CRYPTOMATHiC

SIGNER 6

PRODUCT SHEET

Cryptomathic's e-signature solution is a perfect fit for organizations needing legal certainty for digitally signed assets.

Our subject matter experts have focused on matching best in class protection with interoperability, offering short time to market, simplified compliance and a future proof solution.

Cryptomathic's e-signature solution is highly modular and integrates with legacy systems, enabling your business to evolve with the regulatory landscape.

SIGNER 6
PRODUCT SHEET

CRYPTOMATHiC

DEMONSTRABLE COMPLIANCE

QSCD Certification

- Minimise the regulatory burden by relying on our QSCD, certified to the highest level

CC Certificates	Signature Activation Module	Cryptographic Module
Protection Profile Conformance	EN 419-241-2:2019	EN 419 221-5:2016
Assurance Package	EAL4 with AVA_VAN.5	EAL4 with AVA_VAN.5
Valid until (at least)	2029 (note 1)	5 December 2028
Recognised by SOGIS Participants for Mutual Recognition (2)	Yes	Yes

note 1 - Certification is in progress and expected by end Q1 2024
note 2 - List of participants published here

Readily operate our suite of applications in compliance with the following requirements for operating a remote qualified signature or seal creation device (assuming you following the included practical guidance)

- CEN 419-241-1
- TS 119 431 Parts 1, 2 and 3

LEGAL CERTAINTY

Enhance customer confidence in the signing process and provide legal certainty in the resulting electronic signature

- **Signature Activation Protocol (SAP) fully supports requirements of Sole Control Assurance Level 2 (SCAL2)**
  - using industry best practice security mechanisms
  - protocol based on specification that has undergone formal security analysis (2)
- **'What You See Is What You Sign' WYSIWYS**
  - signer confidence that the 'to-be-signed' document has no hidden artefacts
  - traceability that the signer visualised the 'to-be-signed' document prior to signing
  - WYSIWYS guarantee embedded within the signed document
- **Architected to support privacy requirements**
  - support for pseudonyms
  - confidentiality of signers document

SIGNER 6
PRODUCT SHEET

CRYPTOMATHiC

FULL OWNERSHIP OF BRANDING AND CUSTOMER JOURNEY

Flexibility to build seamless integrations to all your customer journeys, and branded to match your digital experiences to your customer's expectations.

- Build the perfect digital user experience or integrate to your existing customer journeys
- Brand everything including the certificates

INTEROPERABILITY

Our suite of solutions are designed to integrate in the emerging electronic identity and signature ecosystem to facilitate interoperability with signature portal providers, electronic ID providers, other trust service providers

