REMOTE SIGNATURES with TRIDENT RSS

Remote Electronic Signatures are the future. And the future is here, thanks to TRIDENT RSS by i4p.

Creating and providing electronic signatures has never been this easy. With the proper tools, QTSPs can launch their eIDAS-compliant remote electronic signing services right away, offering their customers the opportunity to create electronic signatures in a fast and hassle-free manner.

Electronic signatures

An **electronic signature** as a legal concept is about having **a lasting digital record of an individual's intent**. It can legally **substitute a handwritten signature** or an **official company seal stamp certifying the authenticity of the signature in the digital world**.

To put it simply, it is digital data attached to or logically associated with other digital data, that the signer seeks to verify. Electronic signatures have been used for over 20 years in fields varying from banking and finance to e-government and legal services.

An electronic signature has the same legal standing as a handwritten signature as long as it adheres to specific requirements. In the European Union these requirements are listed under eIDAS, the regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

Types of electronic signatures are the following:

- **Basic:** All electronic types of signatures count as Basic (or Simple) electronic signature if they can provide a proof of acceptance or approval from the signer with some sort of certificate and it counts as evidence even in legal proceedings. This can be a manually written and digitally saved signature on a screen or a click on an 'I accept' button.
- **Advanced:** According to the eIDAS, Advanced Electronic Signatures have to meet specific requirements. They need to be uniquely linked to the individual signer and have to be capable of uniquely identifying the signer. The keys used to create the signature must be under the sole control of the signer. Also, the signature is to be invalidated in the case of any alteration in the signed document or file.
- **Qualified**: A Qualified Electronic Signature meets the requirements of the Advanced Electronic Signatures, and it also needs the keys used to create the signature to be generated by a Qualified Signature Creation Device (QSCD). A qualified certificate should be issued by a Qualified Trust Service Provider (QTSP), it attests to the electronic signature's authenticity to prove the identity of the signatory. According to the eIDAS, **a Qualified Electronic Signature is the legal equivalent of a handwritten signature**.

Modes of electronic signatures are the following:

eIDAS contains regulations about local signing as well as **remote** (or **server) signing**:

- **local signing**: the key used for the creation of the signature resides on the signer's own device (e. g. on a chip card or USB token).
- **remote (or server) signing**: a third party is involved, the signing key is stored on the third party's device and this device executes the signature on behalf of the key owner.

Remote Qualified Electronic Signatures[1]

In case of a remote Qualified Electronic Signature:

- the third party is a QTSP (the European Commission publishes a searchable list of QTSPs and their services[2]),
- the device used is a QSCD (the European Commission publishes a list of the certified devices[3]),
- the signer's certificate corresponding to the signing private key is a qualified certificate (look for the "id-etsi-qcs-QcSSCD" value in the certificate's QCStatement extension[4]),
- the QTSP guarantees sole control for the owners of the signing keys (according to the European Norm EN 419 241-2[5], and
- the QTSP's remote signature service is constantly audited.

According to the regulation, QTSPs providing remote electronic signature services should apply specific management and administrative security procedures in order to ensure that the electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment.

QSCDs have to meet specific criteria as well, listed in Annex II of eIDAS. These devices ensure that the signing keys are unique and kept secret and confidential, can only be used by the rightful owner and are created using trusted and established cryptographic techniques. They also have to assure that the signatures cannot be forged or duplicated. QSCDs must not alter the data to be signed or hide data from to the signer. The QTSP has to issue a qualified certificate for electronic signature which is an electronic attestation that links the electronic signature validation data to the signatory and confirms at least the name or the pseudonym of that person.

Altogether, QTSPs are obliged to use trustworthy systems and products, including secure electronic communication channels, so they can guarantee that the electronic signature creation environment is reliable and is used under the **sole control** of the signatory to prevent unauthorized use by third parties.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910
[2] https://webgate.ec.europa.eu/tl-browser/
[3] https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds
[4] https://www.etsi.org/deliver/etsi_en/319400_319499/31941205/02.03.01_60/en_31941205v020301p.pdf
[5] https://shop.bsigroup.com/ProductDetail?pid=000000000030357421

In order to assure this sole control, a special Signature Activation Module (SAM) is required as a key component of the used technical solution. The requirements for these modules are listed in the European Norm EN 419 241-2 (or Protection Profile (PP) 419 241-2 “QSCD for Server Signing”[6]).

Standards and Certificates[7]

The reliability of these QSCD devices are assured by internationally recognized standards like CC or FIPS. The Common Criteria for Information Technology Security Evaluation (Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. It is operated by 17 certificate authorizing countries and accepted by 31 countries[8].

To understand how the different certifications work, which one suits your specific projects, please read our **whitepaper**.

