cpl.thalesgroup.com

Microsoft | THALES
Building a future we can all trust

Microsoft Azure and Thales Luna HSMs

A Digital Transformation Partnership Ensuring The Security Of Data In The Cloud

Organizational Impact From Digital Transformation

Cloud capabilities continue to alter businesses across the globe creating changes that directly influences the security community. Underlying trends that have always had an impact, such as new technologies, stricter compliance mandates, and more severe security incidents, continue to cause significant change. The shift to remote work is extending indefinitely in many organizations globally, with some choosing hybrid work environments. This digital transformation affects both small and large organizations who continue to adapt their operational processes to create efficiencies and maximize revenue. The rapid pace and complexity of the changes means many organizations are potentially not adequately or compliantly securing their data; certain types of data require certifications that secures the data through a HSM (Hardware Security Module), a physical device whose traditional on premise use can seem counterintuitive to the cloud. However, with the right next generation HSM, you can secure your data as it evolves, on-premises, in the cloud, and across hybrid environments.

Considerations And Challenges

Moving your data to the cloud offers many benefits, but as with any change, it must be well thought out and prepared for especially when it comes to keeping your data secure throughout the process and if you need to incorporate an HSM. Some of these include:

- **Operational** – what data requires your full control, and what doesn't?
- **Access management** – who needs to access which data, and how?
- **Remote/hybrid work environment** – how will the data in its various locations remain protected?
- **Security and compliance** – how will these change when implementing new technology? How will they be met?
- **Location** – what data could be stored in the cloud, and which on-premises?
- **Type** - Do you need a general purpose HSM such as the Luna or one for payments such as payShield?

Reassuringly, Microsoft Azure cloud solutions use Thales HSM technology to address these challenges and deliver a compelling value proposition to users of the service. Let us explore how.

Microsoft Azure and Thales Luna HSMs

By default, Azure generates encryption keys on behalf of customers and manages their lifecycle. For many organizations hosting sensitive data in the cloud, they want to enhance their security and control over their encryption keys for compliance or internal security requirements. These organizations want full control over how and when encryption keys protect and access encrypted data or need to follow security best practices. Additionally, many organizations would like a separation of duties between the party holding the encryption keys and the cloud provider holding the data. This is how Thales Luna HSMs can help.

Microsoft, together with Thales, enable you to own and control encryption key material outside of Azure Cloud in the event that you require complete data sovereignty, compliance with certifications such as FIPS, with enhanced security provided by a Thales Luna HSM. Help your customers easily store and manage cryptographic keys separate from their sensitive data, enhancing encryption key control and data security in the Azure Cloud.

With Luna HSMs, you can:

- Generate and store cryptographic keys
- Establish a common root of trust across applications and services
- Encrypt and decrypt data encryption keys
- Protect secrets (passwords, SSH keys, etc.)
- Isolate keys and signing operations from certificate authorities, host platforms, and operating systems
- Automate key lifecycle control and processes

Luna HSM integrates with Microsoft Azure to make it easy for customers to follow security and key management best practices, while leveraging the power of Azure Cloud.

Flexible Options To Choose From

Thales, alongside Microsoft, offers a number of encryption management solutions leveraging Thales Luna HSMs to secure and protect your data regardless of its location. Thales Luna HSMs can be deployed on-premises, in the cloud, as a service, or across multiple hybrid environments. You have the flexibility to leverage cloud services, the ability to both own and control your encryption keys, and/or reduce the risk of unauthorized data access or data loss.

Luna Cloud HSM Service on Thales Data Protection on Demand (DPoD)

