Xorble

Xorble

Every Server, HSM-enabled by design.

Xorble Key Storage Provider for Azure Key Vault

The most cost-effective way to provide a FIPS-backed HSM service with true native Windows KSP integration for Azure VMs is Xorble KSP for Azure Key Vault

Contents

Introduction to Azure Key Vault

Xorble

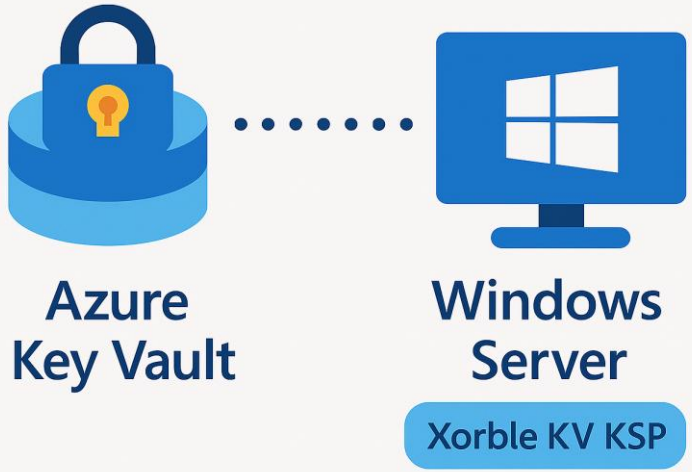
Key Handling in Azure – Key Vault has provided strong cryptographic services since 2015. Fundamentally very strong with no public exploits

Premium Key Vault

- Microsoft managed FIPS 140-2 Level 2 validated Hardware Security Modules (HSMs)

Standard Key Vault

- Keys are protected in software, no dedicated HSM protection for customer keys



Main Issue

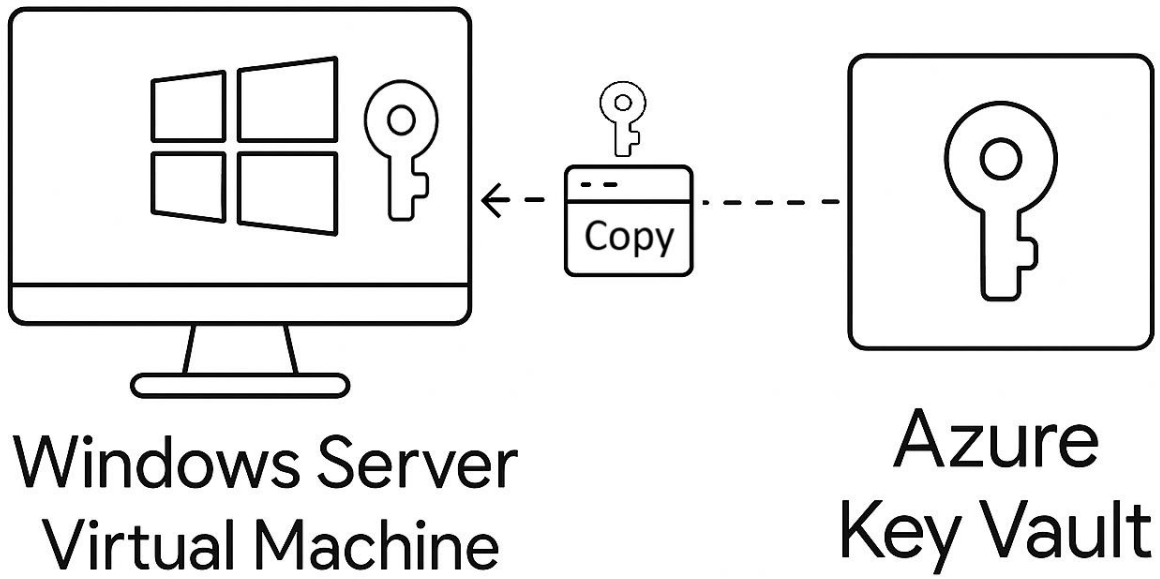
- Microsoft has never provided Key Storage Provider (KSP) that allows native Windows applications to use Key Vault protected keys. Applications were expected to be rewritten
- Therefore, native applications require all keys to be exportable and be copied to the VM via the Key Vault extension
- Azure Key Vault extension for Windows/Linux duplicates keys to VMs – vulnerable to attack

Azure Key Vault – Typical Use

Azure Key Vault extension for Windows/Linux

Key Vault extension retrieves (copies) certificates and keys and installs them on the VM automatically

