INNOVATING FOR PROTECTION

TRIDENT RSS

first one-vendor Remote Signature Solution with CC certified SAM & CM

info@i4p.com www.i4p.com

TRIDENT

MULTI-PARTY CRYPTO MODULE

LONG STORY SHORT

i4p's TRIDENT RSS is the first eIDAS listed Remote Signature Solution with the Signature Activation Module (SAM) coming from the same vendor as the underlying Crypto Module (CM).

For organizations who want to offer their clients, employees, partners and users convenient Remote Signature services without compromising on their security, this is the leanest solution with the lowest cost of acquisition and ownership. For Trust Service Providers planning to offer Qualified Remote Signing services, the only one-vendor solution that is both Common Criteria certified and eIDAS listed is indeed the TRIDENT RSS.

The SAM manages the users of the Signature Service, generates cryptographic keys for them, receives data-to-be-signed through an easily implementable Signature Activation Protocol and securely connects to the CM in order to have it manage the keys.

For the highest possible cryptographic security level, the keys can even be generated, stored and managed in an entirely distributed way using SMPC (Secure Multi-party Computation), another unique feature of our Solution.

TRIDENT RSS DATASHEET

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

CC EVALUATED AND EIDAS LISTED

The TRIDENT SAM has successfully attained Common Criteria EAL 4+ certification (Evaluation Assurance Level EAL 4 augmented by AVA_VAN.5 and ALC_FLR.3 based on ISO/IEC 18045:2008) meeting the requirements of the Protection Profile for QSCD for Server Signing (EN 419241-2) with strict conformance. The underlying CM (Crypto Module) is a Qualified Signature (and Seal) Creation Device (QSCD) under European Union Regulation 910/2014 on Electronic Identification and Trust Services (eIDAS). Thus, together they enable Trust Service Providers to offer both Advanced and Qualified Remote Electronic Signature Services and Remote Electronic Seal Services to Trust Service clients with the highest security and compliance requirements.

EASY INTEGRATION

The TRIDENT RSS comes with a lightweight engine for dealing with crypto processing and signature creating on-behalf of remote users without unnecessary system components in order to be easily inserted into existing signing solutions. The easy-to-use, proprietary SAMAPI provides all functions required for locally or remotely managing the SAM, while the SAP (Signature Activation Protocol) commands can be incorporated into any SIC (Signer's Interaction Component), whether it's one custom built according to a client's specific needs or a standard third-party application, like Acrobat Reader. For this industry standard APIs such as Microsoft CSP/KSP and PKCS#11 are used.

NOT ONLY FOR QTSPS

Although only Qualified Trust Service Providers (QTSPs) offering Qualified Services are obligated to operate a certified solution, we bring one within reach of many more TSPs and other organizations. Now anyone with a need for Remote Signing can build highly secure and convenient services based on our TRIDENT RSS.

WHY OUR 2-IN-1 SOLUTION IS BETTER

i4p is the first and as of yet only vendor to have developed both the Crypto Module and the Signature Activation Module components needed for offering Remote Signature Services, as opposed to having to buy them from separate vendors. For you this means a more consistent product philosophy, integration, management and support. The SAM can reside within the secure perimeter of a TRIDENT HSM (the CM) it uses for storing the signing keys. This solution is leaner compared to multi-vendor solutions. As a consequence, it has significantly lower cost of acquisition and ownership, dramatically improving your potential ROI.

APIs AND STANDARDS USED

- PKCS#11*
- Microsoft CSP/CNG-KSP
- OpenID Connect JWT identity tokens (RFC 7519)
- rsyslog (RFC 5424, 5425 and 5426)
- SAMAPI (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)

AUTHENTICATION

- Built-in multi-factor authentication module (RFC 6238)
- External authentication with JWT identity tokens (RFC 7519)

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

** In the TRIDENT RSS the SAM resides within the secure perimeter of the CM

MULTI-FACTOR AUTHENTICATION

The TRIDENT SAM enables both local and remote users to use multi-factor authentication in order to give the highest level of sole control assurance (SCAL2) to its users. Besides passwords, a Time-based One-Time Password (TOTP) mechanism according to RFC 6238 can be enabled for both administrators and users. The necessary TOTP codes can be generated using any standard application, such as Google Authenticator running on a smartphone. Other external authentication services can be used through OpenID Connect JWT identity tokens.

WHY WE UNDERSTAND YOU BETTER

Not all vendors are created equal. i4p informatics was founded by the former owners of NetLock, a Hungarian QTSP. During our time first as a System Integrator, later a TSP and eventually a QTSP, we became increasingly frustrated with existing cryptographic key management products and their suppliers. After a successful exit from NetLock, the decision was made to utilize our expertise and to found i4p, in order to create the best, most secure and user-friendly Cryptographic Solutions. The result is our family of TRIDENT products and solutions. Not only do we have a late-comer advantage, resulting in leaner solutions that are more efficient and easier to maintain. You will be buying from former colleagues, who exactly understand your needs, frustrations and pains. We look forward to helping you swiftly and successfully deploy your Remote Signing Services.