Increasing the Return on Investment of Your HSM Infrastructure

TABLE OF CONTENTS

INCREASING THE RETURN ON INVESTMENT OF YOUR HSM INFRASTRUCTURE

Organizations often purchase security technology to fulfill specific industry regulations, however, these regulations are only the bare minimum of requirements to ensure the safety of your data and your customers' information.

When developing a strategy for your cryptographic ecosystem, it's important to consider a holistic plan for how hardware security modules (HSM) will be integrated into your existing infrastructure; establishing a security framework by implementing a system of procedures to complement your hardware security solutions; and what other applications you might find for your hardware security module in your organization.

Viewed from this frame of reference, you begin to unlock the true value of a hardware security module and how it can protect your organization and its sensitive data. This whitepaper discusses common dangers enterprises face and the multifaceted advantages of hardware-based data security solutions.

COMPLIANCE: MORE THAN A CHECKBOX

Every industry has its regulatory requirements which, by nature, assign responsibility to certain entities to ensure best practices are followed and protections are enforced. The specifics of these regulations vary from industry to industry, but with the growing confluence of Big Data and the collection of sensitive customer information, one thing has become increasingly common: regulations have been adapting to a growing need for standardization and the development of procedures for securing personal information.

In short, enterprises have a responsibility to safeguard the information they protect and prevent it from falling into the wrong hands. When sensitive information is accessed by unauthorized parties, or data is unintentionally released, it is known as a data breach. The motives for these breaches run the gamut from fraud, to corporate espionage, to state-sponsored espionage or activism, to less intentional breaches involving employee negligence.

PERSONALLY IDENTIFIABLE INFORMATION

"Personally Identifiable Information is defined as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[1]

— NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (NIST SP 800-122)

Enterprises spend a significant amount of time, money, and energy complying with industry regulations mandating the protection of sensitive information. In reality, these regulations are only the beginning of the measures an organization must take to properly secure their sensitive information from possible breach. What's more, the regulatory landscape is constantly shifting. Extra measures that organizations currently take to secure their data may someday become mandatory as regulatory requirements evolve. Thus, while regulations are necessary protections for enterprises and their customers, compliance does not ensure complete safety from data breaches.

While much fear is circulating about the prevalence of breaches and the release of customer data, proper planning and consideration of security options can greatly mitigate the risk and help organizations navigate the waters in an increasingly complex regulatory world and avoid costly breaches.

THREATS TO ENTERPRISE SECURITY

Threats to enterprise security are numerous and well-documented by the media. Hardly a week goes by without reports of large-scale compromises of records, with many of these breaches occurring at large, Tier One organizations. If you are a systems administrator, it may seem like breaches can come from anywhere—and you would be correct in that assumption, based on several studies released in 2016.

According to the findings from Verizon's annual Data Breach Investigations Report, 3,141 confirmed data breaches with over 100,000 reported security incidents were identified in 2016.[2] Among the incidents, 8% came from the retail industry. Retail breaches often result from the vulnerability of their electronic payment terminals. Credit, debit, and prepaid card terminals are often situated in publicly accessed areas and connected to less secure, public networks, placing them at greater risk for criminals to install malware to intercept cardholder information.

These statistics are consistent with the longer-term data collected by the Privacy Rights Clearinghouse (PRC) which began tracking breaches in 2005. Since then, PRC estimates place the number of records compromised at more than 900 million.[3]

Organizations across multiple industry verticals share this risk. Financial organizations represented 35% of the incidents, accommodation industries for 12%, information industries for 8%, government agencies for 8%, and retail for 8%. The most prevalent cause of breaches: 70% from hackers, 19% from lost or stolen endpoint devices such as tablets, laptops and smartphones, and 4% of all breaches were from someone with legitimate access, such as an employee or contractor.[3]

What is evident from these numbers is the diversity of entry points which attackers can and do exploit. According to the Verizon Data Breach Investigations Report, over 80% of attacks on organizations originate as outsider attacks: including hackers or others without authorized access to network systems and data.[2]

Worrying still, is the threat of a breach caused by a rogue, or simply negligent, employee. Breaches of this type range in type from the lost device like a cellphone or tablet to an orchestrated attack. When industry best practices are not integrated into an organization's policies, or are ignored altogether, the stage is set for an internally driven breach.

