Comparing
Cloud Payment HSMs

Steve Pannifer
Aaron Birch

FEBRUARY 2024

consult hyperion
securing tomorrow's transactions

Executive Summary

Cryptographic HSM infrastructure is a costly although critical part of any payment system. Until recently it has been necessary for payments providers to manage their own Payment HSMs – involving both exacting physical security requirements and scarce cryptographic security expertise. These constraints have made it difficult, if not impossible, to migrate payment applications to the cloud.

In response, the HSM industry has developed a number of Cloud Payment HSM offerings. These include 'bare metal' offerings which provide secure hosting but leave the management of the devices to the customer. Other 'Payment Cryptography as a Service' offerings provide more fully managed multi-tenant services.

The payments industry itself has recognised the benefit of Cloud Payment HSMs – Version 4.0 of the PCI DSS standards have been updated to include specific requirements for cloud-based multi-tenant devices. This development will mean that payments providers can adopt these services with confidence, being assured that compliant services have been thoroughly checked.

This paper provides an introduction to Cloud Payment HSMs and compares options and solutions currently available in the market. The objective is to help payment providers gain a better understanding of the potential solutions and the choices that this gives them.

The paper is based on information that is available in the public domain. To find more detail on individual products and services you should contact individual vendors directly.

This paper was commissioned by Verisec.

Contents

Executive Summary 2
1 Background 4
1.1 The need for Payment HSMs 4
1.2 The challenges with Payment HSMs 4
1.3 The solution for Payment HSMs 4
2 Payment HSM Basics 5
2.1 Overview of HSMs 5
2.2 Fundamentals of Cryptographic Key Management 6
2.3 Payment HSMs 7
3 Cloud Payment HSM Options 8
3.1 Option 1: Bare Metal 8
3.2 Option 2: Payment Cryptography as a Service 10
4 Requirements of Payment HSM Infrastructure 12
4.1 Capability 12
4.2 Cost 12
4.3 Coverage 13
4.4 Certifications and Compliance 13
5 Benchmarking 14
5.1 Comparison of Options 14
5.2 Product Benchmarking 15
6 Recommendations 17
Appendix A Glossary 18

1 Background

1.1 The need for Payment HSMs

Payment Hardware Security Modules (HSMs) are critical to payment systems. These specialist devices provide the physical and logical security needed to protect the sensitive cryptographic keys that are fundamental to secure payment systems – including card and mobile payments.

Payment HSMs are built with robust hardware security features such as tamper-resistant casings and secure boot processes, making them highly resistant to physical and logical attacks. Furthermore, they must comply with stringent industry standards such as PCI PTS HSM and FIPS 140-3, ensuring that they meet rigorous security requirements set by payment networks and regulatory bodies. These controls ensure that no one, including system administrators, is able to extract or expose the valuable keys protected by these devices in an unauthorised way.

1.2 The challenges with Payment HSMs

There are a number of challenges payments businesses will face with Payment HSMs including:

- Integration: Payment HSMs have proprietary protocols and varying security configurations which can make deployment and integration complex as well as leading to vendor lock-in.

- Expertise: Payment HSMs are highly specialised devices and so finding and retaining personnel with knowledge and experience of managing them can be difficult. Furthermore, relying on inexperienced personnel could result in operational errors leading to security vulnerabilities and service outages.

- Compliance: Payment HSMs are required to comply with industry standards such as PCI DSS and sometimes local payment industry requirements. Keeping up to date with these and ensuring relevant upgrades have been applied is time-consuming.

- Scalability: Payment systems need to be sized to support peak loads, which can be much higher than the background or average load on the system. This can mean expensive HSMs are under-utilised or even idle much of the time.

1.3 The solution for Payment HSMs

Moving Payment HSMs to the cloud can address many of the above issues – especially where the cloud provider has dedicated Payments HSM expertise and can provide scalable and compliant services. This can enable payment businesses to benefit from the resilience, scalability and business models offered by other cloud services. There are a number of cloud Payment HSM offerings available today. The characteristics of each may not always be clear. This paper examines and compares a number of such offerings to help payment businesses make informed choices on the best approach to cloud Payment HSM infrastructure for them.

