payShield Cloud HSM Technical Brief

De-risk your payment security infrastructure

Executive summary

Organizations increasingly look to trusted third parties to run mission critical infrastructures on their behalf to mitigate downtime risk

Thales takes away the pain of being responsible for your physical HSM estate. You benefit from significant operational savings in many ways including:

- No physical handling of HSMs
- Faster new HSM deployment
- Highly efficient fault diagnosis and remediation
- Fewer IT support calls
- Simplified audit compliance

All HSM interactions your team perform are via secure remote connections – you keep full control of your keys and data. You can operate a hybrid on-prem/cloud environment, leveraging all the management and monitoring tools, smart cards and readers you already possess for Thales payment HSMs.

Benefit from a more efficient way to maintain and expand your HSM estate – the Thales service will likely be better than you can achieve yourself with a similar investment. Eliminate the complex and costly process of physical HSM estate migration typically every 7 years – you are always up to date with the latest security technology.

payShield Cloud HSM is a 'bare-metal' hosted service. It is easy to get started quickly and update your HSM capacity over time as your business requirements change. You inherently **shift the risk to Thales** for keeping your HSMs fully operational without having to make any security compromises.

There is no need to disrupt any of your existing HSM estates or applications. Through full backwards compatibility, you can introduce payShield Cloud HSM for new solutions, extra capacity or as backup for existing applications – we have worked hard to make it **easy for you to operate a hybrid environment.**

Deploying payShield Cloud HSM will free up your team to perform tasks more core to your business – no longer will you need to recruit, train and retain staff purely for HSM installation and ongoing maintenance.

The remainder of this document helps you understand how 'shifting the risk' to Thales can help your organization be more efficient and agile while still retaining full control of your critical assets.

Contents

Service overview

THALES PAYSHIELD CLOUD HSM IS...

...An infrastructure as a service (IaaS) solution for payment HSMs, offering your organization a flexible and secure way to shift the risk to Thales for keeping your critical security capabilities operational, while you still maintain full control of all your cryptographic keys and sensitive data.

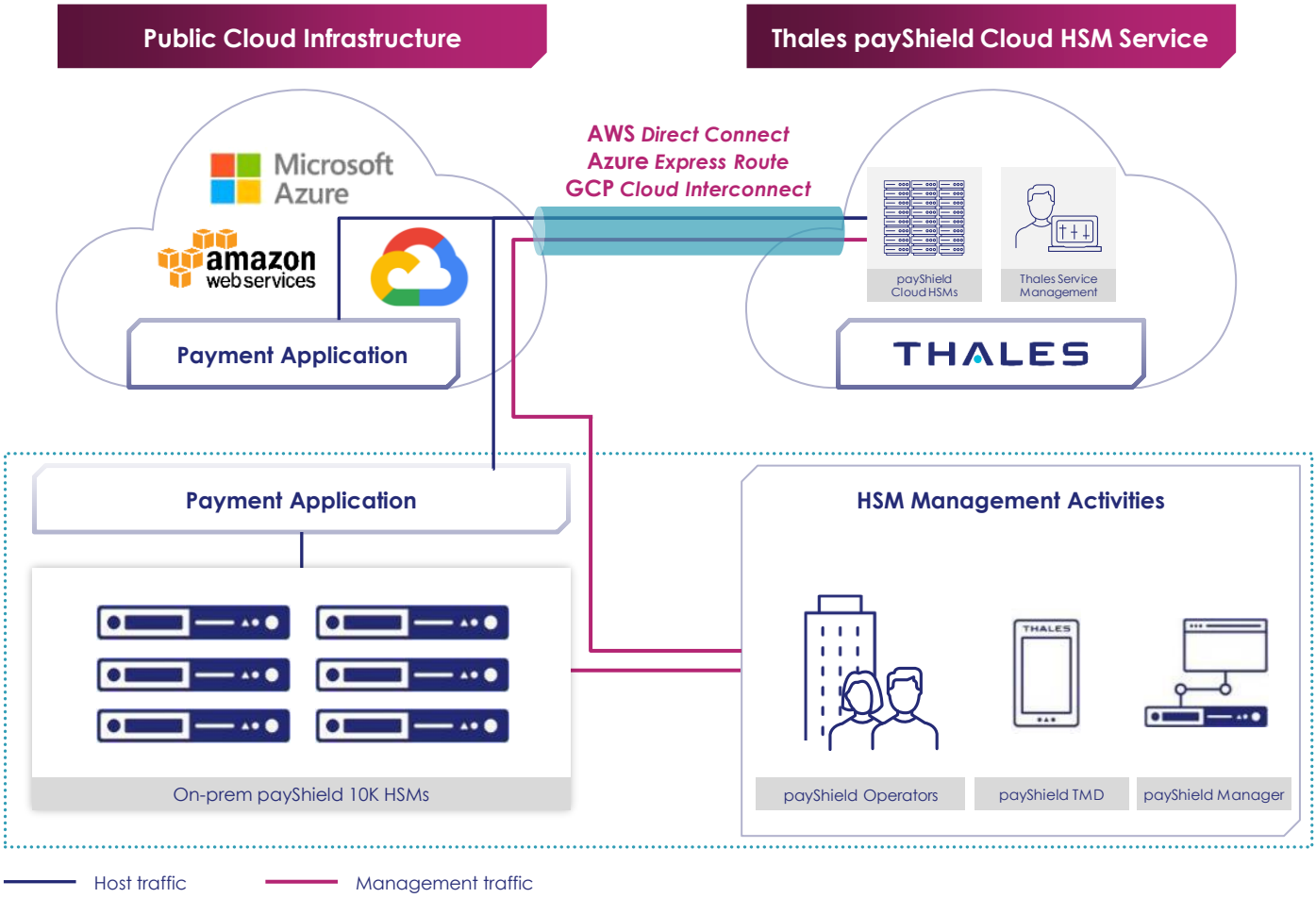
It delivers superior application service availability and lower cost disaster recovery capabilities compared to typical homegrown banking implementations

