

Trustway Proteccio OEM

Design your own Cryptographic Appliance



Trustway Proteccio OEM provides editors and integrators with an open and secure hardware platform for designing certified and scalable cryptographic appliances.

Load your operating systems and applications and benefit from the visual customisation of the Trustway Proteccio OEM module to market your own hardware security appliance.

The Trustway Proteccio OEM offer gives software security solutions a hardware environment that is unique in the world, providing unrivalled levels of security and freedom in the design of hardware security appliances.

The combination of a cryptographic core that is subject to the strictest international security requirements and a complete x86/x64 application environment within a unique hardware appliance offers OEM partners a simple and customisable environment that benefits from the most advanced physical and software security measures on the market.

Bring Your Own Software (BYOS)

Trustway Proteccio OEM offers a complete hardware base (x86-64, HSM) and a simplified procedure for integrating an operating system (OS) and an application.

Its cryptographic core accommodates a key that verifies the OS and the application at start-up and provides all cryptographic services necessary for the appliance.

As Trustway Proteccio OEM is provided as a white-label product with the option for visual customisation of the front, partners have unrivalled freedom to design their hardware security appliance.

The Atos factory in Angers, France, is responsible for the hardware manufacturing process, loading the software locked by the partner, the visual customisation and, if required, delivery to the end client.

All of the Trustway industrial processes are made available to the software publisher partners: designing hardware appliances has never been so accessible!

Certified cryptographic services

The cryptographic core offers all of the certified cryptographic services of the Trustway Proteccio HSM to the OS and the partner application via its standard interfaces.

The Trustway Proteccio OEM solution is particularly adapted to the design of the following types of hardware servers:

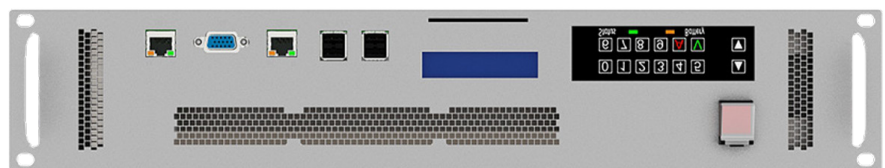
- PKI certification authorities
- OCSP responders
- Servers for eIDAS signature and timestamping
- DNSSEC servers
- Encryption appliances (email, databases)
- Platforms for CASB encryption/authentication
- Key Management Systems (KMS).

OEM development packs

- Secure web/application servers and Webservices.

The software publisher partner gets:

- A development platform (Trustway Proteccio Tuning Platform)
- A signature platform (Trustway Proteccio Code Signing Station).



Trustway Proteccio OEM at a glance

Certified security

The Trustway Proteccio HSM is entirely designed, developed and made by Atos 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), the EU RESTRICTED approval 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.

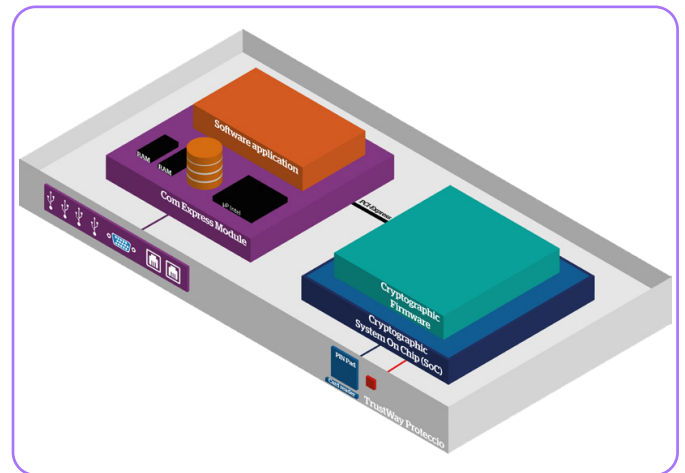
Administration

Trustway Proteccio is fully administered from a simple and ergonomic graphical application. A development station and a signature station are provided so that the software publishers can design the appliances.

Cryptographic appliance

Trustway Proteccio is the only HSM in the world offering an open hardware platform enabling software publishers to load a complete software environment (system and applications).

Beyond the security of the cryptographic operations that it provides, the Trustway Proteccio OEM permits the design of complete hardware security devices on the basis of a material platform provided by Atos as a white-label product that can be customised according to the graphical identity of the software publisher. Beyond the physical security equipment with state-of-the-art technology, the mechanisms for signature and verification of the code bring an unrivalled level of security to hardware appliances.



Characteristics

Certifications

- EU RESTRICTED
- 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.

APIs

- COM express module
- Intel Core 2 Duo or Intel i7 micro-processor, 2 Go or 16 Go
- Storage: 250 Go or 1 To.

Interfaces

- 2 Ethernet 10/100/1000 BASE-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.

For more information: atos.net/en/products/cyber-security/data-encryption/hardware-security-module-trustwayproteccio-oem-hsm

Atos is a registered trademark of Atos SE, November 2022. © Copyright 2022, Atos SE. Confidential Information owned by Atos group, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval of Atos.