2 Payment HSM Basics

2.1 Overview of HSMs

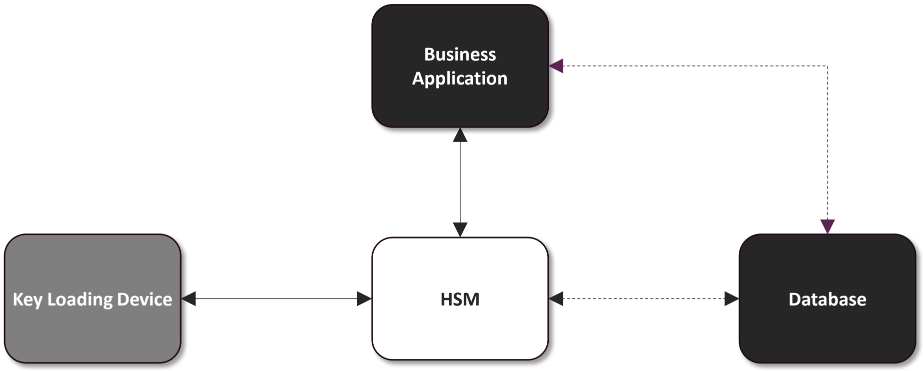

Figure 1, HSM Environment

An HSM is a specialised physical computing device that contains:

- A secure cryptographic processor that performs cryptographic operations.
- Secure memory for holding sensitive data, such as unencrypted keys.
- Random number generator to generate secure keys.

The device housing may be tamper-evident and/or tamper-resistant, so that any attempts to tamper with the device will be detectable and result in the destruction of the sensitive keys held in the device.

The device will employ secure boot mechanisms to ensure that only authorised and verified firmware can be loaded during device startup.

An HSM may interact with:

- A Key Loading Device, which allows key components to be entered into the HSM securely.
- A Business Application, which calls the HSM to perform sensitive cryptographic operations on its behalf.
- An external Database, where encrypted keys may be stored. The encrypted keys may be passed into the HSM directly or via the Business Application.

The only place sensitive cryptographic keys are available in an unencrypted form is within the secure confines of the HSM itself.

2.2 Fundamentals of Cryptographic Key Management

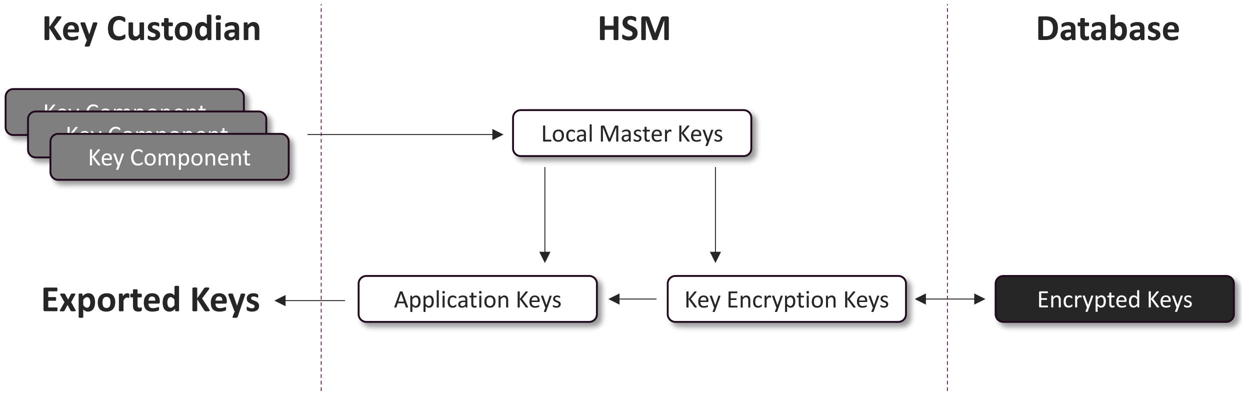

Figure 2, Example HSM Key Management

The goal of a key management is to ensure that Application Keys are protected – and usable only within trusted and known HSMs. This is typically achieved as follows[1]:

- **Local Master Keys (LMKs)** encrypt Application Keys for local storage, typically in a Business Application Database. The LMKs can exist in separate components externally – with each component being held by a separate key custodian. When the HSM is initialized, the LMK components will need to be presented to the HSM (following defined controlled processes). When an encrypted Application Key is then presented to the HSM for processing, the HSM decrypts the Application Key using the LMK prior to performing the cryptographic operation requested by the Business Application.