Protection Profiles (PP) are Common Criteria evaluations that identify security requirements for a class of security devices. Product vendors can choose to implement products that comply with one or more PPs, and have their products evaluated against those PPs, so customers looking for particular types of products can be assured that the offering meets their requirements. The Evaluation Assurance Level (EAL) of an IT product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation. Look for the EAL4+ grade when choosing a QSCD.

The list of products for digital signatures that meet the specific criteria is available on the CC web portal[9]. Fulfilling these requirements is one of the conditions of being accepted to the list of the certified Qualified Signature Creation Devices accepted by the European Commission.

The value of Remote Qualified Electronic Signatures

Since Qualified Electronic Signatures have the same legal effect as handwritten ones, they can be used in virtually all cases where parties have to sign documents. Electronic signatures eliminate the need of having hard copies of documents, which supports green initiatives and paperless offices, while also decreasing costs. Companies that provide the opportunity for their customers and employees to sign documents and invoices electronically can offer faster and simpler administrative processes as well as a more seamless customer experience.

According to a study[10] of The Global Community of Information Professionals, companies find that the two biggest benefits of electronic signatures are **a reduction of administrative work hours** and **an accelerated approval process**. Other advantages of electronic signatures are saving costs related to paper-handling (prints, copies, faxes, courier, and mail) and proven compliance for audit and electronic archiving. They also make it easier to sign documents for remote, overseas, travelling or

[6] https://www.commoncriteriaportal.org/files/ppfiles/anssi-cc-pp-2018_02fr_pp.pdf
[7] http://leidos.com/CC-FIPS140
[8] https://www.commoncriteriaportal.org/
[9] https://www.commoncriteriaportal.org/products/#DG
[10] https://www.aiim.org/pdfdocuments/MIWP-DigitalSignatures-2013.pdf

field-based staff. 81 percent of organizations that start using electronic signatures see a payback of the investment within one 12-month budget cycle.

Remote Qualified Electronic Signatures enable users to **initiate signatures from almost any device, anywhere, any time** – while maintaining the same high level of security. The initiating device (in the Protection Profile (PP) 419 241-2 "QSCD for Server Signing" it is called the Signature Interaction Component, or SIC) is not the QSCD, it simply gives the user sole control over his signing keys. Therefore, it is easier than ever to apply electronic signatures, which can make business processes simpler and faster. They allow authorized individuals to legally sign, without the need to be in an office, or in proximity of the devices required for electronic signing.

A stable basis for remote Qualified Electronic Signatures

Qualified Electronic Signatures require a qualified digital certificate issued by a QTSP and a private key generated on a QSCD device. The criteria for these devices are also listed in eIDAS. The QSCD must guarantee the confidentiality of the electronic signature and the device is responsible for qualifying digital signatures by using specific hardware and software that ensures that only the signer has control over their private key. Only a QTSP may generate or manage qualified electronic signatures on behalf of the signer. To be able to provide remote qualified signature services, QTPSs also need a SAM module which ensures the owner's sole control over the signature, providing exclusive use of the key as specified in the regulations.

i4p's TRIDENT RSS meets the strict requirements listed in the eIDAS and can be used by TSPs. TRIDENT RSS also contains a Common Criteria evaluated Crypto Module that counts as a QSCD, and it incorporates the TRIDENT SAM that also has successfully attained Common Criteria EAL 4+ certification and meets the requirements of the Protection Profile for QSCD for Server Signing. 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 to have it manage the keys.

Therefore, TRIDENT RSS enables TSPs to offer remote Advanced and Qualified Electronic Signature Services and Remote Electronic Seal Services to **equip clients with the most secure services at the highest compliance level**. For the strongest possible cryptographic security level, the keys can even be generated, stored, and managed in an entirely distributed way using SMPC (Secure Multi-party Computation).

i4p is the first and as of yet only vendor to have developed both the Crypto Module and the Signature Activation Module components required for offering Remote Signature Services. Thus, TSPs can now purchase a complete solution from one and the same vendor, incorporated in a single product, offering a more consistent product philosophy, easy integration, management, and support.

The SAM resides within the secure perimeter of the TRIDENT HSM (the CM) it uses for storing the signing keys. This way the use of TRIDENT RSS results in a much leaner and simpler infrastructure compared to multi-vendor solutions, resulting in significantly lower cost of acquisition and ownership, dramatically improving the potential ROI.

Remote Qualified Electronic Signatures are the future

Remote Qualified Electronic Signatures offer ease and convenience to customers, as they can **initiate signatures from any device of their choice**. Due to TRIDENT RSS, TSPs can launch their remote qualified signature services quickly and effortlessly, contributing to the further spreading of electronic signatures, thereby simplifying administrative processes, and reducing associated costs, while reducing the ecological footprint.