Trends in technological development, while they are revolutionizing the way data is stored, accessed, and used, should give organizations pause. Information stored in vast, cloud-based repositories or on unencrypted servers are ripe for a data breach. Additional steps must be taken in order for employees or outside attackers to access the information beyond simple password protection, and limitations must be placed on the ability to transfer large chunks of data using a USB thumb drive or another storage device.

Outsiders have become ever more resourceful in their attacks on organizations. In 2016, a report surfaced describing an online marketplace which has commodified access to hacked corporate systems worldwide. The market offered access to aerospace, oil, and chemical companies for as little as a $6 each.[4]

To mitigate these risks, organizations are taking a varied approach to data security. A mix of policy-based security procedures and hardware-based security systems with a foundation in data encryption are proving effective in preventing both insider and outsider attacks.

COSTS OF A BREACH

Breached organizations experience a number of negative consequences, which ultimately include financial losses, but also less direct losses including a decline in their brand value and potentially a loss of customers. The average cost from a given data breach is $4 million dollars, with an average of $158 per record.[5]

Data breaches are not isolated events exclusive to large organizations, and the impact to a small company can have devastating effects. While the security measures that work for a startup may not always be successfully replicated for larger, Tier 1 organizations, adherence to security principles can boost the preparedness of organizations of all sizes. Without significant prevention of data breaches, organizations are at a greater risk for experiencing the negative effects of a data breach in the future.[5]

Beyond the punitive costs of violating regulations, if an organization is proven negligent, a breach can have far-reaching effects. Risks associated with a breach include:[5]

- Loss of customers and revenue
- Negative publicity in the blogosphere and through media outlets
- Release of personal private information
- Diminishment of customers' and business partners' trust and confidence
- Lawsuits by affected parties and regulatory fines resulting in severe financial losses
- Exposure of confidential proprietary information

Organizations pay a steep price in the wake of a breach. Some regulatory bodies mandate breached organizations undergo a lengthy audit process to determine if proper measures have been instituted to prevent another breach. If the compromised data is related to personally identifiable information, organizations may choose to cover the costs of personal credit counseling or monitoring in an effort to minimize the effects of identity fraud or theft related to the breach.

BENEFITS OF HARDWARE-BASED SECURITY SOLUTIONS

Hardware security modules implemented in an enterprise's security infrastructure are dedicated devices built to protect data using physical, logical, and encryption-based security features. HSMs are versatile solutions which can perform a wide array of functions across multiple industry verticals.

Encrypting and authenticating sensitive data using a secure cryptographic device offers unparalleled benefits for maintaining security, preventing fraud, and ensuring regulatory compliance. Breaches from both insiders and outsiders are valid worries for system administrators, but hardware security modules provide an unrivaled form of protection to defend against these vulnerabilities. These tamper-responsive devices are designed to house encryption keys within a secure boundary, eliminating risks commonly associated with software data security tools.

WHAT IS AN HSM?

A hardware security module, or HSM, is a dedicated, standards-compliant cryptographic appliance designed to protect sensitive data in transit, in use, and at rest through the use of physical security measures, logical security controls, and strong encryption.

Furthermore, attackers are unable to access the clear encryption keys contained within the HSM, even when they physically tamper with the device, whereas a simple keylogger can often prove the downfall of software-based tools. HSMs, however, are capable of identifying unauthorized access or attempted attacks. Attempts at tampering with the hardware will cause the device to immediately erase all sensitive data, providing an additional layer of protection preventing the attacker from acquiring that information.

Additionally, hardware security technology can offer advanced disaster recovery and redundancy features — functions that guarantee continued operation in the event of an unplanned outage. For global organizations with a vast array of mission-critical data in widespread use on a 24x7x365 basis, this reliability is a necessity.

ONE DEVICE, MANY APPLICATIONS

Hardware security modules have wide-ranging applications across many industries, including among financial institutions, manufacturers, healthcare providers, educational institutions, government agencies, and retail industries, to name a few. HSMs are highly versatile solutions, and as such, their applications can be better divided into financial and general purpose (GP) categories. In either financial or GP capacity, an HSM can serve as an important facet of an organization's data security infrastructure.