- **Application Keys** are used to perform the cryptographic operations required by the Business the Application. For payments this could include operations such as PIN encryption or EMV cryptogram validation. They never exist outside the HSM in an unencrypted form.

- A special instance of an Application Key is a **Key Exchange Key (KEK)** or **Transport Key**. These keys are used to encrypt Application Keys that are shared between processing partners. The KEK is typically generated on one HSM and then split into separate components which are held by separate key custodians. The components are sent from one partner to the other partner (following defined controlled processes) and recombined within another HSM. It can then be used to encrypt or decrypt the Application Keys following exchange between partners. As with other Application Keys the KEK is stored locally encrypted under the local HSM LMK.

This provides a secure and resilient approach to the protection of Application Keys – the keys that are used by the business application to perform critical cryptographic business functions.

[1] There will be some variation across different HSM vendors

2.3 Payment HSMs

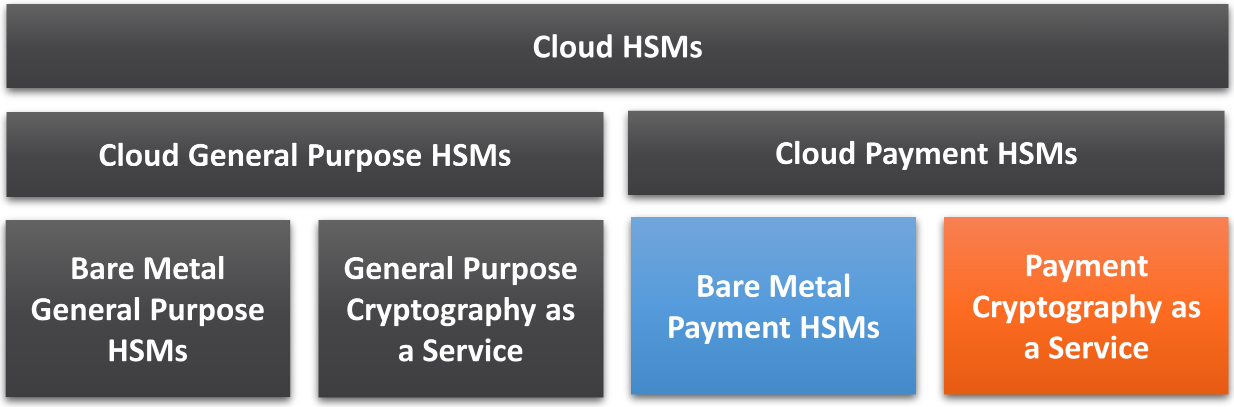
Cloud HSMs
Cloud General Purpose HSMs
Cloud Payment HSMs
Bare Metal General Purpose HSMs
General Purpose Cryptography as a Service
Bare Metal Payment HSMs
Payment Cryptography as a Service

Figure 3, Key Management Types

Cloud-based cryptographic services fall into a number of categories to address the range of different use cases and requirements in the market.

.Firstly, Cloud HSMs can be either:

- General purpose supporting standard cryptographic functions, or
- Payment HSMs supporting both standard cryptographic functions and payment specific functions. Payment HSMs will also need to comply with PCI requirements.

For both general purpose and payment HSMs a further distinction exists:

- Bare metal – where the cloud provider hosts the physical HSM device but the majority of the key management is the responsibility of the business application owner.
- Cryptography as a service – where the cloud provider hosts the physical HSM device but key management is shared between the cloud provider and business application owner.

This paper is concerned only with cloud payment HSMs – highlighted in orange in the above figure.

