Your enterprise is looking to leverage all of the advantages the cloud has to offer, but some of the benefits come at a price. In return for flexibility, scalability and automation, encryption key ownership is often given up to the cloud service provider, taking the control out of your hands and increasing compliance complexity.

When it comes to encryption keys, it is all about control. By default Azure generates encryption keys on behalf of customers and manages their lifecycle. For many organizations hosting sensitive data in the cloud, this lack of sole control and ownership over encryption keys does not meet their compliance or internal security requirements. Instead these organizations want full control over how and when encryption keys are used to protect and access encrypted data.

Gemalto offers a number of encryption management solutions based upon SafeNet Luna HSMs or SafeNet KeySecure to secure and protect your data regardless of its location. With Gemalto, enterprises have the flexibility to leverage cloud services, the ability to both own and control their encryption keys, and/or reduce the risk of unauthorized data access or data loss.

Microsoft Azure Cloud

Microsoft Azure offers organizations 3 different encryption key generation and management options:

- **Azure PFX Import (BYOK)**: Import keys generated in on-premises HSMs to provide additional control over native Azure lifecycles and access to encrypted data.
- **Hold Your Own Key (HYOK)**: Encryption keys utilizing on-premises SafeNet Luna HSMs providing organizations with 100% control over access to encrypted data and key lifecycles—best solution for internal, critical, and confidential data.
- **Azure Cloud Key Vault**: Both key generation and lifecycle control rest solely with the service provider.

**Benefits of PFX Import for BYOK**

Although encryption keys are held by the cloud service provider, leveraging your SafeNet Luna HSM to generate keys (vs the Azure created keys) enables you to:

- Extend your HSM investment, without the need to purchase a separate 3rd party HSM
- Ensure protection of PFX-imported keys in Azure hardware
- Enterprise Security Officers maintain full control over the key generation process, aware of the conditions under which they were created
- Ability to archive a copy of the generated keys – retaining a copy for future audit or data migration
- Enhance control over key lifetimes and usage to support your operational and compliance requirements in the cloud
- Once keys are imported you are able to use and leverage the Azure cloud in the same manner as Azure generated keys

**PFX Import for Azure BYOK**

**Enhanced control over encryption key usage**

As a Gemalto customer, the ability to import keys generated in on-premises HSMs via the Azure Key Vault PFX Import capability provides customers with enhanced control over encryption keys used by Azure Services and applications running in the cloud. The PFX Import is performed in just a few simple steps:

- Generate the keys with SafeNet Luna HSM
- Prepare the keys for import into the Azure Key Vault with Gemalto’s free PFX utility
- Using Azure Key Vault commands, import the PFX file containing your keys and specify that the keys be stored in hardware
- After successfully importing the keys, configure Azure services such as Azure RMS to use the imported keys and grant access privileges
- You have now successfully imported your own SafeNet Luna HSM-generated keys into Microsoft Azure
Benefits of SafeNet Luna HSMs

- Network attached HSM for high-assurance
- Small form-factor option for customers needing to physically remove and store the HSM when offline
- FIPS 140-2 Level 2 and 3 certifications
- De facto standard for the cloud

HYOK

100% confidence and key control

HYOK is a Microsoft Azure Information Protection feature that enables organizations to leverage Microsoft Azure cloud services, and comply with complex regulations and policies by not giving up ownership and control over encryption keys.

The integration between Azure Information Protection and SafeNet Luna HSMs enables organizations to store encryption keys in their on-premises HSMs as opposed to storing keying material in the Azure Cloud. As a result, access to internal and highly sensitive data associated with Microsoft Azure applications and services such as Office 365 are now completely under the customer’s control while still being transparent to end users.

HYOK Benefits

- You generate and manage your encryption keys (vs the default option of having Azure do so on your behalf) according to your own security policies while maintaining sole control of encryption keys
- 100% confidence that encryption keys are not shared or used outside of your control or knowledge
- Help meet internal policy and compliance mandates
- Protect highly sensitive internal information while leveraging the benefits of Microsoft Azure Services such as Office 365
- Azure Information Protection Client makes HYOK transparent to end users
- Encryption keys generated and stored in on-premises, high-assurance, FIPS 140-2 certified SafeNet Luna HSMs

Azure-Generated Keys

100% service provider control

As a security conscious enterprise, the convenience of Azure-generated keys needs to be balanced against the risk profile of the data and applications being protected. For higher-assurance applications and data, it is recommended that organizations retain sole control over the generation of encryption keys.

HYOK and PFX Import options provide customers with greater control while still realizing the benefits the Microsoft Azure cloud has to offer.

About Gemalto’s SafeNet Identity and Data Protection Solutions

Gemalto’s portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions—from the edge to the core. Gemalto’s SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Gemalto can help

Contact Gemalto to help you assess and define the data protection strategy that best suits your organizational requirements, and for integration guides to help speed your deployment.

SafeNet Luna HSM Encryption Strategy Summary

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Need</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Keys Must Remain On-Premises</td>
<td>Control access to encryption keys</td>
<td>HYOK</td>
</tr>
<tr>
<td>Support for Azure-Native Services Such as RMS, Office 365, etc.</td>
<td>Enhanced control over native Azure encryption services</td>
<td>PFX Import for BYOK</td>
</tr>
<tr>
<td>Non-Critical Data</td>
<td>Basic data protection and policy compliance</td>
<td>Azure Generated Keys</td>
</tr>
</tbody>
</table>

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com/contact-us

Follow Us: blog.gemalto.com/security