eIDAS compliant Qualified Local Mass Sealing

Sealing of up to 30 million documents per hour with Utimaco CryptoServer CP5 QSCD
Full on-premise deployment with the highest level of assurance

White Paper

Qualified Local Mass Sealing

Qualified Local Mass Sealing (QLMS) is a comprehensive solution that enables you to digitally sign up to 30 million documents per hour. The on-premises solution is using Qualified Electronic Seals that are compliant with the electronic Identification, Authentication and Trust Services Regulation (eIDAS). It is an ideal solution for mass document or data processing with a high degree of automation.

Enterprises, financial, administrative and healthcare organizations operating their own data centres can implement local QLMS for high performance sealing processes, for example, the sealing of order confirmations, invoices, digital account statements, official certificates, hospital patients' records, etc., as well as for authenticating account access for FinTechs according to PSD2 (Payment Services Directive 2).

The traditional method was and still is to deploy qualified e-seals on smart cards with crypto chips for smart card readers or USB tokens or in the cloud for remote processes.

Only since the Regulation was amended on 1 March 2019 has it become legally admissible to use Hardware Security Modules (HSM/QSCD) for internal digital sealing of documents, which is no longer reserved for Trust Service Providers only.

Based on the QSCD provided by our technology partner Utimaco, our solution for Qualified Local Mass Sealing can process up to 8,600 operations per second with a 2048bit RSA key.

What you need to know

QSCD
Qualified Seal Creation Devices certified according to EN 419221-5, and is compliant with eIDAS (EU) Regulation 910/2014.

Remote identification
Remote identity verification of the organization's legal representative is mandatory to begin the application process for the organization's Qualified Seal.

Sealing Server
For organizations which are looking for a turnkey solution for qualified sealing of documents, a high performance and versatile Sealing Server can be provided in an on-premises deployment model.

Qualified Seal
The Qualified Seal can be provided with a one, two or three-year validity which is issued by an accredited Qualified Trust Service Provider (QTSP).

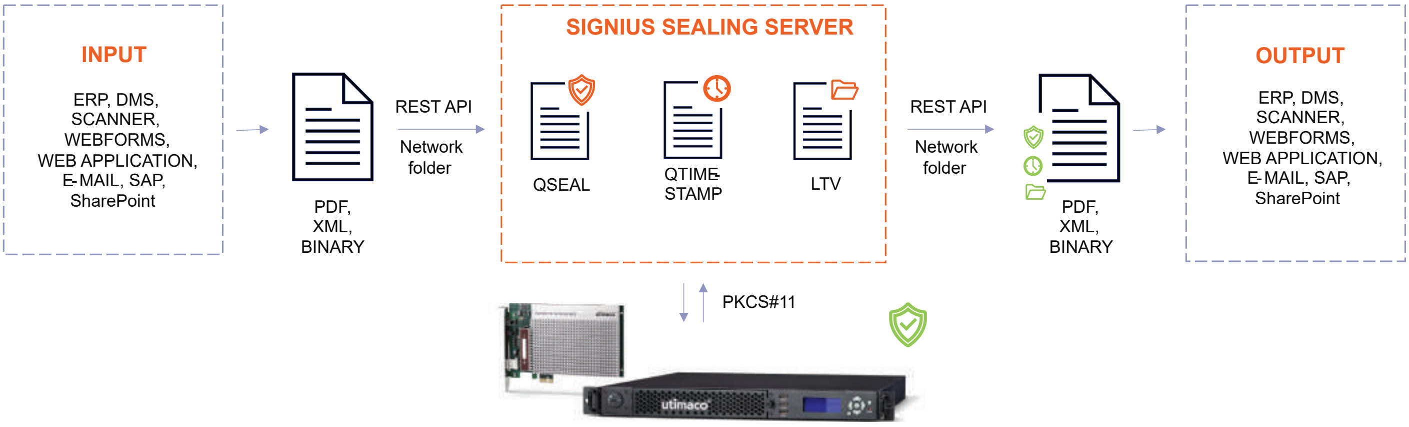
Deployment, Integration and Training
With our experience of two decades in HSM consulting, our experts will support you in the key ceremony and integration of the solution into existing IT infrastructure.

eIDAS
All technologies and processes implemented by SIGNIUS are fully compliant with eIDAS and General Data Protection Regulations.

Advantages of eIDAS compliant QLMS

- ✓ Unlimited sealing of documents without volume based fees charged by Trust Service Provider
- ✓ Mass sealing with over 30 million signatures per hour
- ✓ eIDAS certified and tamper-proof Qualified Signature Creation Device (QSCD)
- ✓ Non-repudiation, confirmed authenticity and guaranteed integrity
- ✓ Ideal for mass document or data processing with the highest degree of automation
- ✓ Replacement of poor performing legacy smart cards and card reading devices
- ✓ Flexible integration with existing signature solutions
- ✓ Wide support for various Document Management, CRM and ERP systems
- ✓ On-premise setup guarantees highest level of privacy and compliance with GDPR
- ✓ Legal compliance recognized in the EU and beyond
- ✓ Long Term Archiving and Qualified Time Stamping available upon request

The sealing process



UTIMACO CRYPTOSERVER CP5
CC-CERTIFIED QUALIFIED SIGNATURE CREATION DEVICE (QSCD)
FOR QUALIFIED ELECTRONIC SIGNATURES AND SEALS

Qualified Electronic Signatures and Seals

A Qualified Electronic Signature is the electronic signature issued to a natural person.
According to eIDAS regulations, Qualified Electronic Signatures (QES) – in contrast to 'simple' (such as a scanned written signature) and 'Advanced' signatures – offer the highest assurance and security levels. A QES has the equivalent legal effect of a handwritten signature.