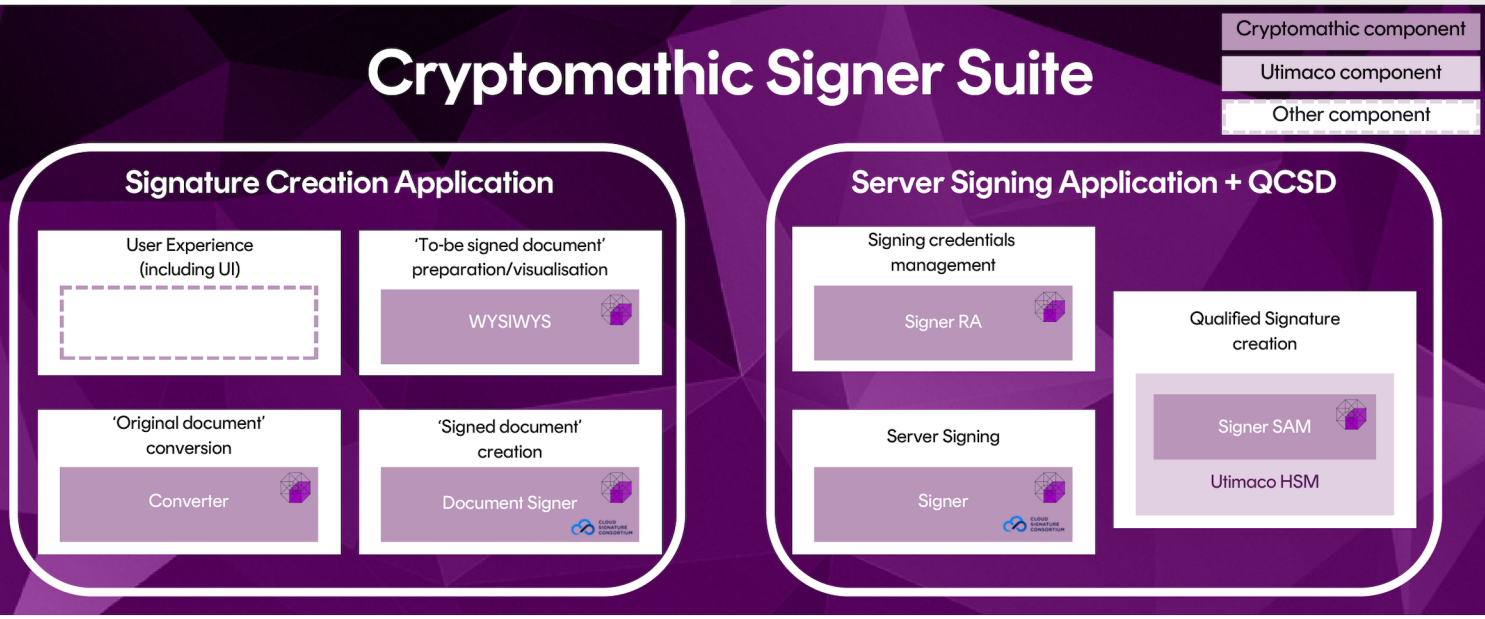
- CSC v2 specification for signature operations
- RESTful interfaces for other user and credential management operations
- Signature Activation Protocol (SAP)
  - enabled by OAuth2 Authorization Code flow (support for FAPI 2 Security Baseline compliance)
- Signature Activation Data
  - enabled by JSON Web Token (RFC 9068) using Rich Authorization Request (RFC 9396)

EASE OF IMPLEMENTATION

Select from a suite of components to integrate and enhance your signature creation application and benefit from a modern standards based market-driven design

- **Components to support your Signature Creation Application (SCA) and Server Signing Application (SSA) + Qualified Signature Creation Device (QSCD)**
  - Converter - Convert 'original documents' to compliant formats
  - WYSIWYS - Prepare and visualise 'to-be-signed documents'
  - Document Signer - Sign/seal/timestamp complete documents (including CSCv2 specification)
  - Signer RA - Manage signing credentials
  - Signer + Signer SAM - Create electronic signatures (CSCv2 specification)
- **Consistent platform for all components (other than QSCD)**
  - RHEL / Windows Server
  - Java (Oracle JDK / Eclipse Temurin)
  - Apache Tomcat

Cryptomathic Signer Suite



For more information visit our website **www.cryptomathic.com**

SIGNER 6
PRODUCT SHEET

CRYPTOMATHIC

FUTURE-PROOFED FUNCTIONALITY

Functionality, backed up by 30 years of experience in electronic signatures, reflecting the most recent developments market needs, ETSI specifications and internet standards, our suite is refreshed to prepare for the expected increase in electronic signatures resulting from eIDAS 2.0

Document Conversion/Validation

Ensure the 'to-be-signed' document is in the correct format to not only receive an electronic signature but also be subsequently validated, preserved and augmented successfully

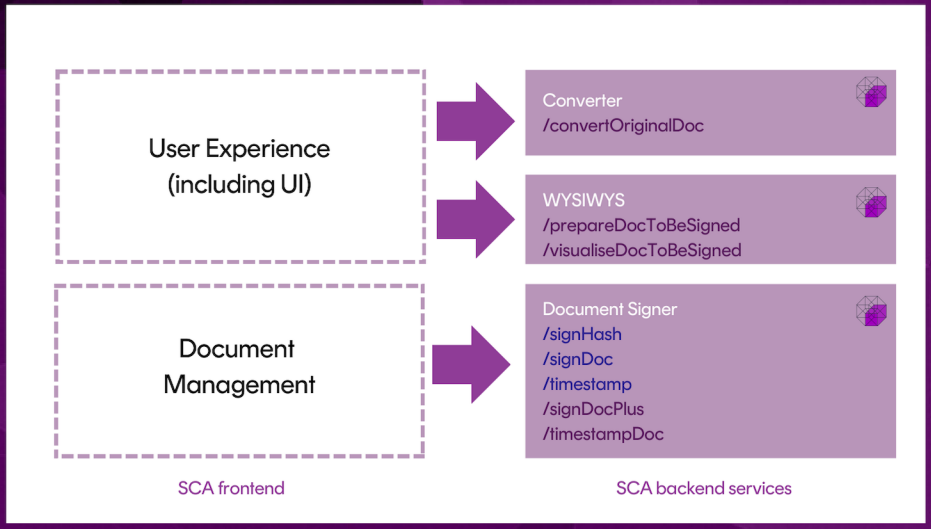
- validate/convert to PDF/A-2 compliant format