It provides high levels of future-proofing, eliminates the complex and costly physical HSM migration process and frees up your security team for other tasks core to your business

It facilitates a low-risk hybrid on-prem/cloud environment with no payment application changes, ensuring cloud migration occurs at your chosen pace while avoiding disruption to your existing operations

Through its scale and global reach, Thales can provide a flexible, scalable and highly-available payment HSM solution, almost certainly better than you can achieve today on your own at a similar price point. Let Thales operate a robust HSM infrastructure on your behalf to help support your business evolution and growth, while simplifying your operational logistics.

KEY ATTRIBUTES OF THE PAYSHIELD CLOUD HSM SERVICE



Thales hosts the HSMs in its **secure data centers**, observing chain of custody audit requirements

Payment applications can be **hosted on-prem** or in a **public cloud**

Access to HSMs via a **flexible subscription service – 60, 250** and **2500 cps performance options** available for production workloads

Applications connect to HSMs **via secure, high performance links**

You have **full control** of the HSMs by using **remote management**

HSM deployment options

When your organization requires hardware security modules **(HSMs) to comply with payment security audit requirements and/or payment network rules**, there are basically **two fundamental choices** available to you – procure HSMs and **take responsibility for everything yourself** or **use a service provider to operate an HSM estate** on your behalf. Until relatively recently most financial institutions took the former approach, resulting in a **proliferation of private data centers operated by the banks**, sometimes in conjunction with trusted third parties. 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.

All options supported by Thales

Thales offers 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.**

Growing demand for a cloud service

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 the hosting of Thales payShield HSMs** available from both **Thales** and a **variety of its technology partners** are in **active use today.**

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.**

Specific benefits of payShield Cloud HSM

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

Typical risks that could disrupt your business

Operating and maintaining your own HSM estate can prove to be very challenging in many cases. It is part of your mission-critical infrastructure with your business at risk if you have any significant period when the HSMs are not available. Some of the factors that you control and for which you accept the burden of responsibility when you operate your own on-prem HSM estate include:

System downtime

The system is much more than the HSMs – it includes **all the networking equipment** and the **connectivity** between your **applications and the HSM estate.** A **robust solution** with **high levels** of redundancy is required to **ensure that a problem with any component does not lead to a prolonged period of downtime, unacceptable to your business.** In the vast majority of cases this involves **investment in multiple data centers** which are geographically separated.

