ENCRYPTION CONSULTING

HSM-as-a-Service

HSMaaS

Encryption Consulting's HSMaaS

The HSM as a Service from Encryption Consulting offers the highest level of security for certificate management, data encryption, fraud protection, and financial and general-purpose encryption. It is globally compatible, FIPS 140-2 Level 3, and PCI HSM approved.

Encryption Consulting's HSM-as-a- Services are suitable for:
- Customers who already have HSM deployed in place.
- Customers who are planning for new HSM infrastructure (Designing and Deploying)

Encryption Consulting's HSM-as-a-Service offers customizable, high-assurance HSM Solutions (On-prem and Cloud) designed and built to the highest standards. We are Vendor- agnostic and provide various options, whichever is best for you to deploy. We ensure Highest Availability around the world and supply our services across the globe.

As a vendor agnostic organization, we have plenty of options for HSMaaS:

A. Entrust N-shield HSM

• nShield HSMs provide a secure solution for generating encryption and signing keys, creating digital signatures, encrypting data, and more. N-shield as a Service gives the advantages of a cloud service deployment together with the same features and capability as on-premises HSMs.

B. Thales Luna 7 HSM

• Thales Luna Network HSMs secure your sensitive data and critical applications by storing, protecting, and managing your cryptographic keys with high-assurance, tamper-resistant, network-attached appliances offering market-leading performance.

C. FutureX HSM

• Futurex hardware security module solutions provide robust encryption, tamper resistance, and logical security to safeguard your most sensitive data. Key lifecycle management, payment encryption, and general encryption are all handled by Futurex HSMs.

Introduction of how HSMs work:

A Hardware Security Module (HSM) is a specialized, standards-compliant cryptographic device that uses physical security measures, logical security controls, and strong encryption to safeguard sensitive data while it is in use, in transit, and at rest. Encryption, which makes sensitive data incomprehensible to everyone but authorized receivers, is at the foundation of an HSM's functioning. HSMs also provide a safe mechanism to decode data, ensuring the secrecy and validity of messages. The keys used for encrypted communication between devices within a Secure Cryptographic Device (SCD) are generated and stored by hardware security modules, which are much more secure than just software.

HSM as a Service

Making access to cryptography as a service accessible and efficient.

Key points:

• Scalable and flexible enterprise solutions can be implemented either on-premises or in the cloud.

• Regardless of where application workloads are occurring, maintain total control over crucial materials.

• Utilize hosted and managed HSMs while deploying to the cloud.

• Leveraging numerous clouds to expand cloud-based cryptography and key management.

• Using performance-based pricing to satisfy urgent security needs can streamline budgeting.

• Lowers the administrative burden of maintaining and managing things.

• With a single click, services may be automatically scaled.

About Cloud HSM

"Cloud-first" is a typical strategy objective of many firms in today's fast-moving enterprise IT landscape. Organizations that migrate to the cloud have access to the scalability, flexibility, and resilience a cloud service provider may offer, as well as decreased maintenance requirements and more stable monthly operational costs. The time when businesses automatically hosted their vital IT infrastructure on- premises is not much in trend nowadays. When cloud apps rely on hardware security modules (HSMs), physical devices that guard the cryptographic keys that serve as the foundation of trust for an organization's encrypted data, this shift in business practices creates friction. HSMs are typically kept in on-site data centers and are controlled by on-site security staff. They are a vital component of a company's key infrastructure and assist clients in meeting regulatory or certification requirements. Finding qualified security personnel to manage HSMs is a continuous challenge given the rising demands on company security teams.

Key Benefits of HSMaaS:

i. Designed to your specifications: We deploy the HSM formatted to your exact specifications, ensuring it meets all necessary compliance and business requirements.

ii. Compliance: Hardware Security Modules (HSMs) help fulfill many different compliancy requirements, including FIPS and PCI DSS.

iii. Features for auditing: Comprises necessary audit skills.

iv. Enforces policies as needed: Provides Capability to create and apply rules to gurantee compliance.

