INNOVATING FOR PROTECTION

TRIDENT HSM

first and only Secure Multi-party Computation capable HSM

info@i4p.com www.i4p.com

TRIDENT

MULTI-PARTY CRYPTO MODULE

LONG STORY SHORT

i4p's TRIDENT HSM is the first physical Hardware Security Module on the market, designed to apply Secure Multi-party Computation (SMPC) for Cryptographic Key Management. It can generate, sign and encrypt RSA key pairs in a revolutionary distributed manner. When configured in the most secure SMPC cluster mode, the secret key will never exist as a whole, on any device, neither at the moment of generation, storage or computing. Every device in the cluster merely stores one part of the key. When configured for the faster (so-called trusted dealer) method, one of the devices generates the key, splits it and then securely distributes the key parts to the other devices in the cluster before irrevocably erasing the whole key.

The signing or decrypting functions are executed on all or, depending on how the cluster is configured, on n-out-of-k devices separately, as the participating devices each use only that part of the key that they are entrusted with to store and protect. The end result of this unique procedure is nevertheless a standard RSA signing or decrypting operation, guaranteeing full compatibility with existing cryptographic services.

TRIDENT HSM DATASHEET

+36 1 700 1200 info@i4p.com www.i4p.com

HIGH AVAILABILITY ARCHITECTURE

Due to its distributed architecture, the TRIDENT HSM can meet even the most demanding availability and load balance requirements. When deployed in remote data centers, if necessary on different continents, it's as disaster-proof as an IT service can be, while still maintaining high signing speeds. Any of the clustered devices is independently capable of communicating with the outside world guaranteeing high availability and optimal load balance.

EASY INTEGRATION

i4p's TRIDENT HSM integrates seamlessly into existing TCP/IP network infrastructures and smoothly communicates with other network devices. The HSM crypto functionality can be utilized using the industry standard PKCS#11 library, OpenSSL, Java Cryptography Extension (JCE), Microsoft Windows Cryptographic Service Provider (CSP and CNG) or i4p's proprietary CMAPI interface. It can also communicate directly with security access modules (e.g. MIFARE SAM AV2) to enable quick and secure integration into ticketing ecosystems.

PROTECTED ENVIRONMENT

Every TRIDENT HSM comes equipped with an integrated Tamper Detection Module (TDM) with multiple sensors that constantly monitor the environment even when the device is not powered. The sensitivity of the TDM sensors can be configured to fit unique operating environments. Also, the TRIDENT HSM allows for unlimited local client applications (LCAs) to be installed into its protected environment. LCAs run in secure containers to ensure that they are isolated from other LCAs as well as from the HSM core. LCAs are created using the industry standard Linux Container Framework.

EIDAS COMPATIBILITY

The TRIDENT HSM has successfully attained its certification as a Qualified Signature and Seal Creation Device (QSCD) under EU Regulation 910/2014 on Electronic Identification and Trust Services (eIDAS). Thus, it enables Trust Providers to offer both Qualified and non-Qualified services, whether it is to generate, validate and preserve electronic signatures and seals, digital certificates and to satisfy the requirements of PSD2 (Open Banking), GDPR (Data Protection) and other current or future directives. All of this with an unparalleled high level of security.

CRYPTOGRAPHIC APIs

- PKCS#11 *
- OpenSSL **
- Microsoft CSP/CNG-KSP
- JCA/JCE Cryptographic Framework
- CMAPI (C++/Java, proprietary)

HOST INTERFACE

- Triple gigabit Ethernet port
- Dual USB port
- VGA display port
- Tamper detection I/O

CERTIFICATIONS

- CC EAL4+ (May 2019)
- eIDAS listing (August 2019)

CRYPTOGRAPHY

- Multi-party asymmetric algorithm: RSA, ECC
- Non-distributed asymmetric algorithms: RSA, ECC
- Other non-distributed algorithms: AES, TDES, DES, SHA256, SHA384, SHA512, SHA1, HMAC, CMAC etc.
- Post-Quantum algorithms: SPHINCS+
- Encryption/decryption scheme: PKCS#1, ECIES
- SAM key management: MIFARE*** SAM AV2

PHYSICAL CHARACTERISTICS

- Format: Standard 1.5U 19" rack mount chassis
- Dimensions: 19" x 21" x 2.58" (482.6mm x 533.4mm x 65.7mm)
- Weight: 19lb (8.5kg)
- Input Voltage: 24V DC (PSU 100–240V, 50–60Hz)
- Power Consumption: 120W maximum, 50W typical

* PKCS #11 Cryptographic Token Interface Profiles, an OASIS Standard
** OpenSSL is a registered trademark owned by OpenSSLSoftware Foundation
*** MIFARE is a registered trademark of NXP B.V.

MULTI-FACTOR AUTHENTICATION

Both local and remote users and administrators can (and we recommend should) use Multi-factor Authentication to access the HSM. Time-based One-time Password (TOTP) authentication according to RFC 6238 can be enabled for any administrators and users. Standard applications, like Google Authenticator, can be used to generate the TOTP codes.

COMMON CRITERIA CERTIFIED

The TRIDENT HSM has successfully attained Common Criteria EAL4+ certification (Evaluation Assurance Level EAL 4 augmented by AVA_VAN.5 and ALC_FLR.3 based on ISO/IEC 18045:2008) both under the Protection Profile for Cryptographic Module for Trust Services (EN 419221-5) as well as under the Protection Profile for QSCD for Server Signing (EN 419241-2) with strict conformance.