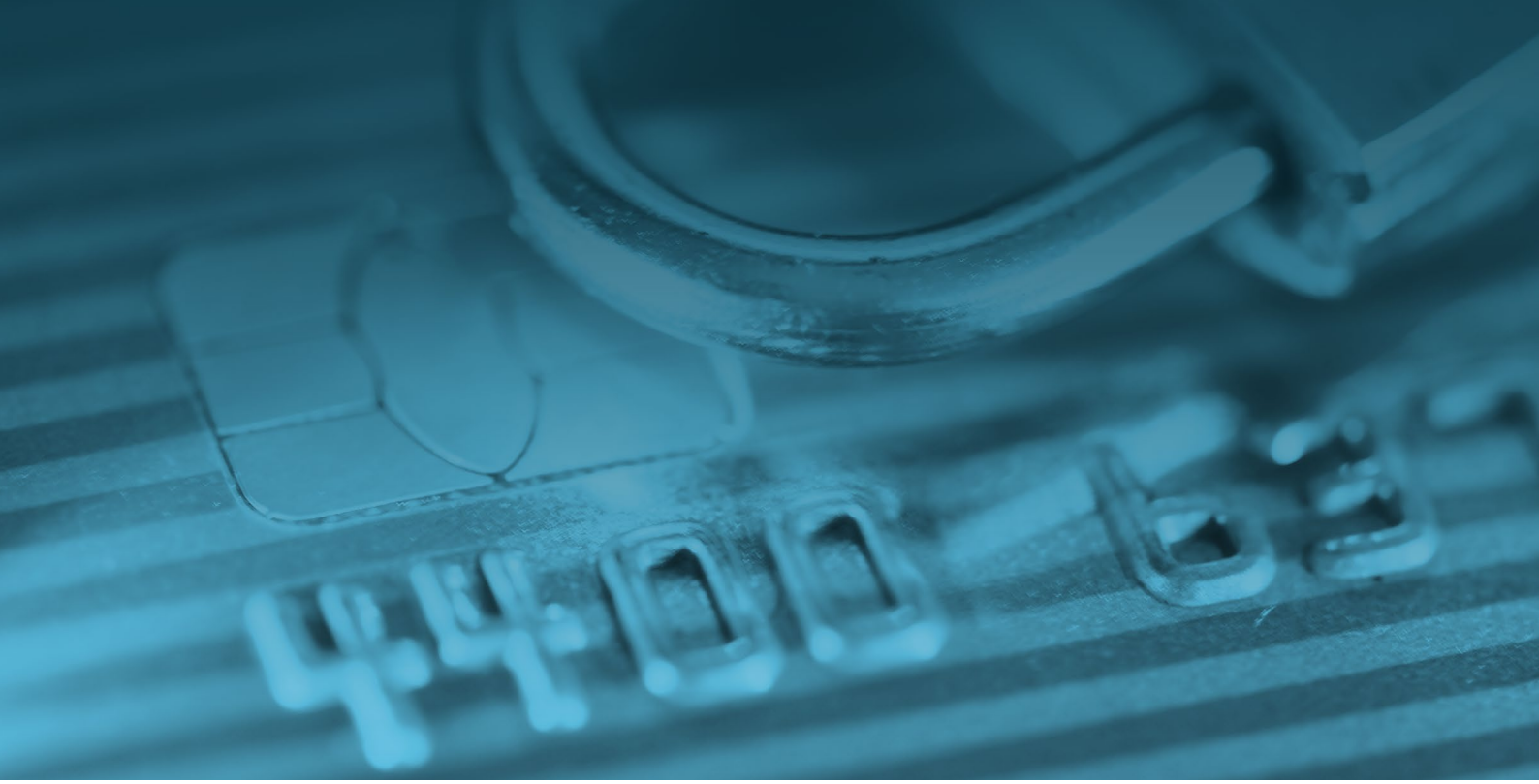

WHITE PAPER

A More Efficient Way of Using Payment HSMs

January 2020

MY HSM by utimaco®

If you are involved in processing retail card and mobile payments or in issuing cards, you have to use Payment HSMs (Hardware Security Modules).

These devices play a major part in securing the payments ecosystem. But they introduce complexity into the IT infrastructure as well as significant costs — not all of which are understood. This paper explains the issues in operating your own Payment HSMs and proposes that accessing the capabilities using a cloud-based service is a more efficient approach.

