MOBILE-ID
Anytime, Anywhere

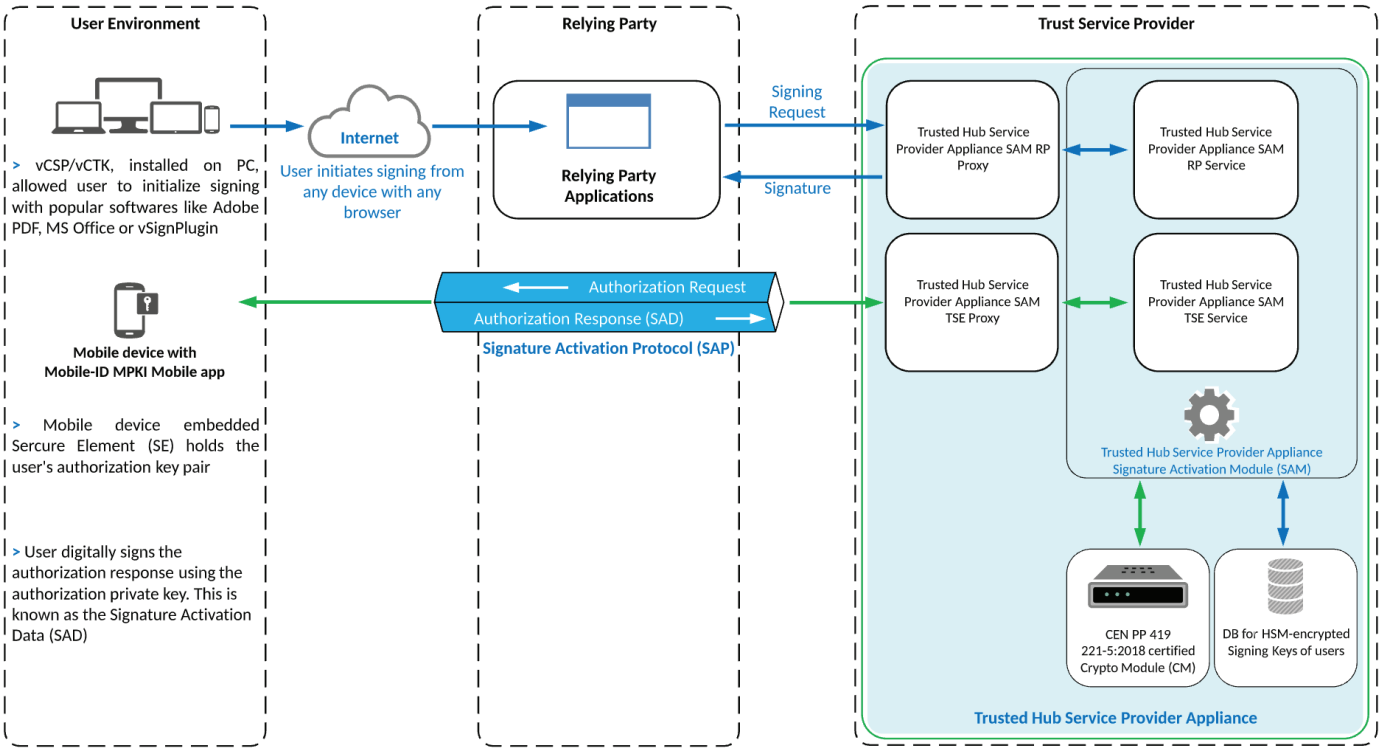
TRUSTED HUB

SERVICE PROVIDER APPLIANCE QSCD

What is the **Trusted Hub Service Provider Appliance QSCD**?

Designed specifically with Qualified Trust Service Providers (QTSPs) in mind, the Trusted Hub Service Provider Appliance QSCD enables remote signing services to be set up and offered to customers. Together with GoPaperless and Trusted Hub Signing Verification Server products, QTSPs are now able to provide fully hosted remote signing services or hybrid solutions, for example, where organizations require an on-premise front-end with a back-end hosted certified environment managing the PKI elements. Watch the video to find out more about Mobile-ID Remote Signing solutions or contact us for further details.

The eIDAS regulation (910/2014) and the new rules EN 419241-2 Protection Profile for remote signing requires that the highest levels of trust are used to ensure that user signing keys remain under the sole control of their owner. Mobile-ID™ created the Trusted Hub Service Provider Appliance QSCD and Mobille-ID MPKI Mobile App, leading the way and being first to market with a Common Criteria EAL4+ certified product which meets the EN 419241-2 Protection Profile – confirmation of providing the highest levels of assurance for Qualified or Advanced Remote Signing.