Every VM gets a copy

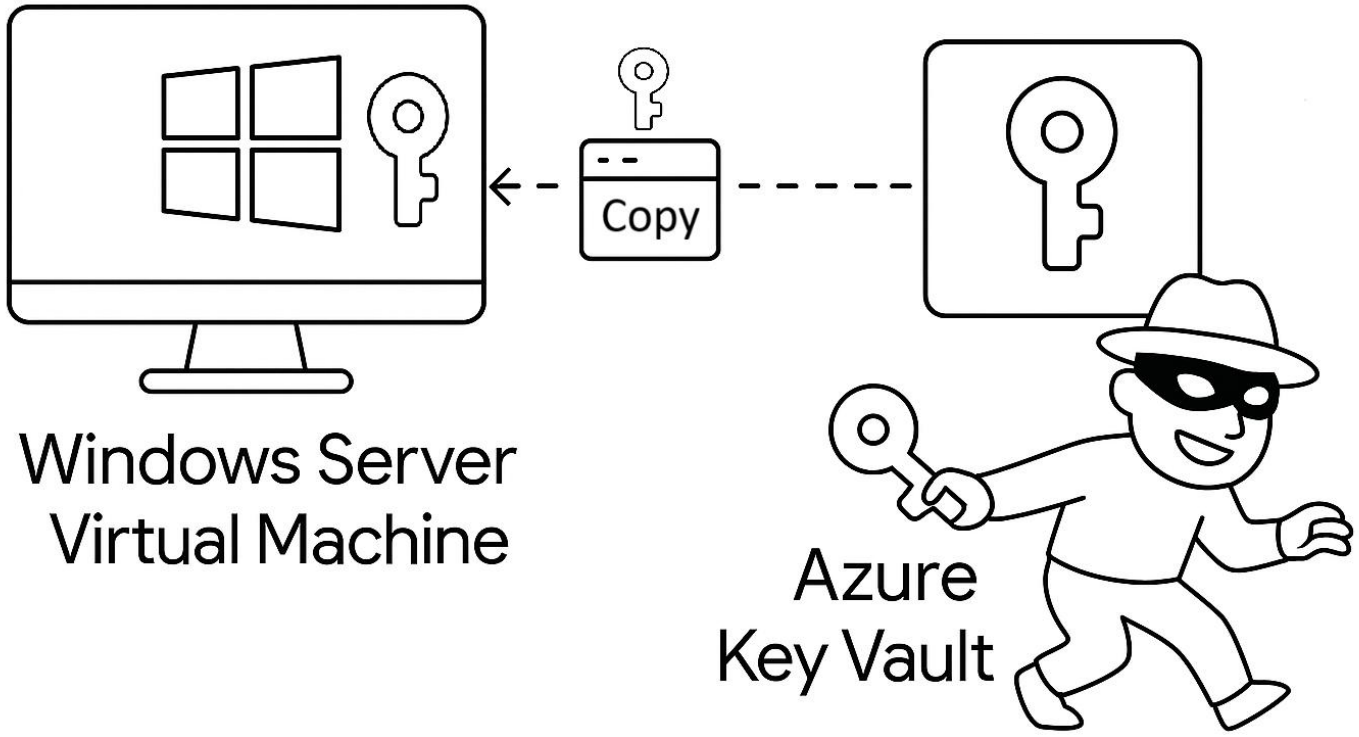


Azure Key Vault – Attack Scenario

Attacker can retrieve keys

Attacker retrieves (copies) certificates and keys

