cpl.thalesgroup.com

THALES

Building a future we can all trust

payShield Cloud HSM

Launch new payment solutions faster

Payment workloads are increasingly moving to the cloud

For many years most payment applications and their associated HSMs were located in private data centers operated by banks or trusted service providers on their behalf - the use of public cloud infrastructures for highly sensitive payment workloads was often not a viable option. As organizations of all sizes strive to become more efficient, there is a drive to reduce the physical data center footprint leading to the cloud becoming an alternative to perpetual ownership of hardware and software.

Banks that have deployed on-prem payment HSMs for over 30 years now have another option to pursue. Momentum is building as financial institutions are moving some or all of their applications to the cloud now that issues relating to security and latency have been addressed. Leading cloud-based solutions involving Thales payShield HSMs available from both Thales and a variety of its technology partners are in active use today. Cloud-native FinTechs are deploying such cloud-based subscription services from the start – their fundamental business model does not require any on-prem presence. Free to choose their cloud configuration, end users expect reduced IT complexity, streamlined security compliance and flexibility to scale their payment solution seamlessly in line with their business growth. This brochure explains how the payShield Cloud HSM service from Thales is at the forefront of security for payment workloads operating in a multi-cloud world.

Glossary

ATM	Automated Teller Machine
cps	Calls per Second
DSS	Data Security Standard
EMV	Europay Mastercard Visa
FIPS	Federal Information Processing Standards
HCE	Host Card Emulation
HSM	Hardware Security Module
KEK	Key Encrypting Key
LMK	Local Master Key
mPOS	Mobile Point of Sale
P2PE	Point to Point Encryption
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
ZMK	Zone Master Key

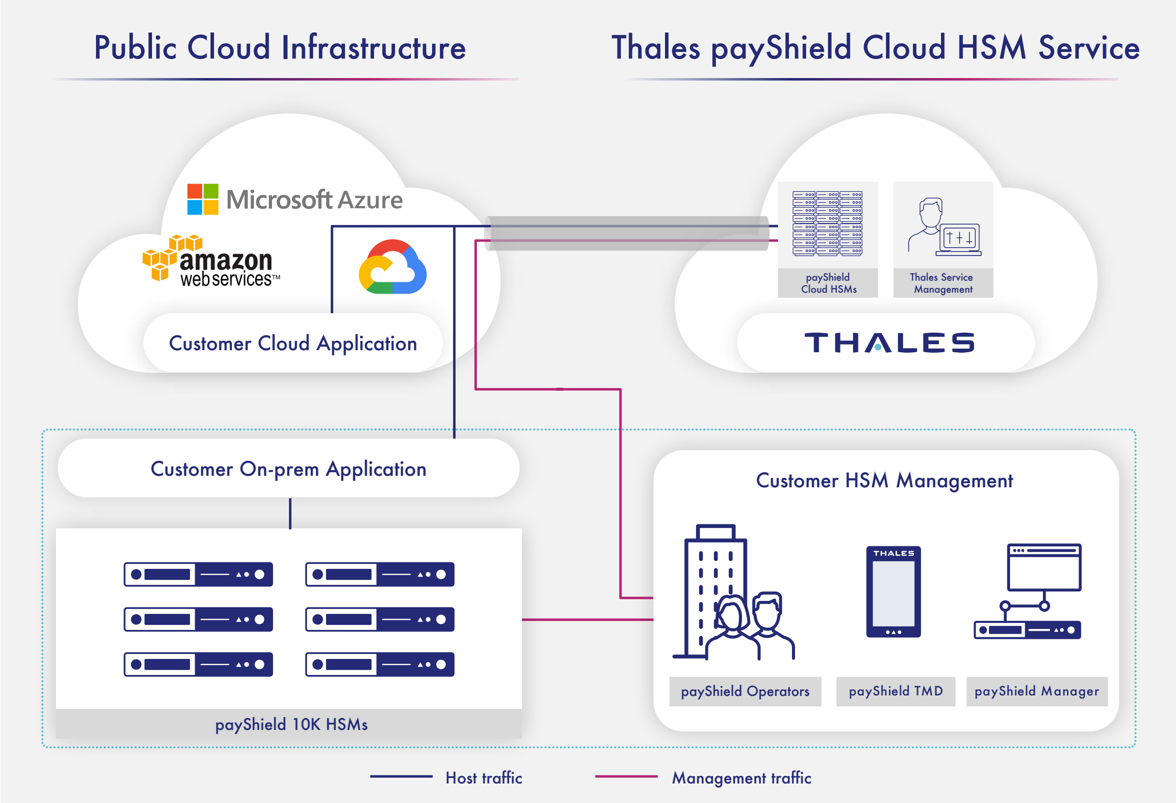
An introduction to payShield Cloud HSM

payShield Cloud HSM is a 'bare metal' hosted HSM service from Thales delivered using payShield 10K HSMs, providing the secure real-time, cryptographic processing capabilities required by payment workloads running in any of the major public clouds. The service addresses the needs of both existing users of payment HSMs and new payment entrants looking to leverage hardware-based security for the first time. Thales is offering its customers a choice of deployment model, namely on-prem, cloud or hybrid (when a mixture of on-prem and cloud HSMs are utilized). Whatever model is chosen, consistent HSM functionality is available with the highest levels of security compliance.

When the cloud HSM variant is deployed, the separation of roles between the end user of the service and the service provider (in this case Thales) differs from the on-prem configuration (where Thales is not directly involved). With the cloud HSM, the physical infrastructure is managed by Thales and the HSMs are housed in data centers under Thales control with high speed links to connect to public clouds running the application workloads.