3 Cloud Payment HSM Options

The two primary Cloud Payment HSM approaches are described below, using the following terminology:

- Business Application – the payment service that requires strong cryptography to meet its business and compliance requirements, such as a payment processing service needing to perform PIN block translation.
- Business Application Owner – the organisation operating the business application.
- Payment HSM Service – the cloud payment HSM service used by the business application to perform secure cryptographic operations.
- Payment HSM Service Provider – the organisation operating the Payment HSM Service

3.1 Option 1: Bare Metal

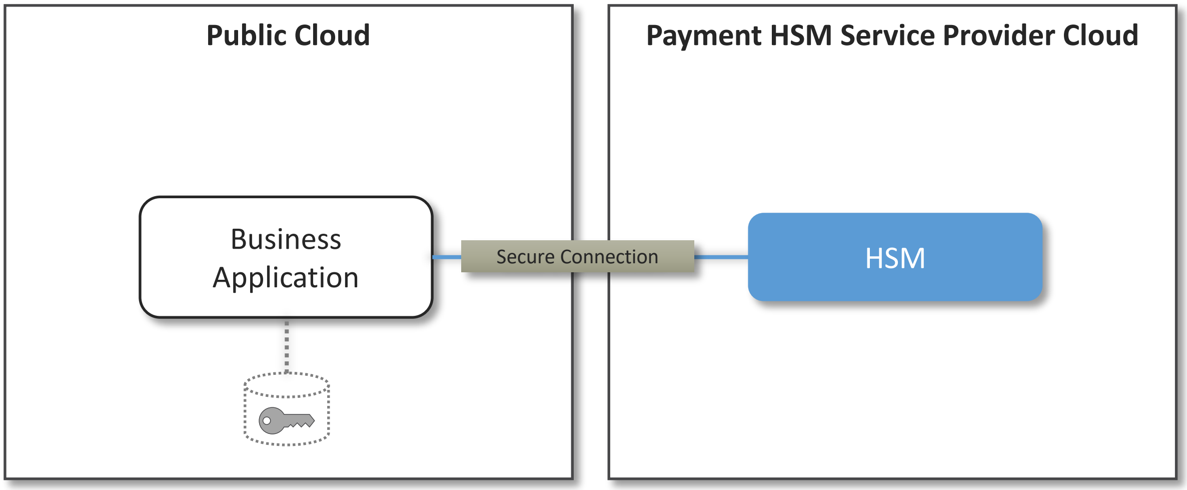

Figure 4, Bare Metal

This option is referred to as 'bare metal' because the Payment HSM Service Provider simply supports the physical hosting of the HSM devices. All administration of the device and key management is performed by the Business Application Owner.

Responsibility

The Payment HSM Service Provider will source PCI-approved HSMs and provide the secure physical environment in which the HSM is located (including physical premises, power, networking and so on). The Provider will also be involved in some aspects of HSM provisioning, depending on the requirements of the specific HSM type. These responsibilities fall within PCI scope and therefore appropriate certifications will be required.

Key management will be performed remotely by the Business Application Owner using tools provided by the Payment HSM Service Provider or HSM vendor. This will include the complex provisioning processes involving multiple key custodians that exist with legacy Payment HSM deployments in on-premises data centres.

In this option then, the Business Application Owner will benefit from the shared secure hosted environment but will need to still maintain a key management capability in-house.

Flexibility

The Payment HSMs will typically be single-tenant with the Payment HSM Service Provider leasing the number of HSM devices required by the Business Application to meet their needs. When more devices are required they can be added and when fewer devices are required, one or more devices can be recycled (following the necessary security procedures) to be made available to a different customer.

This provides some level of flexibility but it does mean that the Application Business Owner will need to lease a sufficient number of devices to support its peak load – which could mean that the Business Application Owner is paying for devices that are lightly loaded or even idle for much of the time

Integration

Access to the Payment HSMs will typically be via the native APIs offered by the HSM vendor. These proprietary APIs can be complex to use, requiring expertise in the specific HSM product being used. Where a Business Application Owner is migrating their existing HSM capability to the cloud, this will be less of an issue as the Business Application will already be integrated with those native APIs. For new Business Applications, the need to use specialist native APIs will add complexity and cost to the development process.

Encrypted application keys will usually be backed up in a database managed by the Business Application Owner.