**Some functionalities of a hardware security module, such as PIN printing and 3-D Secure, must be carried out on a dedicated device.*

GROWTH OVER TIME

An investment in a Futurex HSM is a pivotal step in improving your organization's security, and as such, your organization should select a solution which provides the greatest protection over time. Futurex continues to dedicate resources to producing new features and capabilities for deployed Hardened Enterprise Security Platform devices. After a product's release, Futurex continues to find countless new applications for the technology. These innovations are integral for Futurex customers, who maintain a superior security positioning.

GENERAL PURPOSE APPLICATIONS

CERTIFICATE-BASED MULTI-FACTOR AUTHENTICATION USING MICROSOFT ACTIVE DIRECTORY

Microsoft Active Directory is used by many organizations to manage their corporate Windows domain and handle authentication and security policy administration for their users. Active Directory includes Certificate Services, a hardware security module-supported component used to issue X.509 certificates for the authentication and security of a wide range of applications. Within this environment, Futurex HSMs can be used for both user and device management, and are capable of managing thousands of CAs and SubCAs, with virtually limitless scalability.

SELECTED USE CASES FOR MICROSOFT ACTIVE DIRECTORY CERTIFICATE SERVICES (SOURCE)

- Multi-factor authentication for Exchange, Office 365, ActiveSync, Windows Hello for Business, and more
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Secure wireless networks
- Virtual Private Network (VPN)
- Internet Protocol security (IPsec)

- Encrypting File System (EFS)
- Smart card logon
- Secure Socket Layer/Transport Layer Security (SSL/TLS)
- Digital signatures

Active Directory provides administrators with granular control over username and password complexity, expiry, and rotation policy, however these passwords can be stolen from individual users through malware or social engineering. Multi-factor authentication in a Microsoft Active Directory environment relies on two key factors to validate user identities: certificates generated by an HSM that are installed on the company-issued device itself, and the username and password credentials. By requiring something the user *has* in addition to something the user *knows*, the likelihood of an attack succeeding is dramatically decreased.

Active Directory Certificate Services easily integrates with Futurex HSMs using Microsoft CNG, formerly known as Microsoft Crypto API (CAPI). The integration process for defining a Futurex HSM as a Cryptographic Services Provider is straightforward and involves administrators defining selected variables in a configuration file and placing a .dll on the Active Directory server. Futurex provides an integration guide and a team of expert Solutions Architects to assist with implementation.

ONE-TIME PASSWORD GENERATION FOR ONLINE SECURITY

An organization's online presence can be a particularly vulnerable point for an attacker. Many attacks involve targeting the password validation process, using phishing or keylogging malware to gain knowledge of the user's password, using it at a later point to gain access to systems. A one-time password mitigates this risk by cryptographically generating a password that is valid for a single use. Users can generate one-time passwords for a virtually limitless number of reasons: to supply an auditor with a passcode for a secure facility, for example.

Using the Excrypt API, Futurex HSMs create one-time passwords that are based on Hashed Message Authentication Code (HMAC) using the HOTP specification defined by the Internet Engineering Task Force (IETF). HMAC-based one-time passwords operate by relying on the hardware security modules to generate random data used in the generation of passwords. Because these values are generated inside the HSM, they cannot be viewed by attackers, ensuring the integrity of the access control systems that use them.

SSL/TLS PRIVATE KEY STORAGE FOR WEB SERVERS (APACHE HTTP SERVER AND MICROSOFT IIS)

When exchanging sensitive data electronically, users want to ensure that their data is protected from compromise and that the connections through which they are exchanging information are secure and protected. Mutual authentication is the process by which devices communicate with each other securely, based around public key infrastructure (PKI) in which public and private keys establish authenticity. A significant percentage of modern applications accomplish this through web-based interfaces. When deploying websites or web-based applications, the connection between the browser and the web server should always be protected using Transport Layer Security (TLS), which was formerly known as Secure Sockets Layer (SSL).

Maintaining the confidentiality of the private keys used by the web server to decrypt incoming connections is vital to the success of IT infrastructures. In order to avoid situations such as a rogue employee or other malicious actor gaining access to a web server and stealing the private key, organizations can use hardware security modules to

protect them when not in use. This hybrid solution provides enhanced security for at-rest key storage while still enabling the web server to perform decryption tasks. Futurex HSMs can be used for SSL/TLS private key storage in virtually all major web servers.