With the advantages of a cloud service deployment, Encryption Consuling's HSM-as-a Service offers the same capabilities and functionality as on-premises HSMs. This enables customers to achieve their cloud-first goals while leaving the management and up keep of these appliances in the hands of Encryption Consulting's professionals.

Advantages over others:

a) Delivers security of keys that is FIPS 140-2 Level 3 and eIDAS certified, which is not generally available widely with some cloud key protection solutions.

b) Provides customers a dedicated HSM service that ensures they have complete ownership over their cryptographic keys, and complete job separation ensures that no person may unilaterally change key use restrictions.

c) Supports hybrid cloud deployments and provides simple key migration if on-premises data repatriation from a cloud service provider is necessary.

d) Makes sure customers are in control of their Secrets and keys and can use them throughout their HSM environment, whether on-premises or as a service.

e) Enables clients to move and expand their secure code execution from an on-premises HSM to the cloud on-demand.

EC Managed HSMaas Elements:

Encryption Consulting LLC (EC) will completely offload the HSM environment, which means EC will take care of deploying the HSM environment to lead and manage the HSM environment (cloud/ hybrid or On-Prem) of your organization. EC deploys your HSM environment in a "one subscription fee model." Below are the managed service elements EC offers with our one subscription fee model.

Service Elements	Basic	Extended	Advanced
Key Management Key Management for users/devices, Key backup/ recovery/archival	X		
HSM Operations Management Modifying/updating templates for documentation, policy, and procedures in regard to the HSM	X		
Backup and Restore Backup of good configuration at a regular frequency, Maintaining the backups safely/securely	X		
Patch Management Fixing security vulnerabilities through patch/hotfix upgrade to enhance functional/non-functional feature	X		
Technical/Customer Support Efficient and timely support for 24'7'365 to avoid any service disruptions	X		
Auditing Audit logs/functional logs available on-demand		X	
HSM Support Infrastructure Management Full length support for the entire HSM Infrastructure including single tenant/dedicated Systems for HSM services		X	
Integration with Other Business Applications HSMaaS integration with key enterprise applications (AD, CTM, CCC, etc.)			X
Testing & UAT sign off Provide the test environment to test the applications integration with the HSMaaS solution			X
Major Software Upgrade Software version upgrades up to N-1 of managed HSM systems where N is latest version available from vendor			X

Why Encryption Consulting LLC?

ENCRYPTION CONSULTING
www.encryptionconsulting.com

Encryption Advisory Services

Encryption is used for securely protecting data from unauthorized access. Data encrypted can only be seen by those that possess the key to change the data back to plain text. Encryption is now one of the oldest yet still most effective technology solutions able to have data security for organizations.

Public Key Infrastructure

PKI is a security ecosystem that has stood the test of time for achieving secure Internet-based transactions by the use of digital certificates. Digital certificates have provided security to servers and routers from the very early stages of the Internet through Public Key Infrastructure

Hardware Security Module – HSM

Hardware Security Modules provides protection and strong authentication with cryptographic processing by the use of digital keys inside a physical computing device. This device offers an isolated tamperproof environment which can create and secure cryptographic keys, protecting critical cryptographic operations, all while enforcing self-implemented policies over the keys.

Certificate Lifecycle Management

Certificates typically have a 4-phase lifecycle - Discovery, Enrollment, Provisioning, and End-of-life. To make your PKI mature and reliable, you must have more control over all the phases

Enterprise Encryption Platforms

Does your business have the need to encrypt large amounts of data-at-rest found in structured databases or in unstructured files across physical, cloud, or both types of environments? Do you want to protect data without disruptive changes to applications or business practices?

Cloud Data Protection Services

The transition towards uploading data on the public cloud is now becoming the normal standard. With relying on the cloud for data storage, cloud security must now become the number one priority for organizations

See it in action

Encryption Consulting LLC is a customer-focused cyber security consulting firm providing an array of services in all aspects of data protection.

Contact Us

encryptionconsulting.com

linkedin.com/company/encryptionconsulting

facebook.com/encryptionconsulting

twitter.com/encryptioncons