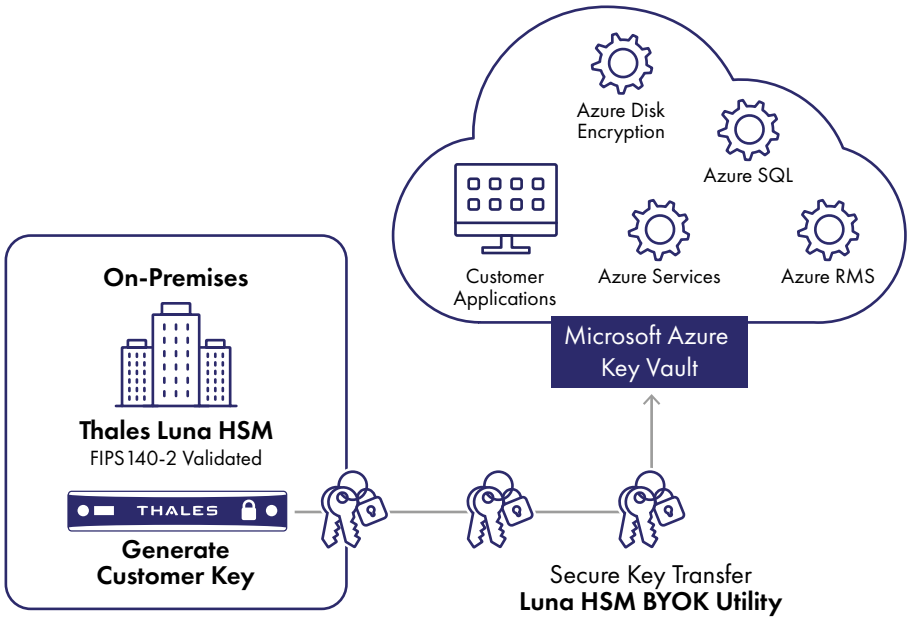
The Luna Cloud HSM service is a generic key vault that can also perform cryptographic operations such as encryption/decryption of data encryption keys, protection of secrets (passwords, SSH keys, etc.), and more, across multiple environments including on-premises, in the cloud or hybrid infrastructures.

Deployed in under 5 minutes, the Luna Cloud HSM service can be used as a root of trust for a wide variety of use cases such as code signing, PKI, Blockchain and IoT and includes an extensive list proven integrations including Microsoft ADCS, Authenticode and SQL Server.

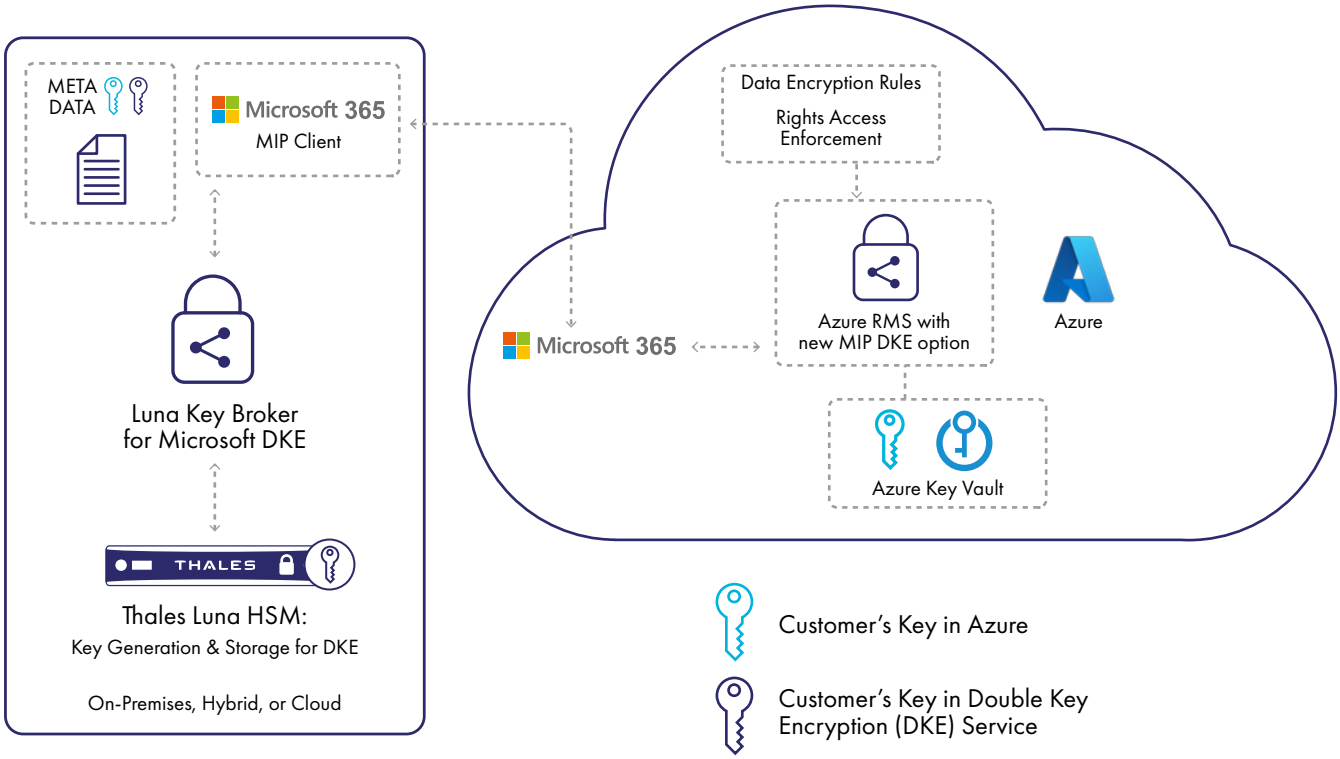
The Thales Luna Cloud HSM service uses a FIPS 140-2 Level 3 certified hardware security module which makes it easy for you to follow data security and compliance best practices while leveraging the benefits of Azure Cloud services.