For Apache HTTP Server, this is accomplished through PKCS #11, a standards-based cryptographic library available on Futurex HSMs. With Apache, the SSL/TLS private key is stored within the HSM's tamper-responsive boundary and only made available for the web server when needed. This stores the key in memory and reduces vulnerability to a wide range of attack vectors. Should a malicious actor attempt to access the private key within the HSM itself, it will automatically enter a tamper state and erase the contents of memory. This process is accomplished by creating keys and certificates, converting them into the appropriate format, and then loading those certificates into the relevant clients.

Securing private keys for Microsoft Internet Information Services (IIS) is performed using a similar process to Apache, but with Microsoft's Cryptography API: Next Generation (CNG) instead. The same usage structure is present with this web server, where decryption takes place on the web server itself, and the private key is only sent when needed and is stored on the HSM at all other times.

DNS SECURITY

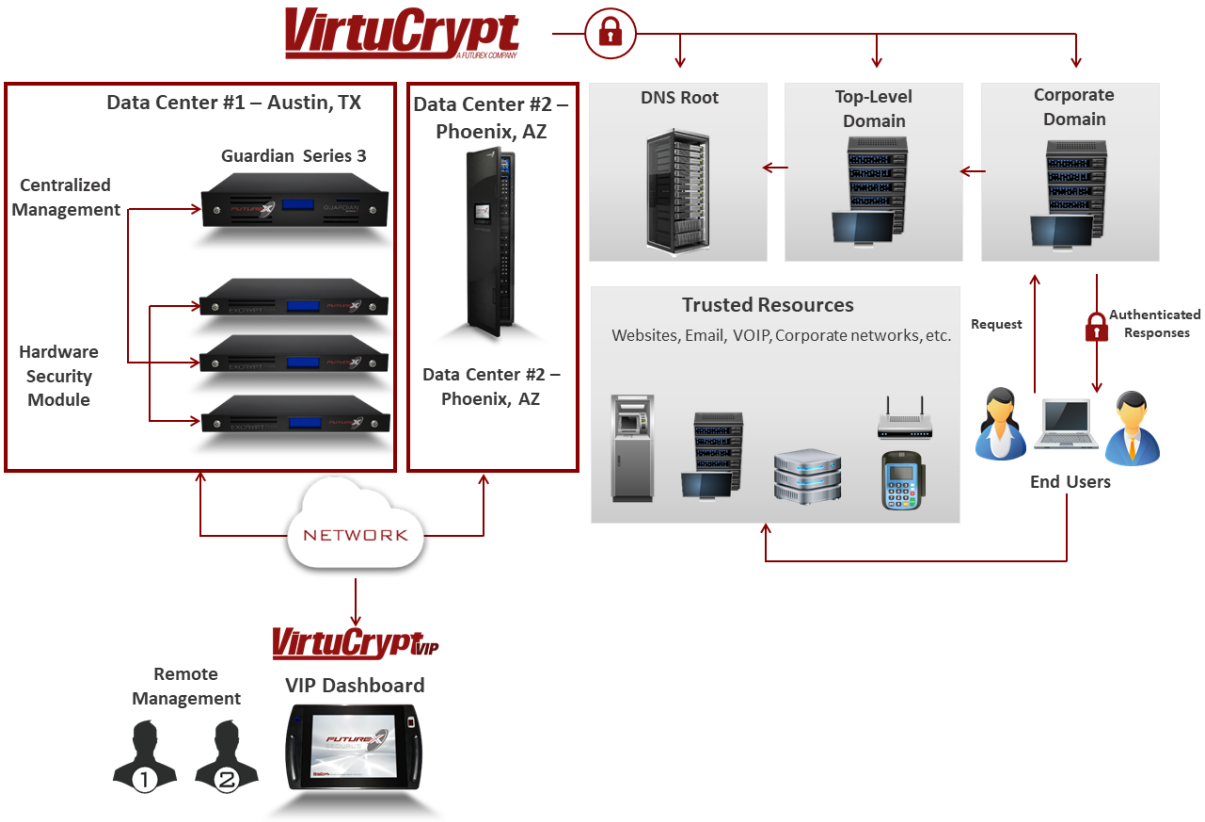
The Domain Name System, or DNS, is critical to modern usage of the Internet. DNS servers, whether public-facing or internal to a corporate network, assign human-readable names to IP addresses and enables communication between users across the network. However, DNS is vulnerable to a number of attack vectors. To remedy these, the Internet Corporation for Assigned Names and Numbers (ICANN) proposed DNSSEC, a security protocol that creates a chain of DNS servers that have been digitally signed by hardware security modules for the purpose of mutual authentication.