Hybrid setups may be possible whereby the Business Application Owner uses Payment Cloud HSM services for some of their cryptography needs but also retains an in-house HSM capability. This may require the use of the same HSM products in the cloud and on premises.

Payment HSM Service Providers may have high speed connections into public cloud environments, to ensure sufficient throughput and low latency requirements of public cloud hosted Business Applications.

Examples

There are several examples of Bare Metal Payment HSM Services such as:

- Azure Payment HSM (provided by Microsoft)
- MYHSM (provided by Utimaco)
- payShield Cloud HSM (provided by Thales)
- VirtuCrypt (provided by FutureX)

3.2 Option 2: Payment Cryptography as a Service

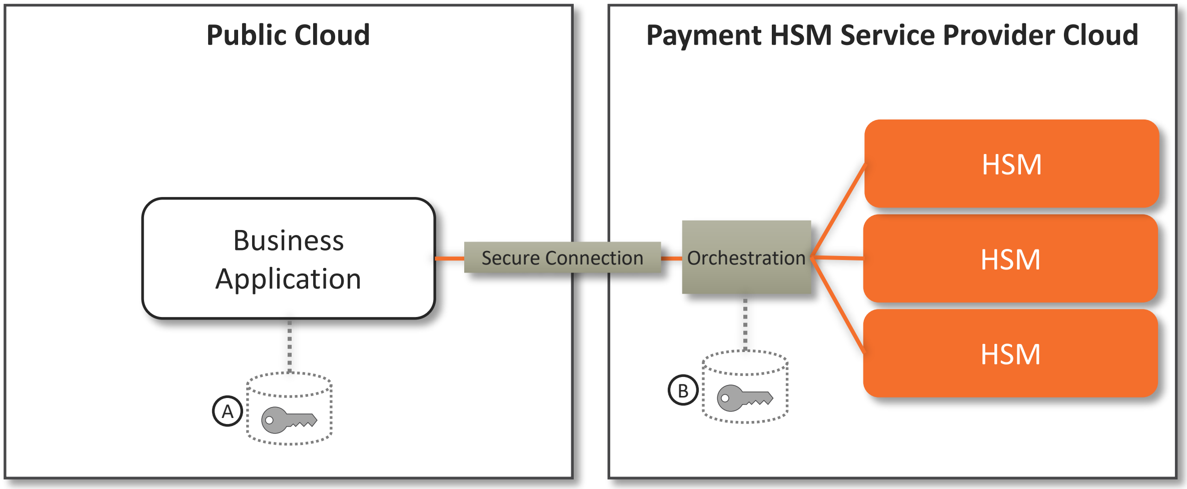

Figure 5, Payment Cryptography as a Service

In contrast to the ‘bare metal’ approach, ‘Payment Cryptography as a Service’ approaches are much more like standard pay-as-you-go cloud services. The Payment HSM Service Provider owns, operates and manages sets of HSMs that are used by multiple Business Applications in parallel. This will require the Payment HSM Service Provider to ensure customer data is segregated in line with PCI requirements. Depending on the constraints of the specific HSM devices being used, meeting PCI requirements will require careful design.

Responsibility

The Payment HSM Service Provider sources, owns, hosts and operates PCI-approved HSMs. The Provider will be fully responsible for HSM provisioning and key management. Appropriate PCI certifications will be required.

In some cases, the Payment HSM Service Provider will provide cloud storage of encrypted Application Keys (database “B” in the diagram above). In others, the encrypted keys will be stored with the Business Application in a database managed by the Business Application Owner (database “A” in the diagram above).

The Payment HSM Service Provider will likely provide a mechanism for Business Application Owners to import keys into the managed Payment HSM Service.

In this option then, the Business Application will be decoupled from the HSM infrastructure and the associated operational overheads. The Business Application Owner will benefit from the shared secure hosted environment as well as the specialist operational support that the Payment HSM Service Provider will be able to provide.

Flexibility

With Payment Cryptography as a Service, the Business Application Owner interacts with a “service” rather than with a “device”. The underlying HSMs will have been arranged so that the service offers full multi-tenancy. Multiple business applications can use the same cryptographic infrastructure simultaneously with the Payment HSM Service Provider ensuring that the service complies with all the applicable PCI requirements.