Key benefits

- **Flexibility** – simplifies sharing of production HSMs across multiple applications, staff and regions
- **Future proof** – offers access to the latest certified payShield hardware and software on demand
- **Scalability** – enables extra HSMs to be added quickly for resilience, backup or capacity
- **Cloud agnostic** – works seamlessly with fast connections to all major public cloud providers (Microsoft Azure, Amazon Web Services and Google Cloud)
- **Cash flow** – avoids up-front investment by offering a flexible, monthly subscription service to improve cash flow



Thales allocates each single-tenant HSM to the customer as part of the subscription service. Each service customer therefore has complete administrative control and exclusive access to the HSMs assigned to them – importantly they can configure each HSM to support multiple distinct applications or use cases (through the multiple LMK capability) in the same way they perform secure segregation today with Thales on-prem payShield 10K HSMs. Once the HSM is allocated to a customer, Thales has no access to any customer data, cryptographic keys or audit logs. Likewise, when the customer decides that the HSM is no longer required, all data and keys belonging to the customer is securely erased to ensure complete security and privacy. The HSM is then free to be assigned to another subscriber as required.

payShield Cloud HSM meets the stringent security requirements of the Payment Card Industry (PCI) and the individual payment brands and networks. It offers a high performance, low latency service that enables you to comply with the same payment security audits that apply to any on-prem HSM infrastructures you may be operating. In a hybrid scenario you can use the same management and monitoring tools (payShield Manager, payShield Monitor and payShield TMD) and associated smart cards and readers for both the on-prem and cloud HSMs.

Typical use cases

The payShield Cloud HSM service uses the same underlying security technology as the on-prem HSMs (and therefore offers identical cryptographic functionality) enabling a broad range of proven use cases to be covered including:

- **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

Service specifications at a glance

Public cloud support	The Thales-controlled data centers have fast connectivity to Microsoft Azure, Google Cloud Platform and Amazon Web Services
Security certifications	The data centers used to host the HSMs are certified to PCI DSS and PCI PIN with the individual HSMs certified to PCI HSM v3 and FIPS 140-2 Level 3
Thales responsibility	Thales controls the following aspects of the service • Managing the physical HSM infrastructure (including installation, cabling and basic network configuration) • Allocation of HSMs to eligible customers of the service • Obtaining ongoing FIPS, PCI HSM and other regional certifications for the HSMs offered as part of a subscription package • Enhancing the cryptographic functionality offered by the HSMs in line with payment market application and security requirements • Providing 24x7 support for matters relating to HSM functionality or operation
Service user responsibility	The service user (i.e. the Thales subscription customer) is responsible for all areas of management and operation of the HSMs under their subscription agreements, namely • LMK management • ZMK and KEK management • HSM configuration • Loading of base/custom software and associated licenses • Audit trail management • Load balancing and redundancy • HSM monitoring
Message protection mechanism	All messages between the user application and the payShield Cloud HSMs are encrypted using TLS communications
Subscription options	Different subscription options are available to suit different throughput requirements • Starter – 25 cps • Silver – 60 cps • Gold – 250 cps • Platinum – 2500 cps All options can utilize standard base software or custom software
HSM options	The service currently supports the standard payShield 10K HSM which is identical to the on-prem device
Management tools	The same payShield Manager, payShield Monitor and payShield TMD tools used for on-prem deployments are used with the service to provide secure remote management and monitoring
Customization options	The software customization service fulfilled by the Thales Professional Services team is available for use with any HSM used in a payShield Cloud subscription

Please refer to the payShield 10K datasheet for further details of the technical specification of the HSMs used in the payShield Cloud service.

A low risk option for existing payShield users

Existing customers of on-prem Thales payShield HSMs will experience many benefits, including:

- **Backwards compatibility** – no need to modify payment applications, facilitating fast-track introduction, especially for new projects
- **Flexibility and efficiency** – simplifies deployment, sharing and management of HSM estates across multiple diverse teams and locations
- **Audit compliance** – eliminates the need to plan and fund hardware replacement to retain audit compliance

Simple to deploy for FinTechs

There are multiple benefits for new payment entrants without a legacy on-prem infrastructure to support, including:

- **Cloud-native environment** –secure remote management capabilities eliminate any physical handling and management activities inside remote data centers
- **Low upfront investment** – flexible subscription package replaces a CAPEX ownership model which improves cash flow when developing or launching new solutions
- **Proven and trusted technology** – provides peace of mind that the underlying technology and host API are being used by thousands of Thales customers across the world

How to subscribe

Please contact your local Thales Account Manager or Authorized Reseller for more information on how you can subscribe to this service.

A vast network of Thales channel partners ready to assist

Thales works closely with its global network of trusted channel partners to help ensure you get the best possible payment HSM solution that can be supported locally. You should be able to find a suitable partner in the country where you wish to deploy that can fulfil your precise requirements. Whether you are looking to add additional on-prem payShield HSMs to your existing HSM estates, exploring the use of cloud payment HSMs for the first time or seeking to migrate your on-prem infrastructure to a complete cloud solution, Thales and its partners will advise a suitable approach and provide long term support.

About payShield 10K

payShield 10K, the fifth generation of payment HSMs from Thales, delivers a suite of payment security functionality proven in critical environments including transaction processing, sensitive data protection, payment credential issuing, mobile card acceptance and payment tokenization. payShield 10K can be used throughout the global payment ecosystem by issuers, service providers, acquirers, processors and payment networks and addresses the latest mandated security requirements and best practices for a wide range of organizations including EMVCo, PCI SSC, GlobalPlatform, Multos, ANSI and the various global and regional payment brands and networks.

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.

Building a future we can all trust

Contact us

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

> cpl.thalesgroup.com <