Attack Vectors Mitigated by DNSSEC

1. *Man-in-the-Middle: most commonly used for data eavesdropping and corporate espionage, this attack routes connections through a proxy and back to the intended destination, with particular effort to avoid detection.*
2. *Cache Poisoning: a form of man-in-the-middle attacks, cache poisoning involves false records being inserted into DNS servers, directing traffic to, or through, malicious domains.*
3. *Denial of Service: attackers overload DNS servers with requests, in an effort to render domains inoperable.*
4. *Fast Flux Hosting: networks of compromised DNS servers are used to mask the source of botnets, spam, malware distribution, and other criminal activity by routing them through proxies.*

DNSSEC applies to more than just websites, it applies to e-mail, corporate networks, Voice over IP infrastructure, and more. By implementing DNSSEC, organizations can guard against some of the most significant, and sophisticated, attack vectors. This includes man-in-the-middle attacks, cache poisoning, denial of service, and fast flux hosting, all of which are defined in more detail below. Simply put, without authenticating DNS, critical gaps in network security existing, creating a platform from which to launch other attacks or engage in corporate espionage.

Using hardware security modules to establish the trust domain is the most secure method of implementing DNSSEC. BIND, the most commonly used DNS software package, supports DNSSEC using OpenDNSSEC, which can use the PKCS #11 cryptographic library to interface with Futurex hardware security modules. After BIND and OpenDNSSEC are installed and configured, the setup process for enabling DNSSEC involves configuring the Futurex HSM and optional VirtuCrypt cloud services, and placing Futurex's PKCS #11 library in a defined location on the DNS server along with a configuration file defining environment-specific variables.



Example DNSSEC Architecture, Incorporating the Futurex Hardened Enterprise Security Platform and VirtuCrypt Cloud Services.

MESSAGE AUTHENTICATION AND DATA INTEGRITY

Message authentication and data integrity are two interrelated yet different concepts, each with the goal of preventing man-in-the-middle attacks. Message authentication is a method to ensure the origin and identity of the sender, whereas data integrity applies to the contents of the message and whether it has been altered. This can be achieved through digitally signing data, or creating a HMAC. The objective of these operations is to verify the authenticity and integrity of the data.

DIGITALLY SIGNING DOCUMENTS

With the increasing prevalence of eGovernment around the world, electronic signatures have become increasingly important in the way business is conducted internationally. Many countries have established regulatory requirements mandating the transmission of invoices and tax documents online, and for enterprises doing business in these countries, it is important to ensure the integrity and authenticity of the messages being transmitted.

Using the RSA algorithm, an HSM can send messages encrypted under a public key infrastructure (PKI). A document is digitally signed using the originating organization's private key, and then encrypted with the destination entity's public key. This signature ensures the recipient can authenticate the source of the message. The document is then sent to its intended destination where it can be validated using the originating organization's public key, and subsequently decrypted by the destination's private key. Following this, the message can then be read or validated as intended.

DIGITALLY SIGNING E-MAILS

Modern enterprises are often almost entirely dependent upon electronic means of communication. Some of an organization's most sensitive information is transferred daily through its various e-mail channels. What is preventing this e-mail from being intercepted and read or altered in some way? In many organizations: nothing. A hardware security module can be used to digitally sign e-mails, ensuring the integrity and authenticity of the message have been maintained. This is achieved through a similar method of signing the documents mentioned in the previous section, with the signing of the e-mail and attachments using the sender's private key and verified using their public key.

