SPONSORED CONTENT | WHITE PAPER

Cybersecurity

HSMs: A Critical Component of an Enterprise's Cybersecurity Strategy

CSO

SPONSORED BY ENTRUST

Cybersecurity

Today's organizations know that data is paramount for seamless operations, positive customer experiences, and future business growth. Enterprises know cybersecurity threats are rising. Data protection has become even more important in today's distributed environment where organizations are pursuing multicloud solutions. Many companies encrypt data using cryptographic keys. But then, too many fail to adequately protect these keys, leaving data vulnerable to internal and external threats. The best way to safeguard cryptographic keys – and ultimately protect critical data – is with hardware security modules (HSMs) that are specifically designed to safeguard and manage them.

The challenges of protecting critical data

Organizations are using more data to do business, remain competitive, and gain better insight in their market and their customers.

This includes personal identifiable data, corporate financial data, customer sales information, HR and sales data, and intellectual property. All can be vulnerable to threats coming from both inside and outside an organization. It's a growing concern, especially given today's distributed environment where data is no longer kept within a defined perimeter. Instead, many companies store data in the cloud and across data centers.

"There's no such thing as a defined security perimeter anymore, it's a very grey area," says Juan Asenjo, director of product solutions and partner marketing at Entrust. "The distributed environment opens more vectors for attack, creating more threats – and more bad actors out there are trying to take advantage of all of this, increasing the risks."

These threats include external threats – hackers that steal data and keys, or inject malware or trojans into infrastructure – and internal threats, from disgruntled staff. Human error can also put data at risk. Threats can come via social engineering, bribery, corruption, or coercion.

At the same time, privacy and data protection expectations for enterprises are high. Companies that fail at protecting their data risk losing intellectual property and customer confidence. They might also face stock market losses, hefty remediation expenses, litigation costs, and even fines.

Most enterprises are well aware they need to safeguard the critical data assets that define their organization and what they do. To protect against these threats, many have turned to encryption, using mathematical algorithms so data becomes inaccessible to unauthorized users. Cryptography keeps data secure, and it also secures internet transactions. Cryptographic algorithms use cryptographic keys to lock and unlock data.

According to the 2022 Ponemon Institute Global Encryption Trends Study, the top five drivers for using encryption are:

- **Protect customers' personal information**
- **Protect information against specific identified threats**
- **Protect enterprise intellectual property**
- **Comply with external privacy or data security regulations and requirements**
- **Limit liability from breaches or inadvertent disclosure**

But cryptography is only as secure as the level of protection given to the cryptographic keys. Asenjo likens it to the lock on a person's front door and its accompanying keys. "The strength of that lock on your door is only as good as where you store the key," he says. "If you put it under your welcome mat, it's easily found, and your protection then is not effective."

Unfortunately, too many organizations either don't know where they store their cryptographic keys or they store them in software, which can make them easy targets for hackers due to the keys' very distinctive footprint in a server's file system. This vulnerability extends to bad actors both outside and inside an enterprise.

It's not uncommon, Asenjo says, for an enterprise to install a database security solution that comes with a measure of cryptography for encryption of information. But then the enterprise stores the keys on the same software level in which the application is running.

"They're putting it under the front-door welcome mat," he says. "If you don't give your keys a higher level of protection, you're not ensuring your cryptographic mechanisms are up to par.

Protecting your cryptographic keys is paramount in order to ensure the integrity of your information and the enterprise."

A comprehensive solution to managing cryptographic keys

Organizations need a way in which to manage their cryptographic keys throughout their life cycle, from their creation, while they're in use, during storage, to deletion and replacement.

When it comes to sensitive and critical data, organizations have to ensure confidentiality, integrity, and availability. They need to follow through after implementing cryptography. HSMs are at the heart of that.

HSMs are devices that are designed to generate and manage cryptographic keys separate from the application(s) they are supporting. "You're purposely putting the keys in a different place, in a vault that's hardware," Asenjo says. HSMs have built-in mechanisms to ensure keys are only used for their desired application, and that only authorized individuals and applications have access to them.