Contents

What is a Payment HSM?

Payment HSMs are devices designed and optimised for use in protecting retail card and mobile payments. They are essential peripherals used in all systems handling these payments and perform security-sensitive cryptographic functions within their secure physical boundary. This avoids security vulnerabilities in the payment networks and in payment software applications which all run on standard IT platforms. The use of Payment HSMs is mandated by PCI SSC (Payment Card Industry Security Standards Council).

The problems with operating your own Payment HSMs

Today, nearly all users of payment HSMs across the world own their estate of HSMs and operate them as part of their on-premises IT infrastructure.

Using HSMs is essential for the security of the payments system, but is expensive. One factor is the purchase cost, bearing in mind that even the smallest organisation needs at least three HSMs to provide resilience and to meet the requirement to separate operational units from those used for development and testing. Large organisations will have an estate with scores of HSMs to provide resilience, scalability, and segregation between applications.

Apart from the provision of equipment there are major costs associated with providing a suitable operating environment and in providing the skilled staff resources to manage and operate them.

Payment HSMs are also in scope for various security certifications and audits, in particular those required by the Payment Card Industry Security Standards Council (PCI SSC). This adds to the cost and complexity of running HSMs.

The implementation and operation of the HSM estate competes with funding and resources which could otherwise be used to develop the organisation's products and services, and create a competitive edge. As a result, most organisations would benefit from a different approach to that of owning their own on-premises HSMs. The desire to take a new path is also being fuelled by the accelerating move away from on-premise IT infrastructure to using cloud-based infrastructure as a service, offering significant financial benefits without compromising service levels.

MYHSM – A more efficient approach

MYHSM offers a new cloud approach to accessing payment HSM facilities, by providing Payment HSMs as a Service. Rather than buying and operating their own payment HSMs, organisations subscribe to the MYHSM service to access HSM functionality, paying a simple monthly fee based on usage levels. MYHSM take over the burden of owning, operating, monitoring, and managing the HSM hardware and software; planning capacity; managing the security of the HSM estate; providing key management services on behalf of the customer organisation; supporting the migration of customer organisations' key databases to and from the MYHSM Service; and handling the appropriate security certifications and audits for the HSM estate.

MYHSM operates the Utimaco Atalla AT1000 and Thales payShield HSMs: the two most widely deployed Payment HSMs. The HSMs are located in multiple highly secure datacentres operated by global partners such as Cyxtera and Equinix, providing high levels of capacity overhead, resilience, and reliability - as well as PCI approvals. HSM capacity used for development and testing is segregated from that used for live operations.

The Standard Service implements MYHSM's security design and configuration and provides capacity options to meet the needs of even the most demanding organisations. Where very high capacities or bespoke functionality is required, organisations may prefer the Dedicated Service.

Why go for the MYHSM Service?

There is a number of benefits in using the MYHSM service rather than developing and operating an on-premises estate of Payment HSMs. Some of these benefits will be more important than others to any particular organisation, depending on its characteristics, needs, current involvement with Payment HSMs, and environment.

The key benefits of using the MYHSM service include:

- **Reduction in capital expenditure.** Using the MYHSM service moves the HSMs from being an item of capital expenditure to being paid for out of operational costs. This may provide benefits in terms of reduced finance requirements and interest charges, and can enhance the Balance Sheet. Because MYHSM fees are based on transaction traffic volumes, costs are linked to actual usage and only rise in line with ongoing business success.

- **Outsourcing Services as a strategy.** The majority of enterprises now have an outsourcing strategy to move away from operating on-premises IT infrastructure. This typically involves the adoption of Infrastructure as a Service and Platform as a Service technologies. MYHSM's Payment HSM as a Service supports this move, letting the user avoid the many problems and pitfalls they would experience if they themselves moved their own HSMs to an internet environment such as the cloud.

- **Total Cost of Ownership (TCO).** TCO looks at the costs of a system over its whole lifetime. These costs consist of numerous factors, including some of those outlined above as well as a number which are not obvious. Comparing the TCO of an on-premises system against that of the MYHSM service is an important factor in an organisation's decision on the best way forward. TCO is discussed in more detail later in this White Paper.

- **Speed to market.** Where a new payment product is being developed by the organisation, it can be brought to market more rapidly by focussing on the development of the core product and its market differentiators rather than having to spend development time and effort on peripheral capabilities - such as payment HSM capability which could be provided by different means.