DATABASE ENCRYPTION

Many organizations require storage of vast repositories of data. Healthcare organizations must store millions of patient records, universities store academic research and student records, and retail organizations must store the transaction records of customers to be able to conduct customer returns or void transactions. Storing records in clear repositories makes them high-value targets for criminals. In some industries, individual records hold a street value in the hundreds of dollars. Negligence falls on the other end of the spectrum. Sometimes the hardware these databases are stored on can be inadvertently lost or can be disposed of improperly, exposing sensitive information to anyone who could casually gain access to them.

For these reasons, it is important to encrypt data while it is at rest. Some databases support encryption using a standards-based library such as PKCS #11 that is linked with an HSM so that data entering the database for storage may be encrypted and only decrypted when access is needed. Futurex supports seamless integration with SQL servers, Oracle databases, and open source databases.

Microsoft SQL introduced transparent data encryption (TDE) in 2008 to provide an alternative to granular cell-level encryption. Transparent data encryption, as the name suggests, is entirely transparent to the user. It provides complete protection for the database without negatively affecting existing applications. Simply put, TDE encrypts the entire database so that database functions such as queries remain fully functional. All data types can be fully accessed without lessening security, unlike how data is handled in cell-level encryption. For added security, TDE provides transaction logs and backups of data.

Cell-level encryption provides strict user controls, including permissions and key management. However, encryption functions must be performed manually. In this form of database encryption, data is decrypted only when manually called upon for usage. Due to the use of salt, data values are also slightly altered after they are encrypted for additional security.

Integration between Futurex HSMs and Microsoft SQL is enabled by the EKM library, which is available for Futurex HSMs. First, users customize the configuration file to meet the specifics of the HSM (IP address, port, and so forth). Afterwards, users register Futurex as the EKM provider in Microsoft SQL. After these steps, users can create or delete keys for use with database encryption. Futurex, as an EKM provider, allows for the keys to be maintained on the HSM,

where it is stored within a FIPS 140-2 Level 3-validated cryptographic module. It is only brought to the database server to actively perform encryption and decryption functions.

APPLICATION ENCRYPTION

Application encryption protects information in the most detailed manner possible, and it is considered among the best forms of protection for data. As the title suggests, application encryption processes data on the application layer. It does not encrypt all elements of the application, but it covers only the information it knows to be proprietary. During encryption, the application provides logical protections, such as access to the data on the basis of user role and on the principle of least privilege. Additionally, the devices provide physical protection, offering a safeguard against and immediate notification of tampering. By utilizing an HSM for application-level encryption, organizations free their applications to perform at a higher capacity.

FINANCIAL APPLICATIONS

TOKENIZATION

Tokenization, a technique for reducing the scope and cost of PCI DSS requirements, is a process by which a token, or a string of characters that represent sensitive data, is generated using a mathematical function. The token then replaces all, or nearly all, instances of sensitive data stored within the merchant system, thereby limiting the risk of data breach while retaining the functionality needed by a variety of business processes. Two common methods to achieve this end include using a hash-based Message Authentication Code (HMAC) or encrypting the data directly.

In a hash-based MAC approach, data is put through a hashing algorithm, resulting in a string of identifying information used to verify the integrity and authenticity of data. These tokens are used by both the merchant and the host in the place of the original sensitive data. Both the clear cardholder data and the matching HMAC-derived tokens are stored in the host's secure database for recall in case they are needed, such as for returns or refunds. The merchant only stores, and has access to, the tokens, which cannot be reversed to derive the original cardholder data.

For the encryption method of tokenization, the host and the merchant are completely removed from the burden of storing cardholder data in the clear. All sensitive data is processed inside the hardware security module. Unlike the HMAC-derived tokens, the encryption-created tokens can be decrypted and detokenized.