No easy way to stop without making keys non exportable



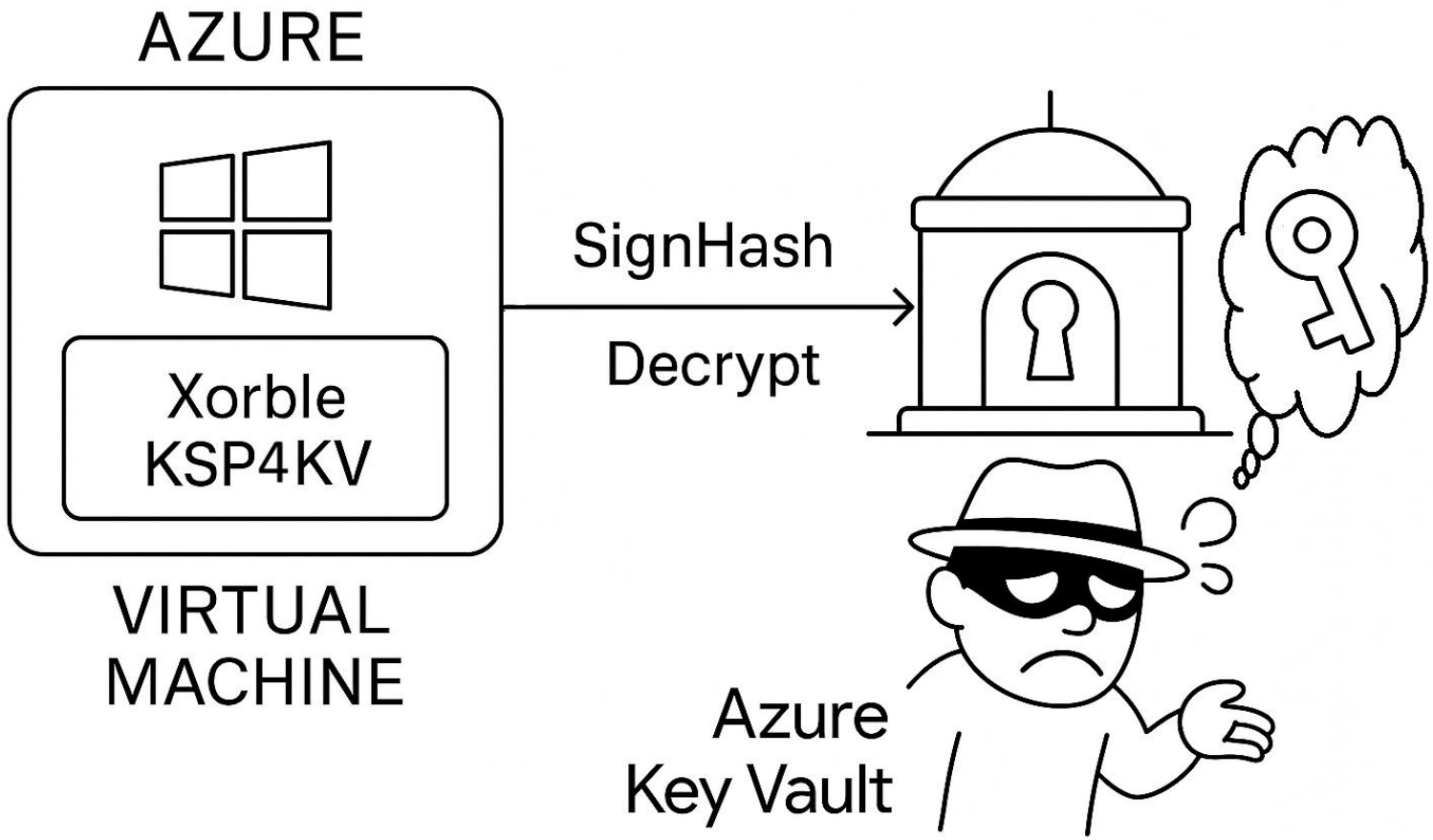
Xorble Key Storage Provider for Key Vault

