sovereignty Strategy

Strong Encryption ♦ Cloud-Agnostic Key Management ♦ Reliable Separation of Encrypted Data and Keys ♦ Flexibility Across Cloud Environments

Data sovereignty has become increasingly important due to cloud computing and global data flows, where data can be stored and processed across multiple countries.

By utilizing strong cryptographic protection combined with the logical management capabilities of a proper Key Management System, organizations can easily enable full Data Sovereignty across your environment, prevent the risk of third-party access under the U.S. CLOUD Act, and ensure compliance with data protection regulations across the globe, for example GDPR & Schrems II, PIPEDA, PDPL, PIPL, PDPA and APPI.

As a leading cybersecurity solution provider, Utimaco serves you with the right tools to enable your Data Sovereignty strategy.

Hardware Root of Trust with General Purpose HSM for Secure Data Encryption		Centralized Key Management System for Reliable Key Access Management	
Utimaco's General Purpose Hardware Security Modules (GP HSMs) provide the foundation for strong protection of digital data and communications. The HSM generates and protects cryptographic keys within tamper-resistant hardware where they cannot be extracted.		While HSMs generate and protect cryptographic keys within tamper-resistant hardware, managing how those keys are distributed, stored, utilized, and rotated across the endpoints within their digital environments is a must for organizations' data sovereignty strategies. Utimaco's centralized Key Management Systems (KMS) enables organizations to: ♦ Keep Full Key Sovereignty: Keeping complete ownership and control over encryption keys based on strict key access mechanism. Control independent from cloud-provider infrastructure to unlock Digital Sovereignty. ♦ Strengthen Data Sovereignty Compliance: Supporting organizational regulatory strategies with clear, independent control over critical security assets. ♦ Address GDPR and U.S. CLOUD Act risks: Reducing Data Sovereignty GDPR exposure and the risk of third-party access under the U.S. CLOUD Act. ♦ Stay Flexible Across Every Cloud: Using Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) across public, private, hybrid, and multi-cloud environments. ♦ Break Free From Vendor Lock-in: Preserving Cloud Data Sovereignty and maintain control wherever data resides.	
Future-Ready Security with Crypto-Agility Digital infrastructures deployed today must remain secure in the face of emerging threats, including advances in quantum computing. Utimaco's GP HSMs are designed crypto-agile, enabling organizations to transition toward post-quantum cryptographic algorithms as standards evolve. Utimaco's GP HSMs are designed crypto-agile, enabling organizations to transition toward post-quantum cryptographic algorithms as standards evolve.		By adopting the application package Quantum Protect to our GP HSMs organizations enable their crypto-agile infrastructure today, enterprises ensure that the trust foundations protecting their AI systems remain secure in the post-quantum era.	
Enable Future-Ready Security with Quantum-Protect			
 Utimaco u.trust General Purpose HSM Se-Series / CSe-Series	on-premises	 Utimaco Enterprise Secure Key Manager	on-premises
 Utimaco u.trust General Purpose HSM as a Service	aaS	 Utimaco Enterprise Key Manager as a Service	aaS

Data Sovereignty is not a feature you switch on — it is the outcome of encrypting your data, controlling your keys, monitoring every operation, and meeting compliance obligations with confidence.

Contact our Sales Team to discuss how to start your Digital Sovereignty Strategy.

For more information about Utimaco products, please visit us at utimaco.com or send an e-mail to hsm@utimaco.com

© Utimaco IS GmbH 09/26 – Version 1.0

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.

utimaco®