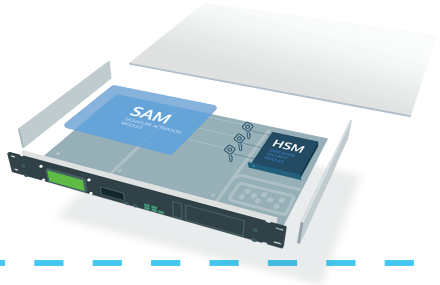
The common use cases for **Trusted Hub Appliance Service Provider Appliance QSCD** are:

- The first product to achieve Common Criteria EAL4+ certification against the eIDAS ETSI EN 419241 standard and the EN 419 241-2 Protection Profile with Level 2 Sole Control.
- Seamless integration with GoPaperless and Trusted Hub Signing Verification Server products and the new Mobile-ID MPKI Mobile App for authorizing signing actions from mobile devices.

- A secure Trusted Path authorization mechanism provides the CEN "Signature Activation Protocol (SAP)" requirements and ensures only the key owner can authorize the use of their centrally held signing key.
- The SAP allows the user to review the "data to be displayed" and decide if this adequately describes what they are being asked to sign, if so they authorize the use of their remote signature.
- Includes Utimaco's most powerful HSM which is CC EAL4+ certified meeting the EN 419 221-5 protection profile – use to generate, protect and process all user signing keys. The Trusted Hub SAM Service can also be configured to just run in software on Windows or Linux for testing or evaluation purposes. It can use software crypto, a software HSM simulator or a PKCS#11 HSM.
- A high performance 1U hardware appliance that meets FIPS 140-3 Level 3 criteria.

Specifications

Component	Specifications
Software	Trusted Hub Service Provider Appliance QSCD v1.0 (EN 419241-2 Certified)
HSM	Utimaco CryptoServer CP5 Se52/ Se500/ Se1500 PCIe (EN 419221-5 Certified) - Signature generation 2048 bit Single signing: CP5 Se52 PCIe 80 tps; Se500 PCIe 640 tps; Se1500 PCIe 900 tps. Bulk signing: CP5 Se52 PCIe 85 tps; Se500 PCIe 2200 tps; Se1500 PCIe 3500 tps. - Signature generation 4096 bit Single signing: CP5 Se52 PCIe 11 tps; Se500 PCIe 100 tps; Se1500 PCIe 160 tps. Bulk signing: CP5 Se52 PCIe 11 tps; Se500 PCIe 230 tps; Se1500 PCIe 370 tps.
APIs	RESTful CSC v1.0.4.0, vCSP middleware supports Windows, vCTK supports Mac OSX, vPKCS#11 middleware supports Linux
Crypto Algorithms	RSA, ECDSA with NIST and Brainpool curves, ECDH with NIST and Brainpool curves, AES, CMAC, HMAC, SHA2-family, SHA3, Hash-based deterministic random number generator (DRG.4 acc.AIS 31), NSA suite B
Operating System	Oracle Linux 8
Database	MariaDB Galera Clustering
Server	AIC-TB116AN with FIPS 140-3 Level 3 Protection Intel Xeon E3-1275 v6 @ 3.80GHz 64 GB ECC DIMM RAM and 1,92 TB SSD



Trusted Hub Service Provider Appliance QSCD Standards Compliance:

EN 419 241-1	Trustworthy System Supporting Server Signing: Part 1 General System Security Requirements
EN 419 241-2	Trustworthy System Supporting Server Signing: Part 2 Protection Profile for QSCD for Remote Signing Trusted Hub Service Provider Appliance QSCD is CC EAL 4+ certified
EN 419 221-5	Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services Trusted Hub Service Provider Appliance QSCD - includes a certified HSM
TS 119 431-1	Policy and security requirements for TSP service components operating a remote QSCD/SCD
TS 119 431-2	Policy and security requirements for TSP service components supporting AdES digital signature creation Mobile-ID™ is working in ETSI Special Task Force 539
TS 119 432	Protocols for remote digital signature creation Mobile-ID™ is working in ETSI Special Task Force 539

Many other relevant standards that TSPs must also consider
e.g.: PAdES, XAdES, CAdES profiles, standards for certificate issuance, timestamping etc.