Keys Not Exportable - FIPS 140-2 Level 2 HSM Protected

Xorble Key Storage Provider for Key Vault

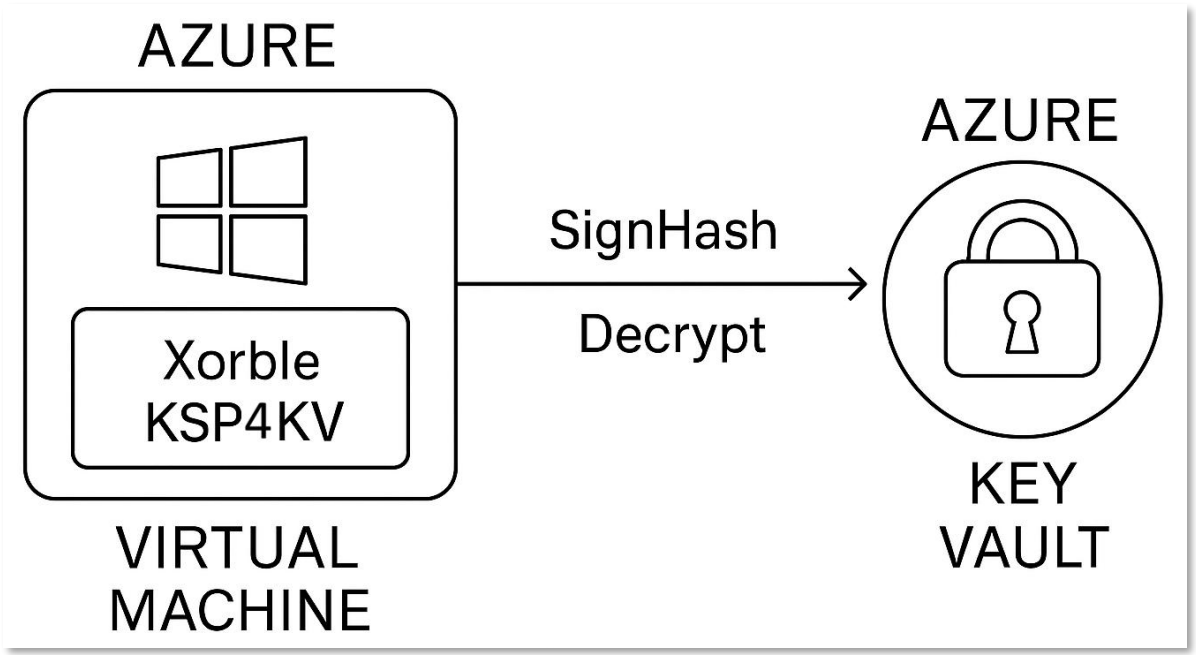
Keys Not Exportable

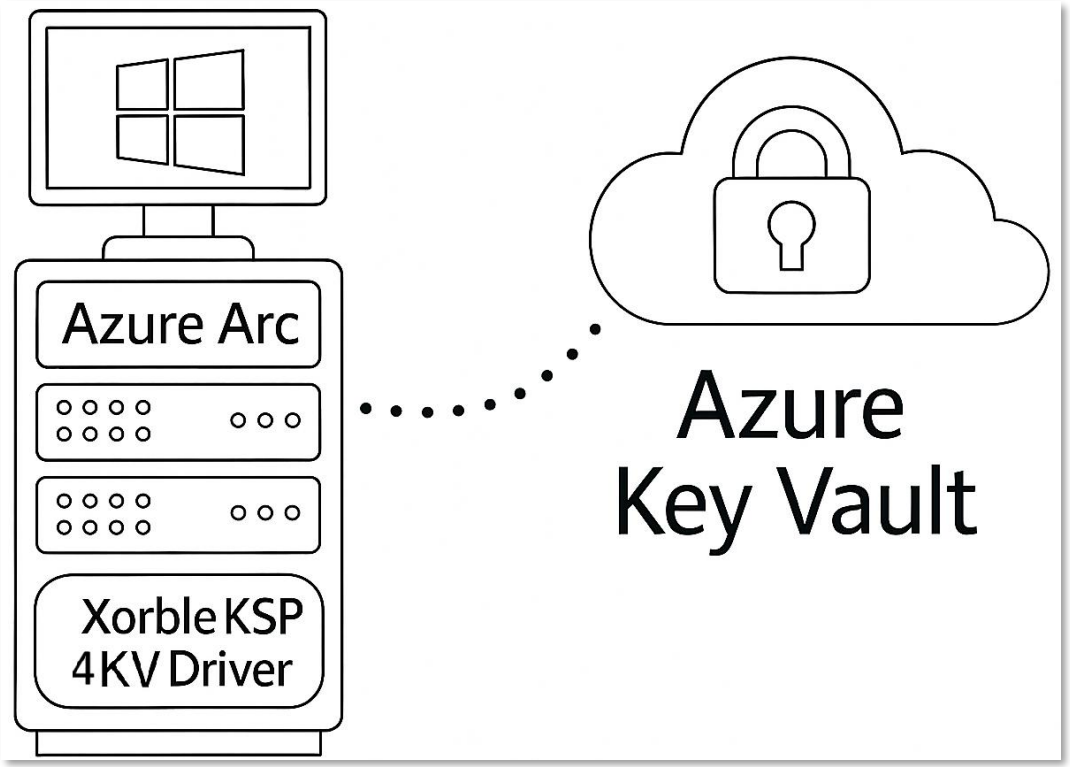
Attacker cannot steal keys



Xorble Key Storage Provider for Key Vault

- Supports
  - Azure Windows Server Virtual Machines
  - Azure Arc Windows Server Machines





Xorble Key Storage Provider for Key Vault

Xorble

- RSA and ECC Support
  - RSA 2048, 3072, 4096 bit signing and encryption keys/certificates
  - ECC 256, 384 and 521 bit signing keys/certificates
- Performance
  - Key Vault limits performance allowed per 10 seconds:

Key type	HSM key CREATE key	HSM key All other transactions	Software key CREATE key	Software key All other transactions
RSA 2,048-bit	10	2,000	20	4,000
RSA 3,072-bit	10	500	20	1,000
RSA 4,096-bit	10	250	20	500
ECC P-256	10	2,000	20	4,000
ECC P-384	10	2,000	20	4,000
ECC P-521	10	2,000	20	4,000

https://docs.azure.cn/en-us/key-vault/general/service-limits

Xorble Key Storage Provider for Key Vault

Xorble

Typical Use Cases

- Active Directory Certificate Services
  - Certification Authority role
  - Certification Authority Web Enrollment TLS/SSL certificates
  - Certification Authority Web Service and Policy Web Services TLS/SSL certificates
  - NDES/SCEP server roles
  - Online Responder (OCSP)
- Web Servers TLS/SSL
  - Protect all web traffic using certificates
- Other TLS application uses
- IPsec Server Certificates
  - IPsec can provide strong tunnel and transport authentication and encryption of traffic
- Domain Controller Certificates

Key Vault Comparison

Xorble

The most cost-effective way to provide a FIPS-backed HSM service with true native Windows KSP integration for Azure VMs is Xorble KSP for Azure Key Vault.

Option	Security Model	Windows Integration (KSP)	FIPS Level	Tenancy	Pricing Model	Monthly Cost (USD)
Key Vault Standard	Copy of keys	Yes (Software)	None	Multi	Per key	$0–$2
Key Vault Premium	Shared HSM	No (REST API)	FIPS 140-2 L2	Multi	Per key+ops	$10–$120
KV Premium + Xorble KSP4KV	Shared HSM via KSP	Yes	FIPS 140-2 L2	Multi	KV + compute	$50–$200
Managed HSM	Dedicated cluster	No	FIPS 140-2 L3	Single	Hourly	~$3300
Azure Cloud HSM	Cluster	PKCS#11	FIPS 140-2 L3	Single	Hourly	~$3300
Dedicated HSM	Appliance	Yes	FIPS 140-2 L3	Single	Hourly	~$3400

Xorble Key Storage Provider for Key Vault

Xorble

Cost Model – Two roles:

- PKI Servers - Typical PKI Server with 4 vCPU cores and 16GB of RAM, cost is about $175/month
- Non-PKI Servers - Typical Server with 4 vCPU cores and 16GB of RAM server cost is approximately $35/month

Costs are aimed low enough to not be prohibitive for use with every server

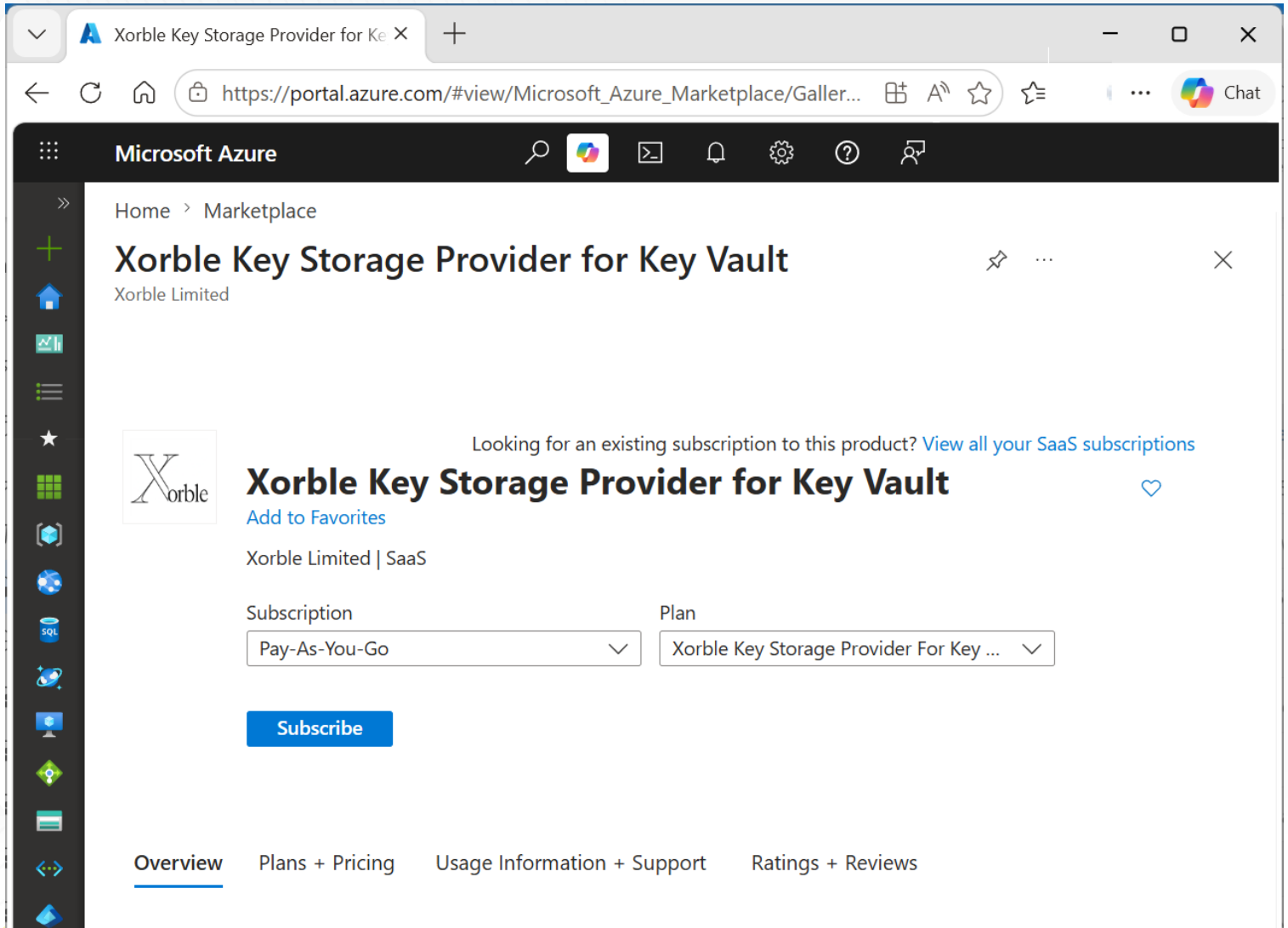
Item	$/hour	$/day	$/month
PKI Virtual Core Cost	0.05019	1.20456	36.6387
PKI RAM Cost (per GB)	0.00240	0.0576	1.752
(Non-PKI) Virtual Core Cost	0.01004	0.24096	7.3292
(Non-PKI) RAM Cost (per GB)	0.00048	0.01152	0.3504

