DTS

Hardware Security Module (HSM)

Hardware Security Module (HSM)

Do you know what a hardware security module (HSM) is? An HSM is a dedicated crypto processor specifically designed to protect encryption keys throughout their lifecycle. HSMs act as trust anchors. They protect the cryptographic infrastructure of some of the world's most security-conscious organizations by managing, processing and storing cryptographic keys in a highly secure, tamper-proof appliance. In this way, it is possible to ensure reliable protection for transactions, identities and applications, because not only the cryptographic keys are protected, but ultimately also services for encryption, decryption, authentication and digital signing.

- Protection of encryption keys over the complete lifecycle

- Extremely secure, tamper-proof, network-bound, high-performance appliance

- Storage, management, processing & protection of cryptographic keys

- Security for transactions, identities & applications or encryption, decryption, authentication, digital signing

Protect your sensitive data and critical applications by storing, protecting and managing cryptographic keys in Luna network hardware security modules. The extremely secure, absolutely tamper-proof and network-bound, high-performance devices are unparalleled on the market. Network connectivity allows them to be easily integrated into numerous applications to accelerate cryptographic operations. You protect cryptographic keys throughout their lifecycle, for your entire encryption infrastructure.

Applications of the HSM:

- PKI key creation & storage (online and offline CA keys)

- SSL/TLS

- Code signing

- Certificate validation & signature

- Document signature

- HSMaaS – environment for public & private clouds

- Transaction processing

- Database encryption

- Smartcard output

- Trusted IoT hardware base

- Blockchain

- Compliance with GDPR, PCI-DSS, HIPAA, eIDAS/IVT, etc.