The Business Application Owner does not need to lease sufficient capacity to handle peak loads but instead can pay based on actual usage of the service. The Payment HSM Service Provider will, of course, need to ensure that the service as a whole can support the peaks it may experience – and this will need to be accounted for in the per-usage pricing.

Integration

Access to the Payment HSM Service will be via REST APIs defined by the provider, although it is possible that the Payment HSM Service Provider could expose the Native APIs as well to provide backwards compatibility to legacy Business Applications.

The REST APIs will likely simplify the interface to the Payment HSM Service, so that the Business Application developers do not need to be experts in specific Payment HSM technology. This simplification may lead to some cryptographic operations, such as those specific to particular markets, may not be supported.

Hybrid configurations employing a combination of cloud and on premises capabilities may be possible, depending on the key management interfaces exposed by the Payment Cloud HSM Service.

Payment HSM Service Providers may have high speed connections into public cloud environments, to ensure sufficient throughput and low latency requirements of public cloud hosted Business Applications.

Examples

Examples of Payment Cryptography as a Service include:

- AWS Payment Cryptography (provided by Amazon Web Services)
- Verisec 10XPAY (provided by Verisec)

4 Requirements of Payment HSM Infrastructure

In order to select an appropriate Cloud Payment HSM Service, the Business Application Owner will need to have a clear view of their requirements. The areas that will be most important in choosing the right solution are as follows:

4.1 Capability

Payment Functionality

The Cloud Payment HSM Service clearly needs to support the cryptographic payment operations required by the Business Application, which may vary depending where the Business Application sits in the end-to-end payments value chain – issuing, acquiring and so on.

The Cloud Payment HSM Service will need to support the particular payment operations and formats for the payment schemes needing to be supported – whether international or domestic.

Interfaces

The transactional interface to the Cloud Payment HSM Service could be based on native HSM APIs or on more abstracted REST API. This may present a trade-off between simplicity and flexibility – the simpler REST APIs may not provide every feature and option available in the native API.

The Cloud Payment HSM Service may also provide management APIs which enable the Business Application Owner to integrate the management of the Payment HSM Service with their other operational systems.

Interoperability

The Cloud Payment HSM Service may need to interoperate with on premises Payment HSM infrastructure where the Business Application Owner wishes to operate a hybrid set-up.

Regardless, migration to and from Cloud Payment HSM Service must be as straightforward as possible to both support the initial move to the cloud but also to avoid future lock-in.

Key Management

The ability to securely import keys via separate key components will be important for anyone migrating from a legacy infrastructure, as this will likely be how key export and import is supported by the legacy system.

4.2 Cost

Technology costs

The full financial benefits of Cloud Payment HSMs are likely to be realized with services that support multi-tenancy as that will allow the sharing of costs amongst the tenants.

For Bare Metal Cloud Payment HSM Services that still follow the single-tenant model modest savings may be realized in shared test environments. For example, a test environment could be created with a published set of keys that any prospective Business Application can use to test their service ahead of moving into production. An alternative approach here could be to provision HSMs for testing on a temporary basis, if that can be made to fit with the Business Application software development lifecycle.

Operational costs

Significant operational cost savings should be possible by moving Payment HSM services to the cloud. Physical hosting costs will be shared with the other users of the Payment HSM services. This may allow data centres (or dedicated rack space in commercial data centres) to be released.

Management costs, including standard IT management as well as cryptographic key management costs, will be shared – especially for the Payment Cryptography as a Service approach where the Payment HSM Service Provider will be responsible for those operational tasks.

Some operational risks, especially concerning retaining specialist skills, will be reduced as well.

4.3 Coverage

Geographic Data Centre Support

Business Application Owners will need to ensure that the Payment HSM Service is available in the required geographic region, to meet business and data sovereignty requirements. This will include:

- The location in which the Payment HSM Service itself is hosted, and
- The public cloud regions to which the Payment HSM Service is connected.