Integration with Azure Marketplace

Azure Marketplace provides a straightforward experience for customers to purchase Xorble KSP4KV

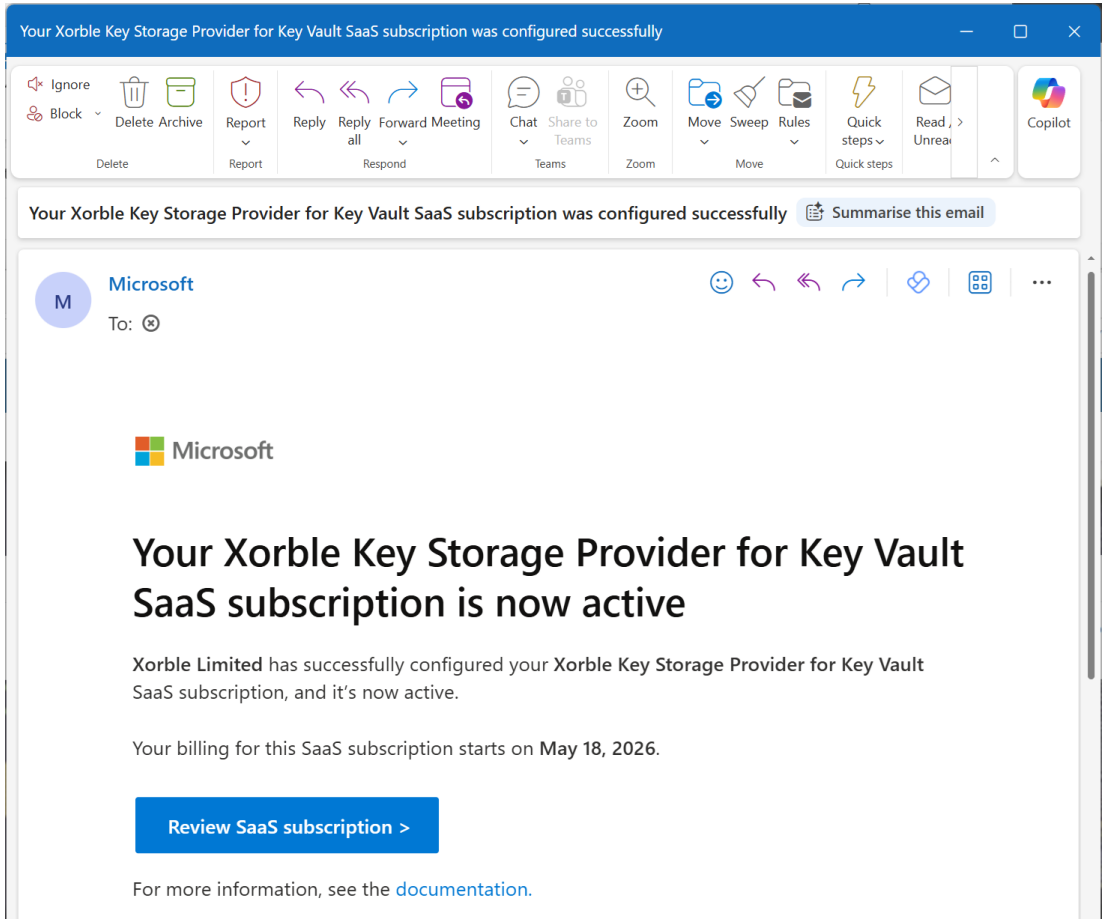
