


# Import HSM-protected keys to Key Vault

02/17/2020 • 2 minutes to read •  +8

## In this article

[Supported HSMs](#)

[Next steps](#)

For added assurance, when you use Azure Key Vault, you can import or generate keys in hardware security modules (HSMs) that never leave the HSM boundary. This scenario is often referred to as *bring your own key*, or BYOK. Azure Key Vault uses nCipher nShield family of HSMs (FIPS 140-2 Level 2 validated) to protect your keys.

This functionality is not available for Azure China 21Vianet.

### ⓘ Note

For more information about Azure Key Vault, see [What is Azure Key Vault?](#)  
For a getting started tutorial, which includes creating a key vault for HSM-protected keys, see [What is Azure Key Vault?](#).

## Supported HSMs

Transferring HSM-protected keys to Key Vault is supported via two different methods depending on the HSMs you use. Use the table below to determine which method should be used for your HSMs to generate, and then transfer your own HSM-protected keys to use with Azure Key Vault.

Vendor Name	Vendor Type	Supported HSM models	Supported HSM-key transfer method
nCipher	Manufacturer	<ul style="list-style-type: none"><li>nShield family of HSMs</li></ul>	<a href="#">Use legacy BYOK method</a>

Vendor Name	Vendor Type	Supported HSM models	Supported HSM-key transfer method
Thales	Manufacturer	<ul style="list-style-type: none"><li>SafeNet Luna HSM 7 family with firmware version 7.3 or newer</li></ul>	<a href="#">Use new BYOK method (preview)</a>
Fortanix	HSM as a Service	<ul style="list-style-type: none"><li>Self-Defending Key Management Service (SDKMS)</li></ul>	<a href="#">Use new BYOK method (preview)</a>

## Next steps

Follow [Key Vault Best Practices](#) to ensure security, durability and monitoring for your keys.

Is this page helpful?

 Yes  No