A Qualified Electronic Seal is issued to and used by legal persons to ensure the origin and integrity of data and documents. A legal person is commonly understood as a legal entity, i.e. a company, enterprise, association and public authority. In connection with Qualified Time Stamps, documents signed with a Qualified Signature or a Qualified Seal provide the highest assurance level of non-repudiation, authenticity and integrity as regards the status of highest assurance.

Qualified Electronic Seals, Signatures and Time Stamps can only be created and used by a Trust Service Provider, which is audited by a conformity assessment body and certified by a national supervisory body and, finally, listed at the EU Trust Service List (EU TSL).

eIDAS & CEN/TS 419221-6

The technical specification, as published on 1 March 2019 (CEN/TS 419221-6), defines the requirements for local applications of EN 419221-5 for qualified electronic signatures or signature creation devices, i.e. in case the signatory or signature creator having direct local control over the cryptographic module. The purpose is to approve the qualified seal creation devices and/or signature creation devices (QSealCD / QSignatureCD) according to (EU) Regulation 910/2014. An appropriate certification of the HSM/ QSCD and its location in a secure server room or computer centre (e.g. with ac cess control) is required for an organization's internal mass sealing.

In such case, operating Hardware Security Modules (HSMs) as QSCD for internal qualified digital sealing of documents is no longer legally or technically reserved for qualified Trust Service Providers only.

UTIMACO CryptoServer CP5 (QSCD)

The Utimaco CryptoServer CP5 is Common Criteria EAL4+ certified according to Protection Profile EN 419 221-5 "Cryptographic Module for Trust Services". This certification allows the compliant generation of qualified digital signatures, seals, and timetsamps according to the eIDAS regulation.

A renewal of the certification is planned in December 2023 which will then be valid until 2028. The CryptoServer CP5 can be extended with a Signature Activation Module (SAM) running inside the certified HSM boundary and following the requirement of Protection Profile EN 419 241-2 by utilizing the CryptoServer SDK development kit.

Technical specifications of Utimaco CP5 QSCD

The eIDAS Compliant and CC-Certified Qualified Signature Creation Device (QSCD)

Key features

- Secure key storage and processing inside the secure boundary of the HSM
- Extensive key management with key authorization
- Key authorization API and tool (acc. PP EN 419 221-5)
- “m out of n” quorum authentication (e.g. 3 out of 5)
- 2-factor authentication with smartcards
- Configurable role-based access control and separation of duties
- Multi-tenancy support
- Remote management
- Dedicated software simulator for evaluation and integration testing
- Supported operating systems: Windows and Linux
- Multiple integrations with PKI applications, etc.
- All features included in product price

Supported cryptographic 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)
- True random number generator (PTG.2 acc. AIS 31)
- Up to 3,000 RSA or 2,500 ECDSA signing operations in bulk processing mode
- All algorithms included in product price

Available models and performance

	CryptoServer CP5					
Hardware Platform Model	**CryptoServer CP5 Se12**	**CryptoServer CP5 Se52**	**CryptoServer CP5 Se500**	**CryptoServer CP5 Se1500**	**CryptoServer CP5 Se15000**	**CryptoServer CP5 Se40000**
RSA Operations per Second	16 RSA 2K Sig/s (18 in bulk mode)	80 RSA 2K Sig/s (90 in bulk mode)	800 RSA 2K Sig/s (2,300 in bulk mode)	1,100 RSA 2K Sig/s (3,600 in bulk mode)	15000 RSA 2K sigs/s	40000 RSA 2K sigs/s

Upcoming: u.trust Anchor high-performance platform with up to 10,000 RSA 2K signatures/s

Contact us for a DEMO or a chat with our eIDAS experts!

About SIGNIUS

SIGNIUS S.A. offers a wide range of eIDAS-compliant solutions for trusted services: electronic signatures and seals for individual and corporate clients, remote customer video identification as well as local mass sealing, timestamping and archiving of documents. We create innovative technologies that drive digital transformation, cover a huge number of processes and add significant value to your organization. Our HQ is based in Poznań, Poland. Our sales offices are located in Warsaw, Prague and Berlin.

About UTIMACO

UTIMACO is a global platform provider of trusted Cybersecurity and Compliance solutions and services with headquarters in Aachen (Germany) and Campbell, CA (USA). UTIMACO develops on-premises and cloud-based hardware security modules, solutions for key management, data protection and identity management as well as data intelligence solutions for regulated critical infrastructures and Public Warning Systems. UTIMACO is one of the world's leading manufacturers in its key market segments.

www.utimaco.com

https://signius.eu **connect@signius.eu** **+48 61 415 22 12**