cpl.thalesgroup.com

Building a future we can all trust

Microsoft Azure Payment HSM delivered using Thales payShield HSM technology

Accelerating payment ecosystem digital transformation

The growing trend for running payment workloads in the cloud

Momentum is building as financial institutions move some or all of their payment applications to the cloud. This entails a migration from the legacy on-premises (on-prem) applications and HSMs to a cloud-based infrastructure that is not generally under their direct control. Often it means a subscription service rather than perpetual ownership of physical equipment and software. Corporate initiatives for efficiency and a scaled-down physical presence are the drivers for this. Conversely, with cloud-native organizations, the adoption of cloud-first without any on-prem presence is their fundamental business model. Whatever the reason, end users of a cloud-based payment infrastructure expect reduced IT complexity, streamlined security compliance and flexibility to scale their solution seamlessly as their business grows.

Potential challenges

Cloud ultimately offers significant benefits, but challenges when migrating a legacy on-prem payment application (involving payment HSMs) to the cloud must be addressed. Some of these are:

- Shared responsibility and trust – what potential loss of control in some areas is acceptable?
- Latency – how can an efficient, high performance link between the application and HSM be achieved?
- Performing everything remotely – what existing processes and procedures may need to be adapted?
- Security certifications and audit compliance – how will current stringent requirements be fulfilled?

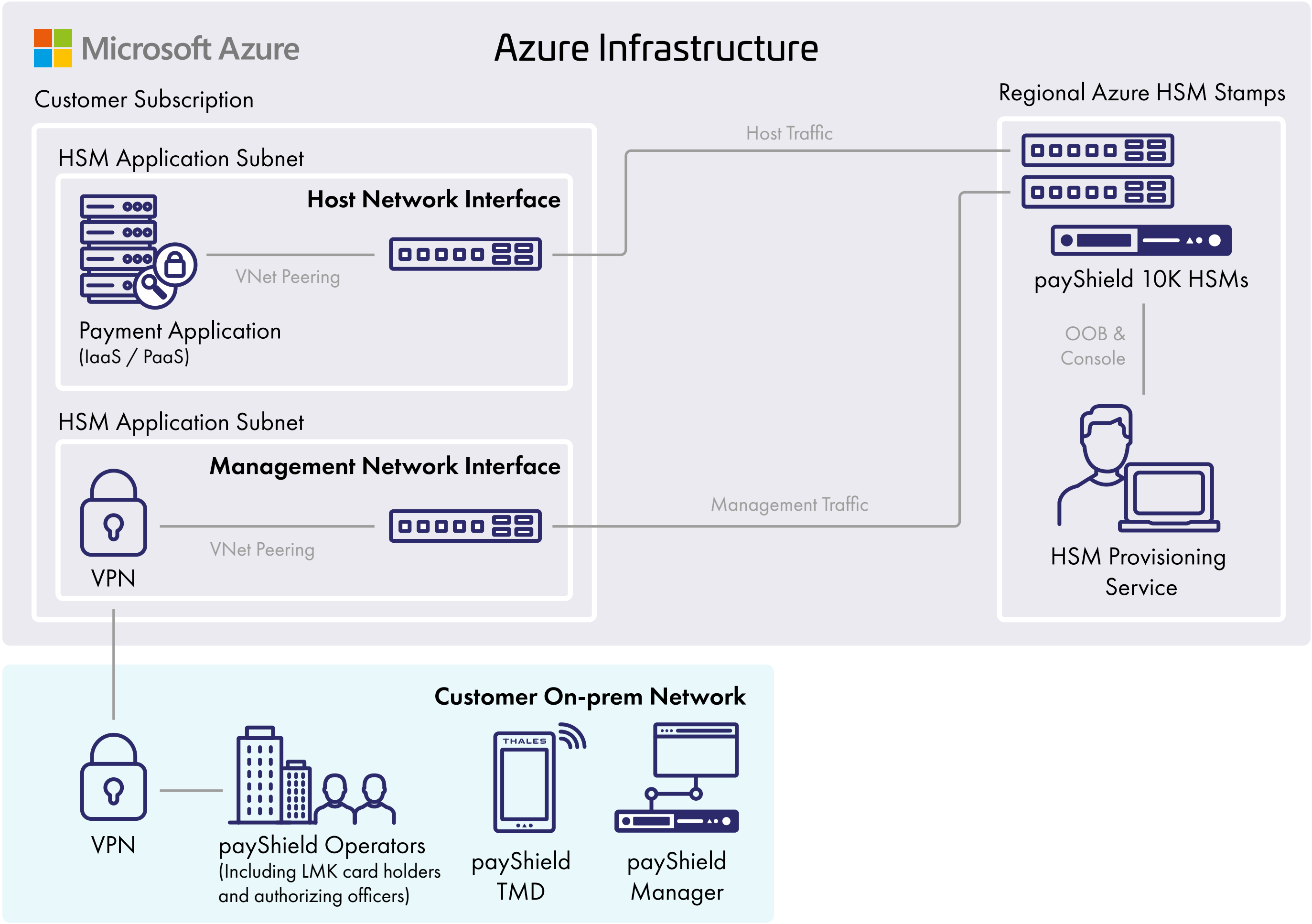
Reassuringly, the Microsoft Azure cloud solution uses Thales HSM technology to address these challenges and deliver a compelling value proposition to users of the service. Let us explore how.