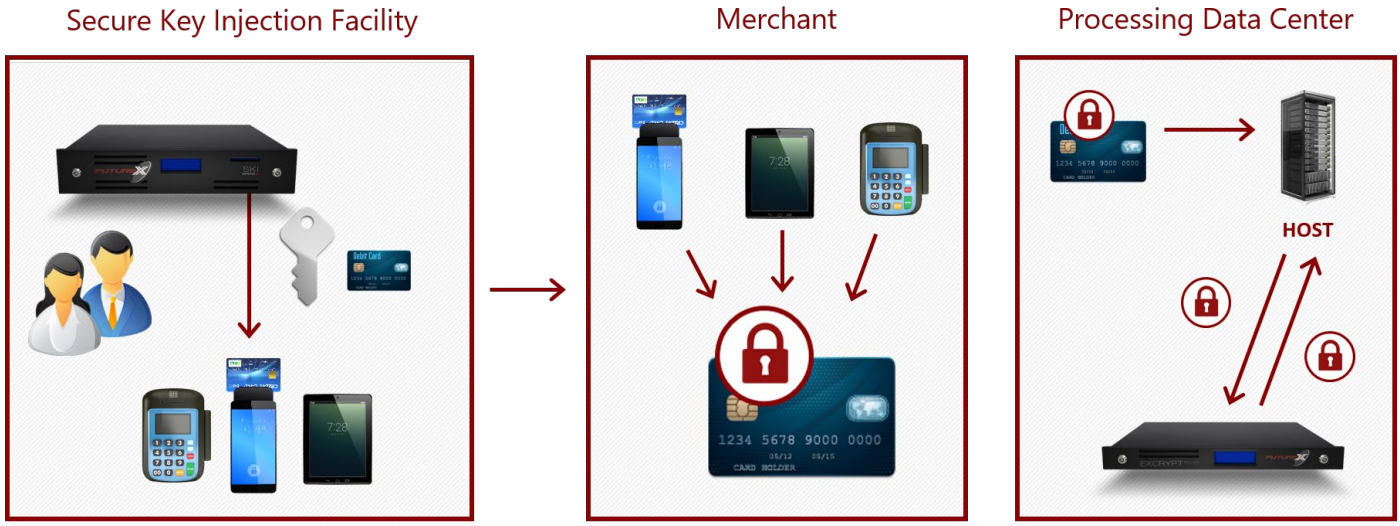
POINT-TO-POINT ENCRYPTION

Point-to-Point Encryption, also known as P2PE, is a robust technique for encrypting data from the moment which cardholder data is captured until it has entered the secure network of the transaction processor. Sensitive cardholder data, which includes the Primary Account Number (PAN), is initially encrypted at the point of interaction. The encrypted data is sent to the transaction processor, where it is decrypted within the confines of a hardware security module, and then is sent to the card issuer for validation. To meet your organization's specific needs, Futurex HSMs support both 3DES and AES encryption algorithms.

P2PE is advantageous because it eliminates clear text PAN data from unsecured communication lines, reducing the scope and cost of PCI DSS compliance and providing a high level of security for organizations transmitting cardholder data. Conventionally, organizations have secured their infrastructure behind their firewall between the host and acquirer but this method does not do enough to protect cardholder information in transit. Without P2PE, sensitive cardholder data is often transmitted in clear text format.

POINT-TO-POINT ENCRYPTION: HOW DOES IT WORK?

- Cardholder data encryption keys are injected within a secure facility.
- Payment terminals, deployed at merchant sites, encrypt cardholder data at the point of interaction.
- Encrypted cardholder data is securely decrypted by the hardware security module.



The PCI Security Standards Council has established six core requirements that P2PE solutions should cover. Since Futurex's Secure Cryptographic Devices (SCDs), which provide the cryptographic capabilities of the HSM, are FIPS 140-2 Level 3-validated, organizations can use them to adhere to a number of requirements, often reducing the scope and cost of PCI compliance.

SECURING ONLINE TRANSACTIONS

An incredible amount of commerce has moved to online retail sites which are also susceptible to fraudulent transactions. In an effort to increase security and curtail fraudulent transactions, a security protocol called 3-D Secure has been adopted by the major credit card brands. Customers are required to enter a value tied to the use of the credit card at the time of the transaction. This value acts like a PIN in debit card transactions as an additional authentication step.

A hardware security module must be used both to generate this value for the card issuers and to validate the transactions. Like PIN issuance, however, 3-D Secure requires a dedicated hardware security module.

PIN ISSUANCE AND PRINTING

In instances where customers need to obtain their debit card PIN but cannot appear at a bank branch in person, their PIN can be securely printed and mailed to their location. PIN printing allows debit card issuers to print PINs directly and securely from a hardware security module. Solutions involving PIN printing should be compliant with PCI PIN Transaction Security requirements, and as these regulations mandate, the PIN printing function must be carried out on a dedicated, single-purpose HSM.

