Semafone – using HSMs to support PCI compliance and keep data secure

Don't let your business fall victim to a cyber-attack

There is no such thing as having too many layers of security when it comes to keeping customers' sensitive data safe; consequently Hardware Security Modules (HSMs) are one level of protection that companies, both large and small, can and are implementing to reduce the vulnerability of information stored within internal systems.

Not just another acronym – what does an HSM do?

If you work for a large organisation, chances are you are already using an HSM whether you're aware of it or not. Essentially, a HSM is a physical piece of hardware that:

- Secures many different elements of your IT estate by encrypting data at rest or during transmission between two or more parties; be they user to user, user to machine, or machine to machine.
- Separates the encryption process from existing applications and users by generating secure keys or encrypting messages, using complex mathematical algorithms.
- Registers unauthorised attempts to access its system as an effort to tamper with the cryptographic keys and responds accordingly, whether this is to audit the data, log the access attempt or trigger alerts to the security team.

HSMs for PCI

HSMs can offer digital signing services for a range of applications and, as they typically sit at the centre of an organisation's secure infrastructure, they form an integral line of defence against cyber-crime. Thanks to this, the latest version of the Payment Card Industry Data Security Standard (PCI DSS V3.1 3.5.2) acknowledges that using a HSM improves cyber security.

By offering this level of security, a HSM makes PCI DSS V3.1 controls 3.5.3 and 3.6.1 through 3.6.5 much easier to address, manage and audit. Once this technology is implemented properly, many of these activities become 'business as usual' and will benefit your entire estate, not just the PCI DSS zones that are under scrutiny.

The Apple approach – HSMs at work

Even tech giant Apple has turned to HSMs to improve security and has created a strategy revolving around using HSM devices to protect the credit and debit cards the Apple iCloud handles, including the safe storage of passwords and app policies. Each customer's data is encrypted by a strong key and then stored in Apple's cloud platform. This strong key is then also given comprehensive protection, which is where the HSM comes into play, securing the strong key alongside additional encryption by the iCloud Security Code.

semafone®
secure voice transactions

Getting your DUKPTs in a row

While there are other virtual solutions on the market, these are often left vulnerable as they rely on manual processes and systems to protect them. This means that once a hacker has gained the original cypher-making tool, they can potentially crack the entire system. HSMs are able to mitigate this risk by using a key management tool called a DUKPT (derived unique key per transaction). Using DUKPT as part of your HSM's deployment means that organisations can encrypt every message individually, with distinct cryptographic codes applied to each package of information, meaning that if one transaction is compromised the others remain secure.

> "Integrating all your payment data, as well as data within your telephony estate"

Put the HSM at the centre of your security

If you're serious about bringing your data security up to the highest standard, it is vital that any system that stores, transacts or monitors data is integrated with a HSM. This should be applied across your entire organisation, to encompass telephony and point-of-sale systems, and not just within e-commerce platforms as is typically the case.

At Semafone we are increasingly helping our clients link all their data to a HSM, regardless of which source it has been collected through. This removes any third party touchpoints and subsequent security processes, which helps reduce the burden of PCI compliance and improves return on investment for your organisation as you no longer have to regulate and secure a multi-layered and complex data environment.

Ultimately, integrating all your payment data, as well as data within your telephony estate, with a HSM brings everything under one roof. This means you can rest a little easier knowing you have not only made PCI compliance easier, but have also bolstered information security organisation-wide.