Introducing the Microsoft Azure Payment HSM Service

The Microsoft Azure Payment HSM Service is a 'Bare Metal' service delivered using Thales payShield 10K payment HSMs to provide cryptographic key operations for real-time, critical payment transactions in Azure. The solution is in public preview and allows service providers and financial institutions to accelerate the digital transformation of their cloud-based payment systems confidently. It meets the most stringent security, audit compliance, low latency and high-performance requirements by the Payment Card Industry (PCI). Users of the service utilize Thales payShield Manager for secure remote access to the HSMs as part of their OPEX-based subscription. Multiple subscription options are available to satisfy a broad range of performance and multiple application requirements that can be upgraded quickly in line with end user business growth.

Glossary

3DS	3D Secure
ATM	Automated Teller Machine
DSS	Data Security Standard
EMV	Europay Mastercard Visa
FIPS	Federal Information Processing Standards
HCE	Host Card Emulation
HSM	Hardware Security Module
IaaS	Infrastructure as a Service
LMK	Local Master Key
mPOS	Mobile Point of Sale
OOB	Out of Band Management
P2PE	Point to Point Encryption
PaaS	Platform as a Service
PCI	Payment Card Industry
PIN	Personal Identification Number
POS	Point of Sale
SPOC	Software-based PIN Entry on Commercial off the Shelf (COTS) Solutions
TMD	payShield Trusted Management Device
VNet	Azure Virtual Network
VPN	Virtual Private Network



Enhanced security and compliance

End users of the service can leverage Microsoft security and compliance investments to increase their security posture. Microsoft maintains PCI DSS and PCI 3DS compliant Azure data centers, including those which house Azure Payment HSM solutions. The Azure Payment HSM solution can be deployed as part of a validated PCI P2PE / PCI PIN component or solution, helping to simplify ongoing security audit compliance. Thales payShield 10K HSMs deployed in the security infrastructure are certified to FIPS 140-2 Level 3 and PCI HSM v3.

Customer-managed HSM in Azure

The Azure Payment HSM is a part of a subscription service that offers single-tenant HSMs for the service customer to have complete administrative control and exclusive access to the HSM. The customer could be a payment service provider acting on behalf of multiple financial institutions or a financial institution that wishes to directly access the Azure Payment HSM service. Once the HSM is allocated to a customer, Microsoft has no access to customer data. Likewise, when the HSM is no longer required, customer data is zeroized and erased as soon as the HSM is released to ensure complete privacy and security is maintained. The customer is responsible for ensuring sufficient HSM subscriptions are active to meet their requirements for backup, disaster recovery and resilience to achieve the same performance available on their on-prem HSMs.

Accelerate digital transformation and innovation in cloud

For existing Thales payShield customers wishing to add a cloud option, the Azure Payment HSM solution offers native access to a payment HSM in Azure for 'lift and shift' while still experiencing the low latency they are accustomed to via their on-prem payShield HSMs. The solution also offers high performance transactions for mission critical payment applications. Consequently, customers can continue their digital transformation strategy by leveraging technology innovation in the cloud. Existing Thales payShield customers can utilize their existing remote management solutions (payShield Manager and payShield TMD together with associated smart card readers and smart cards as appropriate) to work with the Azure Payment HSM service. Customers new to payShield can source the hardware accessories from Thales or one of its partners before deploying their HSM as part of the subscription service.

Typical use cases

With benefits including low latency and the ability to quickly add more HSM capacity as required, the cloud service is a perfect fit for a broad range of use cases which include:

Payment processing

- Card & mobile payment authorization
- PIN & EMV cryptogram validation
- 3D-Secure authentication

Payment credential issuing

- Cards
- Mobile secure elements
- Wearables
- Connected devices
- Host card emulation (HCE) applications

Securing keys & authentication data

- POS, mPOS & SPOC key management
- Remote key loading (for ATM & POS/mPOS devices)
- PIN generation & printing
- PIN routing

Sensitive data protection

- Point to point encryption (P2PE)
- Security tokenization (for PCI DSS compliance)
- EMV payment tokenisation

Suitable for both existing and new payment HSM users

The solution provides clear benefits for both payment HSM users with a legacy on-prem HSM footprint and those new payment ecosystem entrants with no legacy infrastructure to support and who may choose a cloud-native approach from the outset.

Benefits for existing on-prem HSM users

- Requires no modifications to payment applications or HSM software to migrate existing applications to the Azure solution
- Enables more flexibility and efficiency in HSM utilization
- Simplifies HSM sharing between multiple teams, geographically dispersed
- Reduces physical HSM footprint in their legacy data centers
- Improves cash flow for new projects

Benefits for new payment participants

- Avoids introduction of on-prem HSM infrastructure
- Lowers upfront investment via the OPEX subscription model
- Offers access to latest certified hardware and software on-demand

About payShield 10K

As markets and digital payment security standards continue to advance, a secure payment infrastructure is crucial to global business success. Organizations face many challenges in protecting the rapidly growing volume of digital payments – from transaction processing and country-specific mandates to card/device issuance and direct-to-mobile provisioning. Customers can rely on payShield 10K payment HSMs to deliver the protection, performance, and operational efficiency needed to secure digital payments.

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.

Getting Started

To get started with Azure Payment HSM (preview), contact your Microsoft sales representative and request access via email. Upon approval, you'll be provided with onboarding instructions.

> cpl.thalesgroup.com <

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