Visualisation ('What You See Is What You Sign')

Assure the end user that the document they wish to sign has no hidden content and reinforce legal certainty in the process surrounding the creation of the electronic signature

- Support for PDF and XML
- WYSIWYS Policy enforcement (required prior to signing)
- WYSIWYS traceability of process
- PDF
  - rendered as image
- XML options
  - support for common XML renders (Chromium, Firefox & Webkit (3-Windows only))
  - support for XML stylesheet (XSLT)

Signature creation application



For more information visit our website **www.cryptomathic.com**

SIGNER 6

PRODUCT SHEET

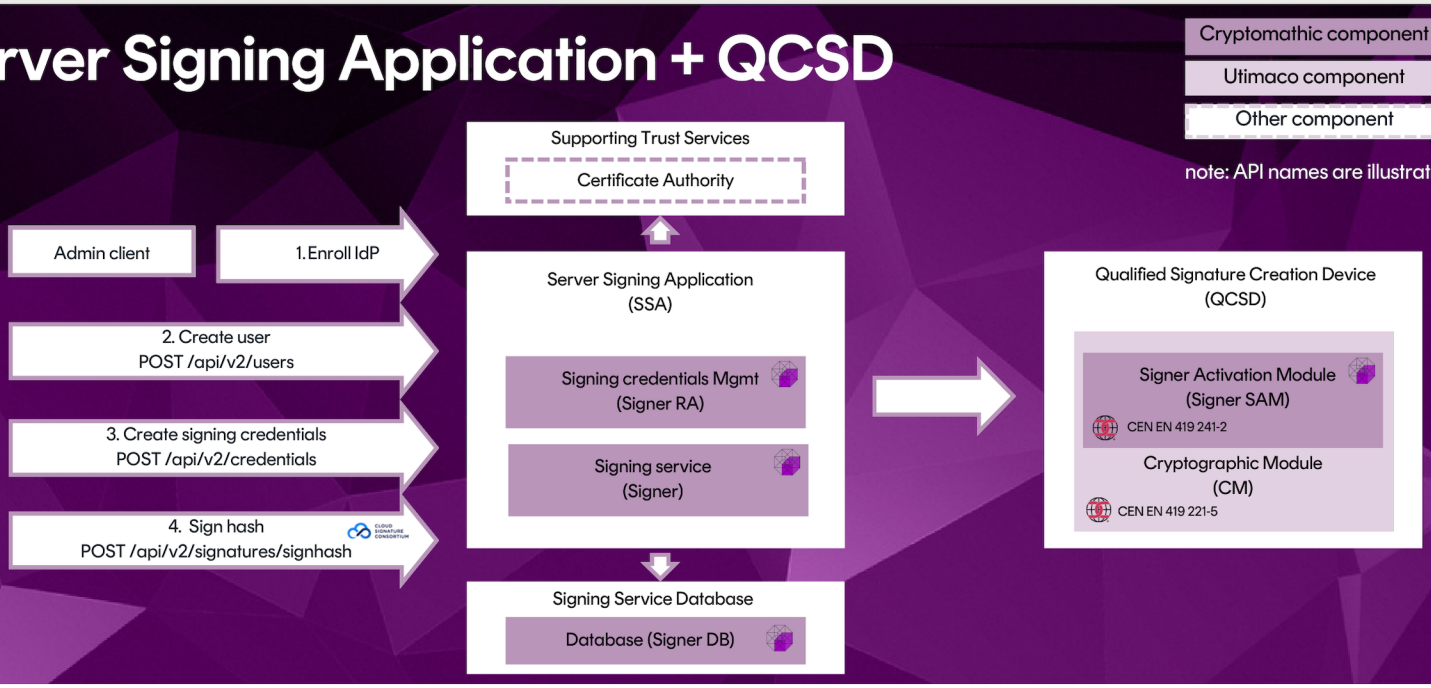
CRYPTOMATHIC

SIGNED DOCUMENT CREATION

Orchestrate the lifecycle of User Signing Credentials (keys and certificates) through a single RESTful interface