PREPAID CARD ISSUANCE

Employees spend an increasing amount of time at work, and some enterprises are large enough to rival the size and complexity of small towns. For the convenience of these groups as well as the benefit of the organization, closed-loop prepaid cards provide an ideal, mutually beneficial solution. Prepaid cards can be loaded with funds for use in the cafeteria, vending machines, or other monetary exchanges, and periodically reloaded with funds for repeated use.

EMV CARD ISSUANCE AND TRANSACTION PROCESSING

Payment card fraud is an increasingly troubling issue for acquirers, issuers and merchants. In 2014, losses of $16.31 billion were reported, a 19 percent increase from 2013. For issuers, counterfeit cards presented at the point of interaction are the main source of losses; for merchant and acquirers, losses occur as a result of fraudulent card-not-present transactions.[6]

EMV card technology has proven effective at deterring fraud and increasing security. EMV stands for Europay, MasterCard, and Visa and is a global standard for chip-based debit and credit card transactions. EMV cards, also known as smart cards, are embedded with a micro processing chip. Smart cards guard against the use of counterfeit cards which are produced inexpensively by criminals who either “skim” card numbers from Point of Sale terminals or purchase large quantities of valid card numbers on the Internet. EMV reduces fraudulent transactions because even if the account data is stolen, it cannot be used to create a duplicate card due to the secure nature of the embedded smart card chip.

An HSM can be used in the issuance of EMV smart cards as well as the processing of EMV transactions. It is essential for a compliant hardware security solution be integrated into smart card-based payment systems to protect the encryption keys needed to validate transactions. EMV cards support Public Key Infrastructure, a two-key encryption system that has been used for many years to provide critical security services for online banking, secure VPN connections, and more.

Validation occurs when EMV cards, used in online mode, and a transaction processor communicate with an HSM to authenticate the cardholder prior to transaction approval.

CONCLUSION: PUTTING IT ALL TOGETHER

It’s important for system administrators to pursue a holistic approach when developing a plan for their cryptographic infrastructure. Investment in an HSM is not a decision to be taken lightly; a best-in-class HSM will be a significant purchase, however if industry experts are consulted during the decision process, an organization can significantly improve the return on their investment.

An industry expert, one with training certifications such as CTGA (Certified TR-39 Auditor), as well as hands-on experience, will be able to see your organization through the same lens an auditor would. A trusted advisor can bring significant experience of how other organizations in the same industry have implemented solutions, and how your cryptographic solution can be specifically tailored to your unique infrastructure.

The very same expert will be able to provide invaluable advice in developing versatile core cryptographic infrastructure that achieves additional business goals beyond simply fulfilling regulatory compliance mandates. A hardware security module is effective in reducing the risk of a breach, but cannot succeed without the proper management of information and people. An old industry axiom states that, "security is a combination of information, people, and technology." All three facets must be properly managed in order to create a secure environment.

Have you considered what other functions your hardware security module can fulfill? Are you using other services to sign your documents or are you considering other encryption methods for your databases? A hardware security module can easily integrate into your current infrastructure and considerably increase the security of your IT ecosystem.

About Futurex

For over 40 years, Futurex has been a globally recognized name in providing secure, scalable, and versatile data encryption solutions. More than 15,000 organizations worldwide have trusted Futurex's Hardened Enterprise Security Platform to provide innovative, first-to-market solutions for the encryption, storage, and transmission of sensitive data.

SOURCES

1. McCallister, Erika; Grance, Timothy; and Scarfone, Karen. “NIST Guide to Protecting the Confidentiality of Personally Identifiable Information.” NIST SP - 800-122. 6 April 2010.

2. “2016 Data Breach Investigations Report.” Verizon Enterprise Security. Apr. 2016.

3. “Chronology of Data Breaches.” Privacy Rights Clearinghouse. Sept. 2016.

4. Khrennikov, Ilya. “Hackers Found Selling Access to 70,000 Company Computer Systems” Bloomberg Technology. 15 June 2016.

5. “2015 Data Protection and Breach Readiness Guide.” Online Trust Alliance (OTA). 16 May 2015.

6. “Global Card Fraud Losses Reach $16.31 Billion.” The Nilson Report. 15 Aug. 2015.

FUTUREX ENGINEERING CAMPUS
OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163