4.4 Certifications and Compliance

PCI

The Payment Card Industry (PCI) Security Standards Council manages the global card payment security standards and associated compliance regime. This includes:

- PCI Data Security Standard (PCI DSS), the overarching security standard.
- PTS Hardware Security Module (PCI HSM), which includes detailed requirements for HSMs including alignment with other industry standards such as FIPS 140-2/3.
- Point-to-Point Encryption (P2PE), which requires the use of HSMs.

Other

In some countries such as Australia, France and Germany specific local payment industry requirements and certification regimes exist.

5 Benchmarking

5.1 Comparison of Options

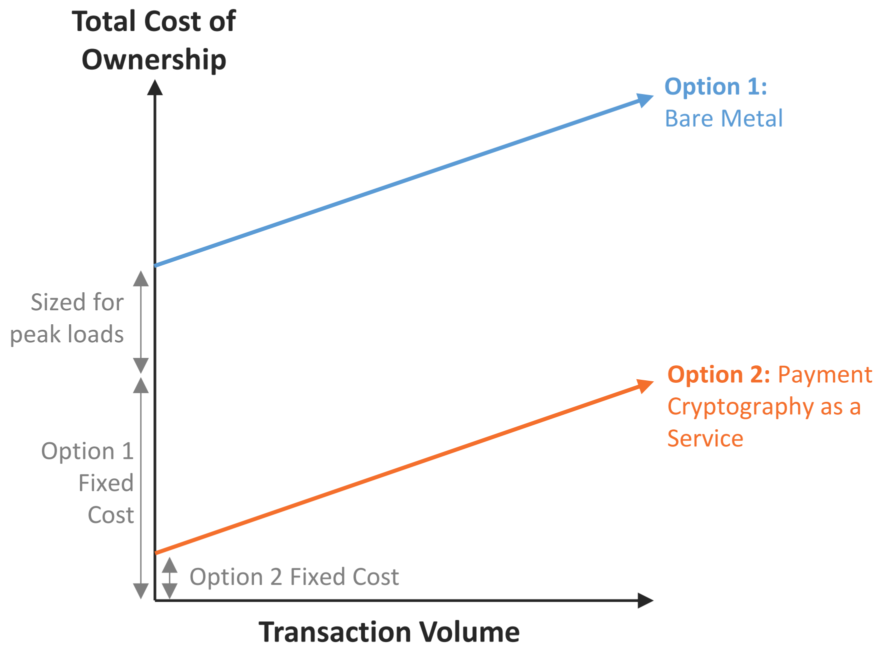

Figure 6, Total Cost of Ownership – Comparison of Options

Figure 6 illustrates the different in the Total Cost of Ownership of options 1 and 2.

The fixed costs are much higher for Option 1 as the Business Application Owner will need an operational team to manage the 'Bare Metal' HSMs and perform all key management functions. Option 2 allows much of this cost to be passed to the Payment HSM Provider.

For Business Application Owners that wish to run a hybrid setup the difference in fixed costs may be negated.

The transactional costs are also higher for Option 1 to start with, as the Business Application Owner will need to pay for sufficient capacity to support peak transaction loads, whereas Option 2 is pay-per-use.

The Business Application Owner will need to forecast the future average and peak transaction volumes and consider their operational support needs in order to determine which option is better for them.

5.2 Product Benchmarking

The table below compares example Cloud Payment HSM Services against the key requirements highlighted in section 4 above. The comparison uses public domain information only. Vendors are scored as follows:

- “Y”: The vendor appears to meet the requirement.
- “N”: The vendor appears not to meet the requirement.
- “?": It is not clear whether the vendor meets the requirement.

