DATASHEET **proNEXT Signature Activation Module**

QSCD for eIDAS remote signing

- ✓ QSCD as an elementary building block for remote signing solutions
- ✓ Remote signing is a user-friendly form of electronic signature
- ✓ Simple integration of remote signing into special processes for trust service providers (TSPs)
- ✓ Cloud-based, location-independent application – lowers the barrier for TSPs to enter the remote signature market

Digital signature from the cloud

Remote signing facilitates the application of an advanced or qualified electronic signature directly from the browser without a signature card and without special software. Prior identity verification is mandatory. The location – whether workplace or home office – is irrelevant; the signing process can be conducted on mobile devices while on the move. That type of remote signature represents a time-saving solution and is particularly advisable for contractual matters that require signatures, but also for contracts that have to be signed by several people. The abort rates of contracts being signed are thus reduced enormously.

Figure above: CryptoServer CP5 by utimaco, ownership & copyright: utimaco

The challenge

The eIDAS Regulation, which has been in force since 2016, has created fundamental and binding framework conditions to enable electronic communication in legally binding form throughout Europe. Particularly in the highest form, i.e., the qualified versions of certificates and seals, specific security requirements have been formulated for TSPs, which on the one hand enable types of application and on the other hand increase the responsibility of TSPs. Therefore, TSPs are required to demonstrate the implementation of these requirements for operation in the qualified environment and the solution components used in the process for the generation of qualified signatures and time stamps, but also of validation and retention services.

ETSI Signature Creation Protocols & Policy Requirements

→ *CEN Standards for remote signing systems*:

- EN 419 241 1: Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements
- EN 419 241 2: Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing
- EN 419 221 5: Protection Profiles for TSP cryptographic modules – Part 5: cryptographic module for Trust Services
- TS 119 431 : Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1-2
- TS 119432: Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation

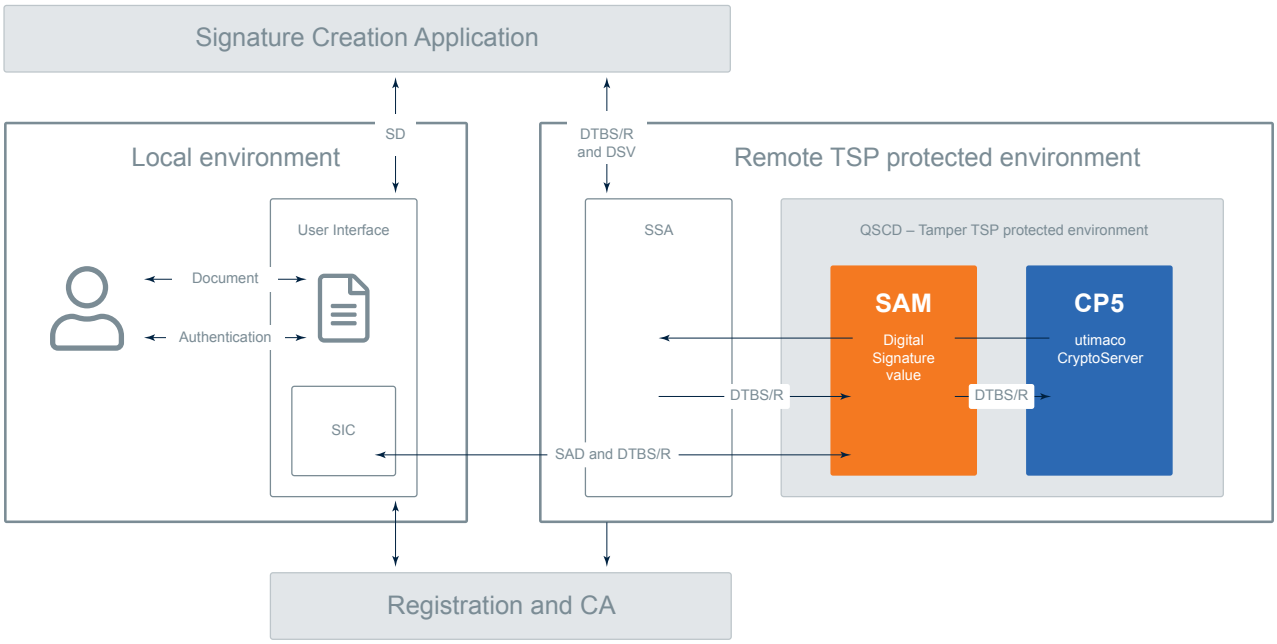
Thanks to eIDAS, users who want to use legally binding digital processes will benefit significantly from using remote signing, which will thus become a key enabler for spreading electronic signatures. However, remote signing also assigns a new role to TSPs, as from now on they will provide additional infrastructure for the signing process. The TSPs will be responsible for providing the required QSCD, which is used through entirely new technological components and can be integrated very flexibly into user processes.

DATASHEET **proNEXT Signature Activation Module**

QSCD for eIDAS remote signing

The solution

Trust service providers who want to offer a remote signing service must ensure that the signer's signature key is used exclusively under the signer's sole control and only for the intended purpose. The system for that type of service consists of a local and remote environment. The signer is in the local environment and interacts with the server signing application (SSA) and cryptographic module (HSM) in the remote environment.



The signing operation is performed using a signature activation protocol that requires signature activation data (SAD) to be provided in the local environment. To make sure that the signer has sole control over the signature keys, the signing operation must be authorized. If that is successful, a signature activation module (SAM) activates the signature key within a cryptographic module (HSM). Both the cryptographic module and the SAM must be located in a dedicated, protected environment.

For remote signing solutions, the interaction of SAM and HSM as a complete QSCD is therefore a vital component and of elementary importance. Utimaco provides the powerful combination of CryptoServer CP5 and CryptoServer CP5 SDK, which allows the SAM firmware to run in the tamper-proof environment of the HSM. CryptoServer CP5 SDK is the ideal choice for developers of such „internal SAMs“ and TSPs operating such a server signature solution.

Conclusion

For TSPs it is of vital importance to check and select the technology components used with regard to conformity to the ETSI standards. The ETSI conformity of utimaco and procilon components has been confirmed and certified by TÜV IT.

The powerful combination of hardware and software components from ultimaco and procilon enables electronic signing using qualified signatures in real time. The remote signing solution has been tried and tested in a pilot project and currently has a unique selling proposition on the market.

Contakt

procilon GROUP
Leipziger Straße 110
D-04425 Taucha
Germany
+49 342 98 48 78-31
contact@procilon.de
www.procilon.de

SecurITy made in Germany