What service downtime has impacted your business in the past 3 years for example?

Security vulnerabilities

On a regular basis all IT-based systems require **firmware or software updates** to **keep pace with security vulnerabilities** that are discovered normally by the product vendors or the security community. In the payments world, it is simply not an option to continue operating a **critical environment with out of date software – you will probably fail your next security audit if you do.** Thales provides **timely updates** to its HSM software to **fix any security issues uncovered** – this is only a small part of the challenge with the **switches, routers and VPNs requiring more regular updates.**

How much effort and cost do you spend in keeping on top of security vulnerabilities and patching?

Insufficient HSM capacity

When you operate your own HSM estate, you have basically **two options** when trying to anticipate future HSM capacity needs – you can **buy more HSMs upfront** than you need at present and keep them in **secure storage** or you can **place an order for new HSMs** when you can see your current capacity is **close to the limit.** In both cases there are potential **delays** and **logistical challenges** in **installing** new HSMs and **configuring** them for production use – typically the time involved is **weeks** rather than days or hours.

How long does it typically take to add a new HSM to your existing estate?

Faulty HSM

When an HSM develops a fault, for whatever reason, it inevitably needs to be **taken out of service** for further investigation and analysis. In the worst case where a hardware reset or software update fails to recover the device to a working state, a **return to the vendor is required** as part of a warranty/service replacement process. All this takes **time** and you will **not be back** at full primary and disaster recovery capacity until the replacement HSM is installed, configured and validated prior to use.

What is your average turnaround time and cost for replacing a faulty HSM?

Skilled staff availability

Payment HSMs are specialist pieces of equipment rather than mainstream computer technology – they need **proprietary security processes and procedures** for correct operation. The staff required to undertake such tasks need to be **trained** and **available** to support your critical infrastructure. Some highly secure tasks are performed very infrequently but the onus is always on you to ensure that the specific knowledge is available at all times, made more difficult when existing trained staff move on to other positions inside or outside your organization.

What challenges do you face in recruiting and maintaining a skilled security team?

Situations ideal for the cloud service

If you have an existing on-prem HSM estate, there are certain situations where it can be advantageous for you to consider implementing the payShield Cloud HSM service as an addition to what you have rather than a direct replacement.

New projects

A totally new project, possibly linked to a new application, will often have a **new project team**, additional HSM requirements and a proof-of-concept (POC) stage. Getting initial approval for a large infrastructure budget which includes data center equipment and HSMs can be **challenging.** The **payShield Cloud HSM service** offers an **easy, low cost approach** to getting started with your project and **does not impact** any of your **established on-prem HSM estates**

Avoids disruption to any existing HSM operations

Extra capacity

When you need additional HSM capacity the cloud service offers a **much faster route** to getting it up and running – you avoid all the **physical handling** and **scheduling** of staff to install, configure and test since Thales takes care of all of this on your behalf. If you are already an existing subscriber to our service, the new HSM will be available the **same day** in most cases. Even if this is your first experience of the service, the time to go live will be **much less** than you can achieve as part of your own on-prem HSM estate. Importantly, on-prem and cloud HSMs can be part of the same HSM estate, ensuring your existing on-prem applications **can make use of cloud** HSMs in a **seamless manner** to support additional cryptographic processing

Delivers seamless operation as part of a hybrid environment

Disaster recovery

Today in servicing the **high availability** and **disaster recovery (DR)** demands of your mission critical payment security infrastructure, you likely will have made some compromises – for example primary locations where you operate without their own dedicated data centers or fewer HSMs than necessary to deliver higher levels of resilience due to cost constraints. Our cloud service offers you to the ability to **leverage our data centers** in countries where **cost would be prohibitive** for you to establish your own private data center. As an added benefit, Thales is launching two data centers in each location where it is rolling out the service so that you can have a **close-proximity DR implementation** to support your primary location. You may also find over time that the cloud service enables you to reduce the number of private data centers you currently operate yourself.