Integration with Azure Marketplace

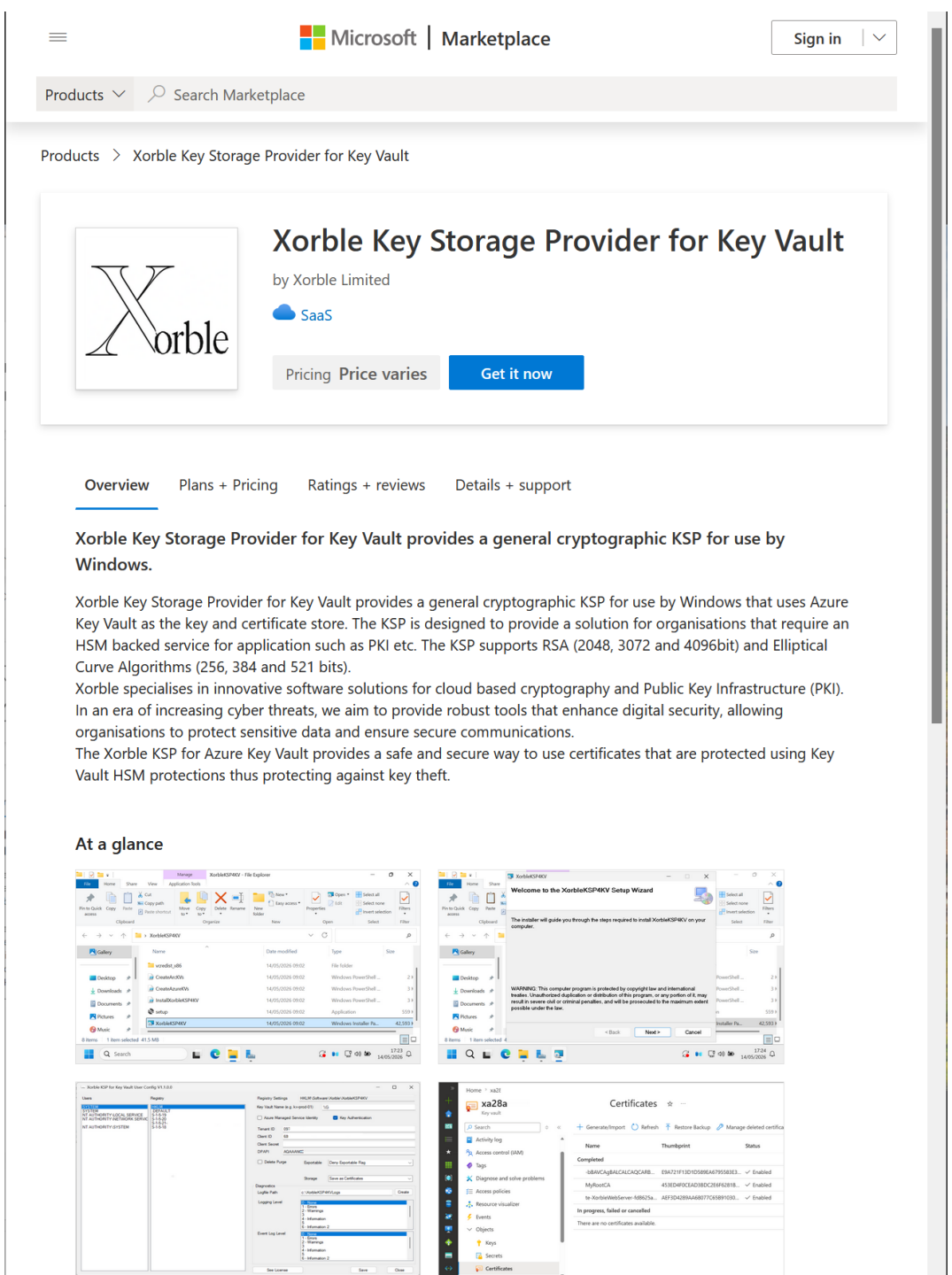
Eases deployment and billing and provides a unified interface