- Cloud Signature Consortium Specification (CSC v2) support for signing operations
- signHash (create an electronic signature based on a hash of the data-to-be-signed)
- signDoc (create an electronically signed document)
- timestamp (obtain an electronic timestamp from a time stamp service)
- credentials (obtain signer key and certificate information for use in the signing process)
- Support for Electronic Signature and Seals
- Support for document confidentiality
- PAdES and XAdES
- PAdES specific
- Signature Image placement
- AdES baseline signature levels:
  - B-B (Basic)
  - B-T (Signature with Time)
  - B-LT (Signature with Long-Term Validation Material)
  - B-LTA (Signature providing Long Term Availability and Integrity of Validation Material)
- Signature Algorithm Digests
  - RSA-SHA-256, RSA-SHA-384, RSA-SHA-512
  - RSA-PSS-SHA-256, RSA-PSS-SHA-384, RSA-PSS-SHA-512
  - ECDSA-SHA-256, ECDSA-SHA-384, ECDSA-SHA-512
- Time-stamp-authority (TSA) integration
  - RFC3161 (no identification, signed CMS, JSON authentication)
- OCSP Responder integration
  - standard, authenticated proxy, unauthenticated proxy

Server Signing Application + QCSD



For more information visit our website **www.cryptomathic.com**

SIGNER 6
PRODUCT SHEET

CRYPTOMATHiC

SIGNING CREDENTIALS MANAGEMENT

Comprehensive support for the creation of electronically signed or sealed documents for all common use cases and requirements using a standards based easy to use RESTful interface

- Signing Credentials Management
  - Keys protected by QSCD
  - Support for Privacy of Identity
  - RESTful API
- Supported Certificate Authorities
  - Smart ID Certificate Manager (formerly Nexus)
  - PrimeKey EJBCA
  - Entrust
  - Cryptomathic CA
- Supported protocols
  - RFC 4210 (CMP - Certificate Management Protocol)
  - RFC 5272 (CMC - Certificate Management over CMS)
- Solution support for Certificate Profiles and Statements (ETSI EN 319 412)
  - Part 1 - General
  - Part 2 - Natural Persons
  - Part 3 - Legal Persons
  - Part 5 - QCStatements

SERVER SIGNING (INCLUDING QUALIFIED SIGNATURE CREATION DEVICE)

Create Electronic Signatures and Seals through a standards based RESTful interface with a unified Signature Activation Protocol (SAP) and Signature Activation Data (SAD)

- Administration
  - Access controls enforced by QSCD
    - Dual-control
    - Multi-factor authentication
    - Authorization
  - Integrity protected audit control
- Configuration Support
  - Qualified Electronic Signatures (QES) and Advanced Electronic Signatures (AdES)
  - Electronic Signatures and Electronic Seals
  - Multiple Identity Providers
  - Multiple Signature Creation Applications / Signature Portal Providers
  - Multiple signing credential types:
    - Short-lived credentials / long-lived credentials
    - Key usage policy enforcement

SUPPORTED KEYS

- **NIST elliptic curves (P-256, P-384, P-521)**
- **Brainpool elliptic curves regular (P256r1, P320r1, P384r1, P512r1)**
- **Brainpool elliptic curves twisted (P256r1, P320r1, P384r1, P512r1)**
- **RSA 2048, 3072, 4096**

SUPPORTED SIGNATURE ALGORITHM DIGESTS

- **RSA-SHA-256, RSA-SHA-384, RSA-SHA-512**
- **RSA-PSS-SHA-256, RSA-PSS-SHA-384, RSA-PSS-SHA-512**
- **ECDSA-SHA-256, ECDSA-SHA-384, ECDSA-SHA-512**
- **Database (MariaDB, MSSQL, Oracle)**