Enables rationalization of your existing data center facilities

Risk management

The value that Thales brings by taking care of the **installation, cabling, network configuration** amongst other specialist or proprietary tasks is **significant** – these are the things that can take **a lot of time** and require **detailed procedures** if you are not doing them very often. By having many more data centers, spare HSM capacity and skilled staff available 24x7 inevitably means that the Thales cloud service is **more robust** and has **higher uptime** that what you could do yourself with a similar investment. As an added benefit your **valuable security team** get freed up to carry out other tasks more core to your business.

Shifts the risk to Thales for keeping your HSMs fully operational

Application consolidation

Mergers and acquisitions (M&As) have been commonplace throughout the payments industry over the past 10 years or more. Often financial institutions end up with a set of applications operated by geographically diverse teams, each with their own sets of HSMs with the data centers in different locations. **Optimization and application consolidation** is normally a **primary objective** in such circumstances especially when a cloud-based alternative is available. The Thales payment HSM family has the **broadest range of proven integration** with **all the leading payment applications** from the leading vendors **globally.** Our cloud HSM service will likely offer **off-the-shelf compatibility** with all the different applications you find you now own as a result of M&A activity – any proprietary requirements can be addressed quickly by our **customization service** which has served **thousands of Thales customers over many years.**

Offers proven integration with all major payment applications

Operational Savings

When using our payShield Cloud HSM service, you can expect significant operational savings compared to running your own on-prem HSM estate.

Freeing up staff

Elimination of HSM installation and maintenance tasks – no need for any of your team to visit a data center, all HSM access is carried out using **secure remote connections**

Less time and staff required to deploy an HSM (less order administration, policies and procedures, scheduling of activities, supporting DR sites, networking, testing, monitoring and diagnostics)

Reduction in IT help desk calls

Future-proofing

Access to **more data centers globally** for application deployments, **capacity expansion and disaster recovery**

Latest payShield hardware and software always available on-demand for you to access via subscription – **simpler upgrade** to new hardware with **software updates under your control**

Elimination of complex, lengthy and costly periodic physical HSM migration process when you need to adopt **newer certified technology** to pass security audits

Data center infrastructure investment and ongoing maintenance

No physical data center equipment needs to be purchased or owned by you, **eliminating large upfront costs** – you have access to all the same type of capabilities by a **flexible** monthly subscription

Switches, routers, firewalls and VPNs are always kept **up to date** in a **timely manner** (and **automatically included** as part of your subscription)

Improved uptime for your HSM estate – Thales expects to deliver a **better level of service** compared to an in-house team, especially when a new HSM needs to be added or replaced due to a fault

Inherent security you can trust

Certified implementation

Our service uses **leading edge technology** which is kept **up to date** with the **latest software** updates and s**ecurity patches.**

Our data centers are formally v**alidated** against PCI DSS and PCI PIN to **simplify** your payment **security audits.**

Our HSMs are **certified** under the **PCI HSM v3** and **FIPS 140-2 Level 3** security standards together with some regional standards

You control your data and keys

Thales has **no access to your sensitive data** or any of your **cryptographic keys** or your **audit logs.**

Each subscription is linked to a **dedicated HSM for your exclusive use** – no other service user can access your HSMs.

Support up to **10 applications securely** from a single subscription through the multiple LMK capability

Cloud service utilizes payShield 10K HSMs

Same signed software is used for the on-prem and cloud environments – you are in **complete control** of the software loading process.

TLS secured sessions supported between your application workloads and the cloud service.

Full management and **monitoring** available using common set of tools you are likely using already for on-prem payShield devices – payShield Manager, payShield Monitor and payShield TMD

THALES

Shared responsibility

Thales Responsibilities

- Install HSMs in data centers
- Cabling/connection to routers/ switches
- Network configuration
- Diagnostic checks
- Make available for allocation to subscriber
- 24x7 support
- Update to meet ongoing payment industry functionality, certification and audit requirements
- Replace any faulty HSMs ensuring minimum possible downtime