Getting Started and Deployment

Go to the Azure Marketplace to deploy: https://marketplace.microsoft.com/en-us/product/xorble.xorblekeystorageproviderforkeyvault





KSP Deployment - Designed to be automated

Xorble

Install designed to be automated end to end
Download the KSP MSI from:

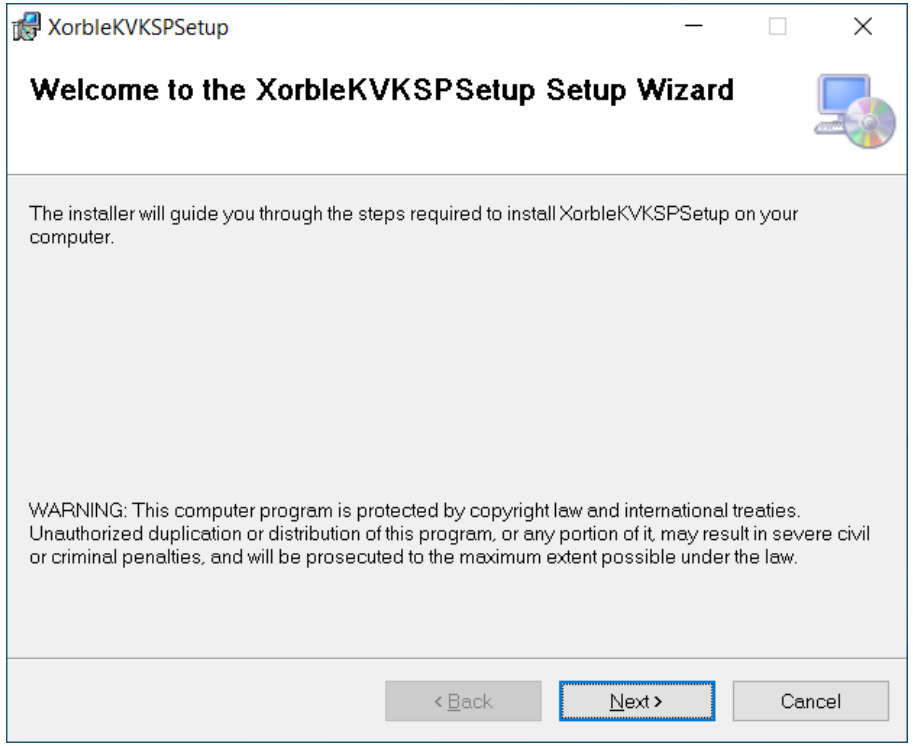
- https://xorble.com/download/
- Install can be automated via PowerShell/Azure Run Books with sample script.

Key Vault Name by default is derived from managed Identity

- Makes automation of the build easier
- Sample PowerShell scripts for Azure and Arc setup

Requires Access to various URLs:

- https://<vaultname>.vault.azure.net
- https://login.windows.net
- https://xorblekvksplicensingapp.azurewebsites.net



Conclusions

Xorble

- Every Server, HSM-enabled by design
  - Costs are aimed low enough to not be prohibitive to enable for **every** server
  - Microsoft managed FIPS 140-2 Level 2 HSM for every server
- Typical Use cases
  - Microsoft based PKI (ADCS), Web Servers TLS/SSL, Other TLS applications, IPsec, Domain Controller Certificates
- Supports Windows Server Azure Virtual Machines and Arc Machines
- KSP Deployment - Designed to be automated
- Integration with Azure Marketplace
  - Azure Marketplace provides a straightforward experience for customers to purchase Xorble KSP4KV
- The most cost-effective way to provide a FIPS-backed HSM service with true native Windows KSP integration for Azure VMs is Xorble KSP for Azure Key Vault

Xorble

Xorble

Every Server, HSM-enabled by design

Xorble Key Storage Provider for Azure Key Vault

The most cost-effective way to provide a FIPS-backed HSM service with true native Windows KSP integration for Azure VMs is Xorble KSP for Azure Key Vault