- **Reduced infrastructure pressures.** By using the MYHSM service, user organisations avoid the cost of providing and maintaining datacentre and network infrastructure to support the HSMs. This is discussed in more detail later.
- **Pressure on staffing resources.** IT systems in general, and HSMs in particular, are hungry for skilled staff resources. By subscribing to the MYHSM service these pressures on staff resourcing caused by the estate of HSMs are minimised. This is discussed in more detail later in the section on Total Cost of Ownership.
- **Security Compliance.** Systems and data centres used for payments need to be regularly audited against various security standards such as PCI DSS and PCI PIN. Undergoing these audits, and implementing changes demanded by them, can be a major strain on organisations. By using the MYHSM service rather than on-premises HSMs, the audit pain is reduced because it is MYHSM that is taking the strain.

The remainder of this document focuses on TCO, explaining the factors that should be taken into account when evaluating the costs of each approach.

Total Cost of Ownership

In the previous section we have identified the factors that are relevant in deciding whether to deploy Payment HSMs on-premises or outsource them as a service. Here we focus on the comparative costs of these factors. Some of these cost components may be more relevant than others, depending on the organisation's circumstances and where that organisation is in its system and product development lifecycle.

Overview

The table below provides a brief summary of the cost factors. More detailed explanations are provided in the next section.

Table 1 — Overview of cost factors

TCO Factor	On-Premises Payment HSMs	Using MYHSM Service
Staff resources	Significant effort to install, operate, and maintain HSMs, and to design and implement PCI-compliant security	Major reduction in demand on skilled staff
Data centre facilities	Costs of providing, operating, and securing a suitable operating environment.	No cost
HSM Vendor support charges	HSM Vendor support services have to be taken out (for best practice and to be PCI-compliant).	No cost
External Audit Costs	Fees paid to QSAs for annual/ bi-ennial PCI DSS and PCI audits.	Some reduction in fees
Regular replacement of HSM hardware	Capital costs of purchasing. Costs of disposal of old HSMs. Updating of procedures and training.	No cost
Introduction of new applications/systems	Most of the above costs, plus longer time-to-market.	Most of these costs avoided

Costs of Operating Payment HSMs On-Premises

Operational Costs – Staff resources

It needs a significant number of staff to operate an estate of HSMs. Generally, HSM activities account for only part of each person's workload, but taking the HSMs out of the equation will free up resource to be more profitably redeployed elsewhere in the company. The staff roles involved in running HSMs are:

- **Network Operations staff.** Resource will be required to maintain the network elements that are used by the HSMs, and to take account of the HSMs when making changes to the general network configuration.

- **IT Operations staff.** These will be involved in monitoring the health of the HSM estate, investigating and resolving hardware issues and other errors, regularly updating HSM firmware, replacing and configuring failed units, and reconfiguring units as the organisation's requirements change. They may also need to be present to enable Security Officers to perform their activities on the HSMs. At least two IT Operations staff must be available 24x7 to provide a comprehensive service.

- **Security Officers.** These staff are required to manage the security of HSMs, and are responsible for maintaining their security settings and holding Local Master Key (LMK) components. They are also responsible for determining action in the event of an actual or perceived security breach on the HSMs, and for undertaking forensic investigations. At least two security officers must be available at any time, although more will be required for some activities if the organisation's standards require the use of more than two LMK components.

- **Operational Key Custodians.** The creation and loading of operational cryptographic keys require multiple (typically three) Key Custodians, each "owning" one of the components that is used to form the key. Depending on the organisation's size and structure, the Key Custodian roles may be held by IT Operations staff or Security Officers. Generally Key Custodians do not need to be available outside of normal working hours.

- **Security Architects and Internal Auditors.** There is an ongoing involvement by these roles to ensure that the HSM estate meets the evolving security needs of the organisation. They will also be heavily involved in preparing for PCI audits (such as DSS and PIN) and in addressing any HSM-related issues that emerge from those audits.

- **Staff turnover.** Every organisation experiences some level of staff turnover. When a member of staff needs to be replaced the organisation incurs significant costs such as HR admin, advertising and recruitment agency fees, management time, training, and the delay of getting up to speed.

All of the above costs apply to an on-premises HSM strategy. By using Payment HSM as a Service the vast majority of these costs can be avoided.

