trustway proteccio netHSM

TrustWay Proteccio is a hardware security module (HSM) providing software solutions with a high-performance and highly secure environment where they can carry out their most sensitive cryptographic operations.

The combination of its physical security equipment and a cryptographic core that is subject to the strictest security requirements brings one of the most certified cryptographic modules in the world to company information systems and cloud services.

With its simplified implementation designed for autonomous deployment, critical environments get an optimum solution for unconditional security of their sensitive data at the most competitive price.

Certified cryptography

TrustWay Proteccio manages all sensitive cryptographic operations of security applications (PKI, signature, eID, encryption, etc.).

Its 100% European architecture provides the most secure cryptographic implementations, based on over 20 years of research and development in France and subject to the most demanding international certifications.

Already deployed in the most critical environments (operators of critical infrastructures, defence, energy, telecommunications), TrustWay Proteccio ensures that national agencies and companies have the reliability of state-of-the-art architecture and the robustness of a product designed to meet the strictest security requirements in the world as closely as possible.

Resource optimization

Due to the strong partitioning offered by TrustWay Proteccio, the same equipment can be used securely by several distinct applications.

A single HSM can therefore be used by different security applications independently of each other, providing the same level of security and compliance as the operation.

High availability and optimized performance

The sharing of TrustWay Proteccio HSMs in network clusters allows secure cryptographic pools to be created that benefit from a native load distribution and automatic key replication.

Each pool can be accessed transparently by software applications without any modification to their source code.

The combination of strong partitioning and native clustering gives architects and administrators an unprecedented degree of flexibility that permits customised sizing and an optimal response to specifications for infrastructure and performance.

Ease of installation and administration

TrustWay Proteccio HSMs take care of all technical and security conditions inherent in the deployment and utilisation of hardware technology.

They have simplified administration procedures, significantly reducing the risks related to the deployment of cryptography and its use in the very long term by diverse teams.

TrustWay Proteccio HSMs, their partitions and the security policies to which they adhere are administered centrally by a unique application designed to guarantee technical independence and ease of use that are unique on the market

Bull
atos technologies

TrustWay Proteccio HSM at a glance

Certified security

The TrustWay Proteccio HSM is entirely designed, developed and made by Bull in France. It complies with the security assessments of the most demanding certification processes.

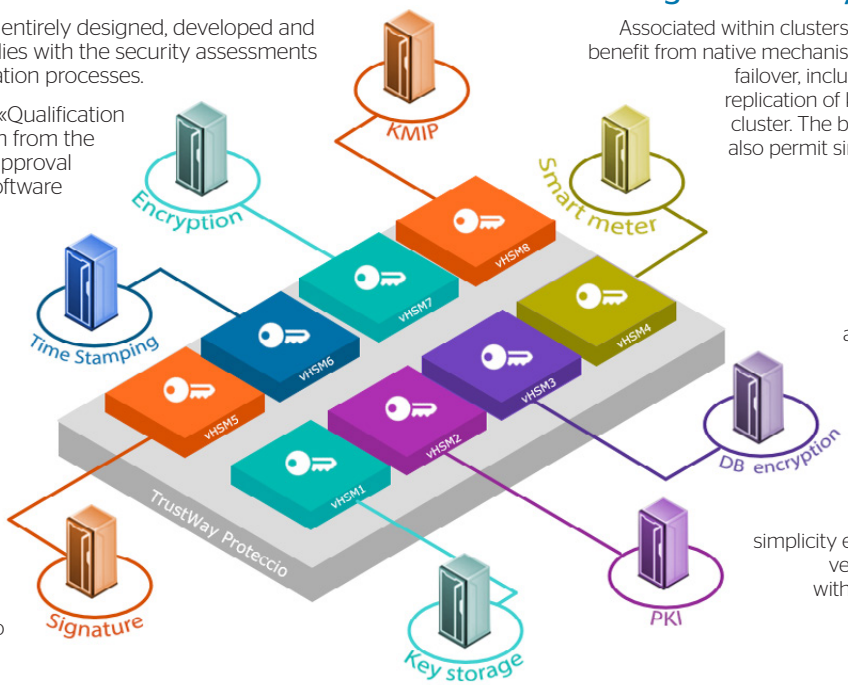
The certification CC EAL4+, the «Qualification Renforcée» (highest qualification from the ANSSI) and the NATO SECRET approval cover all of the hardware and software architecture.

Virtual HSM

Eight virtual HSMs can be used simultaneously in a single TrustWay Proteccio HSM.

Each virtual HSM is an independent, secure partition (access control, users, cryptographic operations, logs, auditors and administration).

This strong partitioning permits a physical HSM to be shared among various applications, while still benefitting from a level of security identical to the deployment of several pieces of equipment.



High availability, failover, backup

Associated within clusters, TrustWay Proteccio HSMs benefit from native mechanisms for high availability and failover, including automatic and secure replication of keys on all members of the cluster. The backup and restore features also permit simplified implementation of recovery plans

Administration

TrustWay Proteccio is fully administered from a simple and ergonomic graphical application.

Centralised operations for deployment, administration and audit within a single application known for its simplicity enables reliable, secure and very long-term management without specific technical skills.

Certifications

- Common Criteria EAL4+ compliant with CWA 14167-2-PP
- NATO SECRET
- Compliant with eIDAS
- «Qualification Renforcée» (the highest qualification from the ANSSI)
- FIPS 140-2 level 3 (in progress).

Algorithms

- Asymmetric encryption: RSA
- Symmetric encryption: AES 128 to 256, 3DES
- Electronic signature: RSA PSS, PKCS v1.5, ECDSA
- Hashing: MD5, SHA-1, SHA 256, SHA 384, SHA 512
- Supported named curves: ANSI, NIST, ANSSI and all curves up to 521 bits, including Brainpool curves.

Administration

- Cryptographic profiles definition
- Secure updates of embedded software
- Load balancing capability.

APIs

- PKCS#11
- OpenSSL
- Java Cryptography Architecture/Extension (JCA/JCE)
- Microsoft Crypto API (CSP), Cryptography Next Generation (CNG).

Interfaces

- 2 Ethernet 10/100/1000BASE-T ports
- 4 USB2 ports
- 1 VGA port
- Integrated keyboard and chip card reader
- Redundant electrical supply
- Restart button on the front
- Secure RPC over SSL to Windows, Linux and AIX 32/64 servers.

Performances

- Asymmetric: up to 1600 sign/s
- Symmetric: up to 200Mbits encrypted by second.

CT_170606_LPM_F-Proteccio_netHSM_en3

bull.com/cybersecurity-trustway-proteccio-nethsm

Trusted partner for your **Digital Journey**

Atos