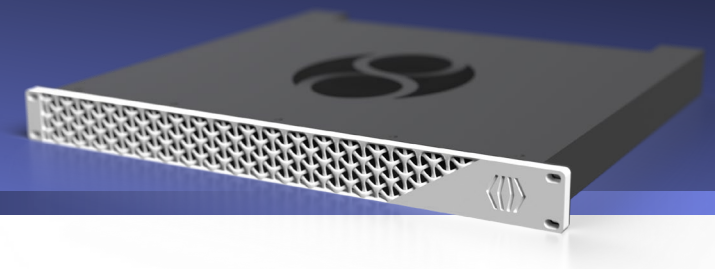
IDEMIA

SPHERE

Hardware Security Module

Scalable
Versatile
Energy efficient

Unlock the power of a first-of-its-kind Secure Element-based Hardware Security Module designed to support multi-domain use cases with unparalleled efficiency, security, and adaptability.



Solution overview

IDEMIA Sphere HSM transforms traditional Hardware Security Module (HSM) design. Its distributed architecture based on a matrix of Secure Elements (SEs) eliminates the limitations of traditional monolithic Hardware Security Modules that rely on a single crypto-processor. Each Secure Element is a tamper-resistant microcontroller that both protects cryptographic keys and performs cryptographic functions. This unique architecture translates into practical advantages.

Parallel processing: The matrix of SEs allows multiple operations to be processed in parallel, overcoming the sequential limitations of legacy HSM.

Hardware-level isolation: Each SE provides an independent security boundary. This hardware isolation allows to implement segregated key domains within the same HSM.

Flexible security domains: The architecture supports allocation of independent SEs to different applications, customers, or trust domains.

Key benefits

Reduced TCO*

Reduces upfront, support, and operations costs (including energy consumption) and allows to pay as you grow.

Scalability

Supports millions of keys and high transaction loads without frequent upgrades, hardware replacements, or architectural changes.

Versatility

Delivers parallel cryptographic operations, built-in hardware multitenancy, and versatile use-case support.

*Total Cost of Ownership

Main features

Unlimited key storage
IDEMIA Sphere HSM security architecture enables virtually unlimited key capacity, centrally managed and distributed across an HSM cluster. It supports active clustering with both load balancing and automatic failover.

Energy-efficiency
With a maximum power consumption of 50 W per appliance, IDEMIA's HSM consumes less than half the energy of traditional legacy HSMs. This efficiency reduces electricity costs and lowers environmental footprint in the data centers where it is deployed.

Versatile cryptographic capabilities
This single, converged HSM delivers a unified solution for every critical cryptographic requirement from secure key lifecycle operations and TLS offloading to managing Public Key Infrastructure (PKI), certificate authorities, and code-signing.

Secure by design
IDEMIA HSM has achieved top-tier security certifications, including FIPS 140-3 Level 3. These certifications confirm that it meets stringent global standards for cryptographic key protection, supporting compliance mandates across various industry verticals.

In-field performance upgrades
IDEMIA Sphere HSM allows additional performance licenses to be activated remotely, enabling higher performance levels without replacing hardware.

Post Quantum readiness
IDEMIA Sphere HSM is designed to withstand the threats of quantum computing and ensure data remains secure well beyond today's standards.

Sovereignty
Engineered, designed, and pre-configured in France (EU), IDEMIA Sphere HSM ensures customers complete sovereignty and transparency for mission-critical systems, aligning natively with EU data-protection and security directives. It allows full control over cryptographic infrastructure and keys, reducing exposure to risks.

Technical Specifications

Asymmetric algorithms	〉RSA (KeyGen, SigGen, SigVer, Signature Primitive – FIPS 186-4) 〉Diffie-Hellman 〉ECDSA(NIST, Brainpool & secp256k1 curves) 〉KAS-ECC (SP800-56A Rev. 3) 〉KDF (SP800-108)
3G/4G/5G algorithms	〉TUAK and MILENAGE
Symmetric algorithms	〉AES - CBC / CMAC / ECB / GCM / CTR / CCM 〉TDEA (3DES)** 〉HMAC, SHA-1 HMAC, SHA-224, HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC
Supported hash and message digest algorithms	〉SHA-1, SHA-2 (224, 256, 384, 512 bit), SHA-3 (224, 256, 384, 512 bit)
Supported platforms	〉Windows 〉Linux
Application Programming Interfaces (APIs)	〉PKCS #11 〉RESTful API 〉OpenSSL 〉Cryptographic High Level Frame Interface (*)
Host connectivity	〉1U Rack-Mount Appliance: 2 Gigabit Ethernet port 〉Desktop Appliance: 1 Gigabit Ethernet port
Appliance / Form Factor	〉Desktop Appliance 〉1U Rack-Mount Appliance
Power consumption	〉Desktop Appliance: 20 W (energy-efficient for office environments) 〉1U Rack-Mount Appliance: 50 W (optimized for data center deployment)
Certifications	〉FIPS 140-3 level 3
Operating temperature	〉IEC 60068-2-1, 2-2 (-10°C to +70°C)
Storage temperature	〉IEC 60068-2-1, 2-2 (-40°C to +85°C)

(*) Proprietary interface based on High Level HSM frame to optimize parallelization of the request. This Services may be completed based on your needs
(**)Only allowed in non-strict FIPS mode

Why IDEMIA Secure Transactions?

Backed by decades of expertise in security solutions, IDEMIA Sphere HSM delivers robust protection, scalability, and long-term data security, empowering organizations to confidently navigate the challenges of today's digital landscape, including post-quantum migration, advanced cyberattacks, and evolving regulatory requirements. Learn more about IDEMIA Secure Transactions' cybersecurity offer here.

1.4B+
physical & digital credentials protected by cryptography every year

6M+
cards personalized by Sphere to date

1st
company to announce a crypto-agility solution for post-quantum

IDEMIA SECURE TRANSACTIONS