Operational Costs – Data Centre

Payment HSMs need to be accommodated in data centres providing networking, security and protection against environmental factors (such as power outages, temperature, fire, flooding, earthquakes). Apart from the initial capital costs of setting up a datacentre, there are various ongoing running cost components:

- A share of datacentre overheads such as air conditioning, lighting, staffing, property taxes, back-up power supply, interest payments or asset value write-down.
- Electric power consumed.
- Opportunity cost: if the datacentre rack space is fully utilised, then the HSMs may be occupying rack space that could be allocated to other priority projects.

These costs are completely avoided if the MYHSM service is adopted.

Operational Costs – Support Contracts

The organisation must take out a vendor support contract on each HSM. This is advisable in any case but becomes essential to comply with PCI requirements to access and implement the HSM vendor's current software. The cost of support contracts over the lifetime of an HSM can exceed the initial purchase costs of the equipment.

When using the MYHSM service, this cost becomes the responsibility of MYHSM, and is covered by the standard subscription cost of the service.

External Audit Costs

The organisation will need to undergo regular security audits against relevant PCI standards such as DSS and PIN. This will incur costs both in terms of the organisation's staff, as already mentioned, and fees for approved and qualified external auditors. These external fees will be related to the complexity of the system and infrastructure being audited: reducing the complexity by not having an estate of on-premises HSMs means that these fees can in turn be reduced.

Replacing End-of-Life HSMs

HSM vendors typically bring out new HSM models every 5-7 years. The new model may be attractive to the organisation because of new capabilities it offers, but the organisation will in any case have to move to the new model because of the PCI requirement to continue deploying vendor security updates, to have access to certified products when buying additional capacity, and to avoid having a cocktail of different models in operation.

Replacing the estate of HSMs introduces a number of costs:

- The cost of buying the new product, adding to Capex.
- The opportunity cost of buying the new product (i.e. not being able to apply those funds to other projects)
- The time for IT and Network Operations staff to install the new HSMs.
- Evaluation of the new HSMs by Security Architects and Internal Auditors, and the implementation of revised procedures adapted to the new HSMs.
- Added complexity in the next round of PCI audits.
- Testing.
- Re-training of IT Operation staff, Security Officers, and Key Custodians.
- Secure disposal of the old HSMs.

The majority of these costs are negated by using the MYHSM service. MYHSM will implement the new HSMs in a way which is transparent to the user such that operations will continue uninterrupted during and after the migration to the new models.

Introducing New Systems or Applications

The costs we have discussed above will apply to all users, including those who have systems which are already operational. In addition there are significant HSM-related costs relevant to any organisation that is undergoing a major change in its IT structure, such as introducing a new system, launching a new application, or moving to a new datacentre.

- Building additional data centre, network, and rack space capacity.
- Recruiting new staff.
- Design of IT and Network infrastructure to service the HSMs.
- Security design for the HSM estate.
- Acquisition of HSM capacity. The categories of costs will be similar to those discussed already under *Replacing End-of-Life HSMs,* although the levels of some of these costs will be higher.
- Delayed time to market: by competing for staff resources and its demand for infrastructure facilities, the HSM estate will prolong the time to introduce the new system or application. This may hinder the ability

of the organisation to meet corporate, legislative, or regulatory schedules, or reduce or delay the benefits from projects which are designed to increase revenue or reduce costs.

- PCI certification.

These costs can be reduced or avoided altogether by using the MYHSM service rather than building an on-premises estate of HSMs.

Costs of Using the MYHSM Service

Use of the MYHSM service involves an on-boarding charge and a simple monthly subscription fee, replacing most of the intricate structure of costs associated with on-premises implementations. This fee is predictable, fixed, and linked to usage volumes.

Summary

Payment HSMs are a valuable and essential asset in securing the world's payment networks and are needed to satisfy payment industry security mandates, but they come at a price. Whereas user organisations have traditionally owned and operated their HSMs as part of their on-premises IT systems, new technologies and the burgeoning interest in the cloud makes MYHSM's Payment HSM as a Service a realistic and compelling alternative.

For a monthly fee organisations can access the payment HSM capacity they require without the pain of having to buy, implement, operate and manage the HSMs or providing the infrastructure, skills and resources that they demand.

Want to learn more?

If you would like to run a detailed model that illustrates how MYHSM could reduce TCO in your organisation's environment, please contact us through www.myhsm.com

If you are interested in learning more about MYHSM, please visit: www.myhsm.com