Your Responsibilities

- Connection to Cloud HSM
- HSM software and license update
- HSM security configuration and master key management (LMK, ZMK, KEK etc.)
- Audit trail management
- Ensure sufficient subscriptions to meet backup, load balancing, disaster recovery and redundancy needs
- Overall payment system audit compliance for your payment applications

Subscription logistics

SUBSCRIPTION OPTIONS

4 options available

Production tiers
(minimum 36-month commitment)

Silver: 60 cps, LMKx2
Gold: 250 cps, LMKx5
Platinum: 2,500 cps, LMKx10

Each subscription tier contains:
- **Premium package**
- **Legacy license**
- **Remote Management license**

Starter tier
(fixed 6-month commitment)

Starter : 25 cps, LMKx2

Subscription contains:
- **Premium package**
- **Legacy license**
- **Remote Management license**

Required

Management tools

payShield Manager **smart cards** and **smart card readers**

payShield TMD (including smart cards)

Note that the above management tools are not included in the subscription, but **existing smart cards / card readers / payShield TMDs** from on-prem payShield 10K deployments **can be used** with payShield Cloud HSM

Optional

Software customization service

Recent payShield 10K custom software developed for on-prem usage is **fully compatible** with payShield Cloud HSM

Any earlier version of custom software (built using a base release before v1.5a) will **need to be ported** before it can be used with the cloud service

IMPORTANT OPERATIONAL ATTRIBUTES

Control

You have full control and remote management of your HSMs

Thales has no access to your data or keys

Full segregation from other service users

Audit compliance

HSMs are certified to PCI HSM v3 and FIPS 140-2 Level 3

Thales data centers are certified to comply with PCI DSS and PCI PIN requirements

Overall payment system audit compliance remains your responsibility

Management interface

Remote management only

Same tools as with on-prem HSMs – payShield Manager and payShield TMD

Full backwards compatibility enabling use of same smart cards and LMKs for both on-prem and cloud HSMs

Service availability

HSMs housed in secure data centers, optimized to support critical infrastructures and processes with 24x7 support from Thales

Work with Thales to design a highly available service to meet your SLA requirements

Thales professional services available to assist with your scalability and high availability requirements

ON-BOARDING PROCESS

GO

1

Select regional data center(s)

2

Determine number of HSM subscriptions required
(each is single-tenant)

3

Choose performance option for each subscription
(silver, gold, platinum)

4

Place order

5

Connect to payShield HSM
(work with Thales to establish connection to HSM
for configuration and host commands)

6

Add options to subscription
(e.g. additional LMKs, increase performance,
optional licences, custom code)

DIFFERENCES RELATIVE TO ON-PREM HSM INSTALLATIONS

Subscription rather than ownership model

No physical contact with HSMs

All HSM management activities must be via payShield Manager

Base/custom software must be v1.5a or later

Ability to leverage PCI certification of data centers in addition to HSM certifications

UPGRADE OPTIONS
add HSMs or upgrade licenses on demand

Production tier subscriptions can be upgraded at any time

Silver to Gold
(60 cps to 250 cps)

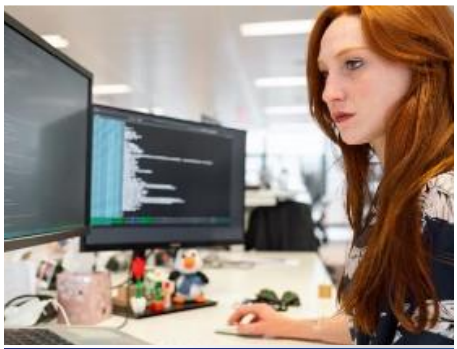
Gold to Platinum
(250 cps to 2,500 cps)

Selected optional licenses can be added to a subscription at any time

PS10-LIC-FF1 NIST FF1 algorithm support

PS10-LIC-VDSP Visa Data Secure Platform support

Available as license upgrades via Thales Support



New base and custom software can be uploaded to the cloud HSM at any time

New **HSM software** and **licenses** are downloaded via the Thales Support Portal

SECURE DEALLOCATION

When you no longer require a subscription, the following process is followed:

1 You **release** the HSM using payShield Manager

2 The HSM is **deallocated** and you **no longer have access** to it

3 Your **keys**, **data** and **logs** are **securely erased** from the HSM

4 The HSM **configuration settings** are **reset** to their default values

5 Thales installs the **latest base software** into the HSM

6 Thales makes the HSM **available for new subscriptions**

Architecture benefits

Customer control

Many Thales customers still want **full control** over their keys – this is why our initial offering is a **'bare metal' service**

Thales uses its **own specialist, proprietary out-of-band (OOB) management tool** to perform **low level configuration** and **HSM allocation or deallocation**

At no time does Thales have **any access to your keys, sensitive data** or **audit logs**

Low latency

Thales data centers are **in close proximity to** the **major CSP data centers** – you choose which CSP you wish to use

Fast interconnections are supported to deliver **low latency** between your **cloud-based applications** and the **payShield Cloud HSM service**

Easy to deploy

Easy to get started with **no large upfront investment necessary** – offers you a **lower cost disaster recovery** option for existing on-prem HSM estates

Minimal impact on your staff training and operational procedures relating to HSMs – works just like an on-prem payShield 10K

Timely availability of payment HSM capabilities for countries in which you operate when import and export of physical HSMs is complex, costly or lengthy

Ideal for fintechs with no prior on-prem HSM deployments – **helps with compliance** with the more stringent security audits

Backwards compatibility

Fundamental technology is the same as on-prem payShield 10K HSMs which is **proven in mission critical environments**

Enables you to **leverage existing payShield management tools** and **smart cards** when using the **cloud** service for the **first time**

No host client means **seamless operation** in a **hybrid environment**

Environmentally friendly

Streamlined shipments of HSMs to **fewer locations** worldwide

Reduced travel requirements for **installation** and **maintenance**

Optimized usage of products – **longer lifecycle** including eventual disposal or recycling

Key takeaways

When you wish to leverage a flexible, low-risk cloud HSM service to support new payment projects, payShield Cloud HSM is available now to deploy.

With our cloud service you shift the risk to Thales for keeping your HSM estate fully operational while freeing up your staff for other core tasks

Through extensive backwards compatibility you avoid application changes and can seamlessly operate a hybrid environment

You gain rapid access to latest certified hardware and software on-demand while eliminating the periodic physical HSM migration

THALES
Building a future we can all trust

Thales as an organization has been committed to a proactive and responsible approach to environmental protection for **more than 15 years**.

Our payShield Cloud HSM service with its **higher efficiency**, **lower transport demands** and **optimized data center** footprint plays a small but important goal in this overall objective.

Learn more about the payShield Cloud HSM service on our web site.

Abbreviations and glossary

ABBREVIATIONS

CSP	Cloud Service Provider	**PCI**	Payment Card Industry
DR	Disaster Recovery	**PIN**	Personal Identification Number
DSS	Data Security Standard	**POC**	Proof of Concept
FIPS	Federal Information Processing Standards	**RMA**	Return Material Authorization
HSM	Hardware Security Module	**SLA**	Service Level Agreement
IaaS	Infrastructure as a Service	**TCO**	Total Cost of Ownership
LMK	Local Master Key	**TLS**	Transport Layer Security
OOB	Out-of-Band Management	**TMD**	Trusted Management Device
OPEX	Operational Expenditure	**VPN**	Virtual Private Network
PaaS	Platform as a Service		

GLOSSARY

Bare-metal	payShield Cloud HSM is an example of a bare-metal service where subscribers are renting access to HSMs as part of an IaaS offering
Downtime	A period of time when the service is not available to process cryptographic requests
Fintech	A financial technology company that seeks to make financial services more efficient and accessible for both business and consumers
Hosted	A service where a third party (in this case Thales) provides subscribers access to HSMs in its data centers over a secure cloud-based or internet connection
Hybrid	An HSM estate that has a combination of on-prem and cloud-based HSMs
Latency	The typical delay (normally quoted in milliseconds) between the service receiving a processing request and the subsequence response being delivered
On-prem	IT infrastructure hardware and software applications that are hosted on-site, normally in a private data center
Uptime	The percentage of time that the cloud service is expected to be available and active with 99.99% being a realistic target for the payShield Cloud HSM service


THALES