Cloud Payment HSM Service	Azure	FutureX	MyHSM	Thales	AWS	Verisec
Type	1	1	1	1	2	2
Capability						
Payment Functionality						
Support for standard issuer functions	Y	Y	Y	Y	Y	Y
Support for standard acquirer functions	Y	Y	Y	Y	Y	Y
Support for standard data preparation functions	Y	Y	Y	Y	N	Y
Local requirements and variations	Y	?	?	Y	N	Y
Interfaces						
Native API	Y	Y	Y	Y	N	Y
REST API	N	Y	?	N	Y	Y
Interoperability						
Support for hybrid architectures	N	Y	?	Y	N	Y
Key Management						
Key Component Import	Y	?	Y	Y	N	Y
Cost						
Technology costs						
Multi-Tenant Production HSMs (Shared Costs)	N	?	Y	N	Y	Y
Multi-Tenant Testing HSMs (Shared Costs)	N	Y	Y	?	Y	Y
Operational costs						
Shared hosting costs	Y	Y	Y	Y	Y	Y
Shared key management costs	N	?	Y	N	Y	Y
Coverage						
Geographic Data Centre Support						
Asia	N	Y	Y	?	N	?
Australia	N	Y	Y	?	N	?
Europe	Y	Y	Y	?	N	Y
Middle East	N	N	?	?	N	Y
North America	Y	Y	Y	?	Y	?
Certifications and Compliance						
PCI	Y	Y	Y	Y	Y	Y
Market Specific Certifications	Y	?	?	Y	N	Y

Our key observations from reviewing these example services are:

Capability

All Payment HSM Services in the market support the mainstream payment functions and protocols. Where support is incomplete this will be due to either:

- Abstracted REST APIs being presented to simplify integration but which do not include the full range of features available when calling native HSM APIs directly.
- Products that do not address particular local market requirements.

Cost

The cost benefits of Cloud Payment HSM Services will be greater where costs can be spread across service users, especially where HSM multi-tenancy is realized. As discussed above this is a key differentiator between Option 1 and 2.

Operational costs benefits can also be realized when the Payment HSM Service Provider takes responsibility for complex key management processes.

Where the Payment HSM Service is part of a wider cloud offering, there may be minimum volume or spend requirements in order qualify for the Payment HSM Service.

Coverage

The geographic coverage of the assessed providers varies. This may be due to Cloud Payment HSMs being a relatively new development, so that over time as services mature and demand increases, so will geographic coverage.

Compliance

All providers claim PCI compliance, as it is fundamental to the delivery of payment services. Business Application Owners should review the PCI certifications to understand the scope carefully – what payments functions were in scope of the certification, any caveats regarding the use of those services, and the assumed responsibility of the service user.

The PCI responsibility matrix should be used to clearly understand what the Business Application Owner and Payment HSM Service Provider respective responsibilities are.

6 Recommendations

Cloud Payment HSM Services will enable payment providers to move their services into the cloud whilst ensuring that those services remain secure and compliant. There are several key benefits of doing so:

- Cost – Payment-grade cryptographic services are expensive to build and operate. Specialist providers are better placed to provide these services efficiently and enable costs to be shared across their customer base.
- Compliance – Specialist providers will be exclusively focused on ensuring that their services are compliant and so are well placed to keep abreast of industry and individual HSM product level changes.
- Scalability – Cloud-based services offer the ability to scale more easily.
- Resilience – Specialist providers, who in turn will use highly available cloud infrastructure should be able to offer resilient services with very high levels of availability.

To assess which Cloud Payment HSM Service best meets your needs you will need to:

- Determine which services are available in your region.
- Understand your compliance requirements.
- Assess whether the specific functions and features you require are supported.
- Assess the migration options from your current cryptographic services.
- Consider whether you wish to take a hybrid approach.
- Use your forward-looking transaction volume forecasts to enable you to calculate the TCO for each vendor.
- Seek to take a flexible approach that avoids future lock in.

Appendix A Glossary

Term	Definition
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
KEK	Key Exchange Key
LMK	Local Master Key
P2PE	Point-to-Point Encryption
PCI	Payment Card Industry
PCI DSS	PCI Data Security Standard
PCI HSM	PCI PIN Transaction Security (PTS) Hardware Security Module (HSM)
PCI PIN	PCI PIN Security Requirements
PIN	Personal Identification Number
TCO	Total Cost of Ownership

consult hyperion

securing tomorrow's transactions

Head Office: Consult Hyperion | Tweed House | 12 The Mount | Guildford | Surrey GU2 4HN | UK

US Office: CHYP USA Inc, a Consult Hyperion Company | 234 Fifth Avenue | New York | NY 10001