Azure Infrastructure

Bring Your Own Keys (BYOK)



Double Key Encryption (DKE)



Microsoft 365 Double Key Encryption (DKE) Get added security using two keys: one created and held by Microsoft in Azure, and another created and held under customer control	Encryption keys utilizing Luna HSMs provide organizations with 100% control over access to encrypted data and key lifecycles — best solution for highly sensitive content that requires additional protection.
Bring Your Own Key (BYOK) Tenant root keys generated by customer	Create encryption keys in your own environment and then securely bring those Luna HSM protected keys directly into Azure Key Vault for use.
Keys Generated by Microsoft Tenant root keys generated by Microsoft	Both key generation and lifecycle control rest solely with Microsoft.

MORE SECURE

Key Partnership Benefits

Flexibility

- Choose from various solutions offered by Thales that best fit your needs; all integrate to work seamlessly with Microsoft

Security & Compliance

- Comprehensive separation of duties solidifying trust in Azure Cloud
- Enhanced security with support for advanced Azure Cloud features

Operations

- Streamline your operations through centralized key management for on-premises, hybrid or multi-cloud environments
- Simplify encryption key management with secure key generation, storage, distribution, deactivation and deletion across multiple clouds
- Manage both native Azure Cloud keys as well as BYOK/DKE keys

Platform Benefits

Peace of Mind

Create, manage, and store your keys in a tamper-proof root of trust, where your keys never leave in plain text form.

Data Sovereignty

Ensure global compliance and best standards by storing and managing your keys in FIPS 140-2 Level 3 validated HSM.

Key Control

Control your keys and ultimately your data by generating keys in an on-premises, tamper proof HSM.

Flexibility

Take your keys where you want to go with the ability to use the same key in multiple clouds.

Scalability

Scale your business and continue your digital transformation by leveraging technology in the cloud.

Disaster Recovery

Ensure business continuity by keeping a secure copy of key in your possession.

Typical Use Cases

Thales Luna HSMs can be used for any use case, any application, any industry, and any environment. Some common uses are:

- 5G
- Code signing
- Blockchain
- IoT
- PKI
- Quantum
- Remote signing
- SSL/TLS
- ID's for Manufacturing
- Cloud key ownership
- DevOps

For highly regulated industries such as **financial services**, **government**, and **healthcare**, their sensitive data requires the highest level of control and security. These organizations choose the Double Key Encryption (DKE) offering, since it is the most secure. This enhanced data protection capability enables organizations to benefit from the full power of Microsoft 365 collaboration and productivity tools while protecting sensitive data and meeting data privacy regulations and requirements.

Suitable For Both Existing And New Hsm Users

Whether you are setting up an HSM for the first time, or looking to re-structure your existing HSM, Thales Luna HSMs are flexible and able to handle encryption use cases on-premises, in the cloud, and across hybrid environments.

Learn more about Azure Dedicated HSM at Dedicated HSM - Hardware Security Module | Microsoft Azure or about Double Key Encryption at Double Key Encryption with Luna Key Broker. Or simply contact your Microsoft or Thales advisor to schedule an assessment with a team of experts that will help to assess, plan, and implement the best solution.

About Thales Luna HSMs

Thales Luna HSMs have led the market for more than 25 years, and are the foundation of digital security for traditional and emerging technologies across all environments, including hybrid, multi-cloud. Affording you the flexibility to meet your business needs and compliance needs securely and efficiently, Thales provides a high assurance, FIPS 140-2 Level 3 HSM for any use case, any application, any industry, and any environment.

About Microsoft Azure

The Azure cloud platform is more than 200 products and cloud services designed to help you bring new solutions to life – to solve today's challenges and create the future. Build, run and manage applications across multiple clouds, on-premises, and at the edge, with the tools and frameworks of your choice.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us