What's more, HSMs ensure the policy for the use of cryptographic keys cannot be altered by any one individual or entity without checks and balances and dual controls. Much like a customer and banker are both needed to open a safety deposit box at the bank, with HSMs changes to an enterprise's keys must be approved by more than one person.

In today's environment of increased and ever-more-sophisticated threats, HSMs are a vital component of every enterprise's cybersecurity strategy, Asenjo says. HSMs provide a secure environment to generate, use, and manage cryptographic keys — and they deliver defense in depth for data and keys so bad actors ultimately go elsewhere.

HSMs also uphold best security practices. They offer security reassurance to organizations, enabling greater control. They're also versatile — they can be used across a wide range of applications including public key infrastructures (PKIs), cloud, the IoT, digital payments, blockchain, and code signing, to name a few.

The top benefits of HSMs include:

- **Adding an extra layer of security**
- **Protecting cryptographic keys**
- **Providing resilient key storage**

- **Warding off hackers**
- **Facilitating regulatory compliance**

Certified HSMs offer peace of mind

HSMs that are certified, like Entrust nShield HSMs, give enterprises enhanced protection.

Certified HSMs meet globally recognized standards for cryptographic robustness, including the Federal Information Processing Standards (FIPS) and the Common Criteria. “It’s important the devices are certified. It’s an independent good seal of approval,” Asenjo says.

Entrust’s nShield HSMs are specially designed to deliver a certified hardware environment and are offered as an appliance, embedded card, or a USB device. The appliance can be deployed at an on-premises data center, or it can be leased through an as-a-service subscription (nShield as a Service).

nShield HSMs enable organizations to secure keys within a carefully designed cryptographic boundary that employs robust access control mechanisms, so keys are only used for their authorized purpose. nShield HSMs ensure keys are always available to applications when they’re needed via sophisticated key management, storage, and redundancy features. This delivers high performance to support demanding applications and transaction rates.

Regardless of their form-factor or deployment option, Entrust’s nShield HSMs provide robust key generation for signing and encryption to protect sensitive data and transactions. Entrust’s nShield HSMs:

- **Isolate keys from the application(s) and software environment**
- **Implement strong user authentication and separation of duties**
- **Enable implementation of custom applications within the FIPS security boundary**
- **Simplify secure key backup and deliver strong policy enforcement**

“Another capability that makes nShield unique is its overarching management architecture, called Security World,” Asenjo says. Security World takes keys and breaks them into individual components. Then, those components are stored in different locations, and can only be reconstituted within the HSM. “That gives a higher degree of security and resiliency,” Asenjo explains.

Entrust customers have benefitted from nShield helping them better protect their sensitive data. Novacoast, a company that manages digital security for other enterprises, collects data on its customers, including names and phone numbers. The company prioritizes risk avoidance and mitigation and wanted to follow security best practices. With nShield, it's been able to successfully protect cryptographic keys, ensuring data travels securely between different applications.

Meanwhile, Hungarian Qualified Trust Service Provider Microsec provided message security services for the Autobahn GmbH des Bundes, the German highway operator, and its infrastructure's cooperative intelligent transport system (C-ITS) utilizing Entrust HSMs.

With the help of nShield, around 6,000km of European roads are C-ITS enabled. Suitably equipped vehicles, road users, service providers, and road operators are all networked and can securely exchange anonymized data with one another. This has enhanced road safety for drivers, passengers, and maintenance workers by creating a fully digital, connected, and automated traffic system.

As the business world continues to evolve and more companies operate in a distributed environment and migrate to multicloud environments, additional key management challenges are emerging, Asenjo says. Enterprises must be prepared.

"When you have different cloud environments using different cryptographic mechanisms, how do you bring all that together? You need visibility and you need to apply security controls in a consistent manner. nShield provides a root of trust for underpinning cryptographic keys, bringing a level of consistency to organizations."◆

To learn more about HSMs and the benefits of Entrust's nShield, click here.