Product Sheet

Signer

Freedom to digitally sign documents remotely
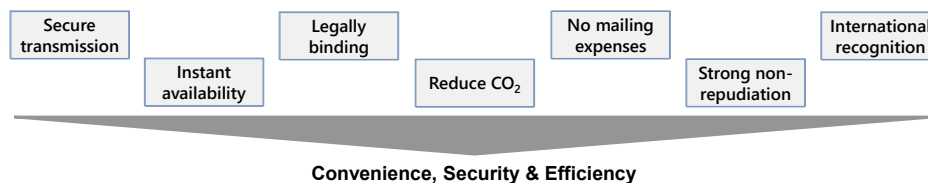
Fully eIDAS compliant

CRYPTOMAThIC

The ability to offer an end-to-end digital service with legally binding user consent reduces costs, increases security and offers greater confidence in transactions.

Offering the same legal value as handwritten signatures, Signer gives users a smooth and seamless signing experience with complete transparency as to the document or transaction being signed.

Suitable for banks, governments, and trust service providers, Signer prioritises user convenience and security to provide scalable signing technology for greater efficiency and business growth.

Centralised architecture reduces complexity and makes integration with existing business processes and applications easy.

� Provides migration from paper signatures while retaining the same legal value

▶ Offers excellent user-experience: On desktop, tablet and mobile

▶ Full audit-trail of what was signed, when and by whom

▶ Delivers Qualified Electronic Signatures (QES) recognised in the EU and beyond

▶ Available to install on-premises or as a managed service (fully or partially)

Secure transmission		Legally binding		No mailing expenses		International recognition
	Instant availability		Reduce CO_2		Strong non-repudiation	

Convenience, Security & Efficiency

Typical Use Cases

- Banking: Loan applications, contracts, transfers, new accounts, high value transactions, etc.
- Government: Tax returns, notary, stamp duty, applications and registrations...
- Health care: Records, prescriptions, journals

Flexible Deployment

- In-house - Run Signer in your own data-centre for complete control
- Hybrid model - Outsource parts of the IT but retain control of the PKI service as a TSP
- Trust service provider - Access a Qualified Trust Service and get the necessary API to sign your documents for your customers; nothing to host

User Experience

Users start by logging on to a web application or service that controls the business workflow. When a document or transaction needs to be signed, the user is invited to "View and Sign" on their screen.

The document is securely rendered in the browser using WYSIWYS technology, which ensures that only the authentic document can be signed. The user can inspect the document before committing to it.

To securely sign, the user is required to authorise the signature operation with strong authentication. Once the signature is generated, it is then embedded into the PDF or XML document in a standard format so that the user or any relying party may validate the QES signature afterwards.
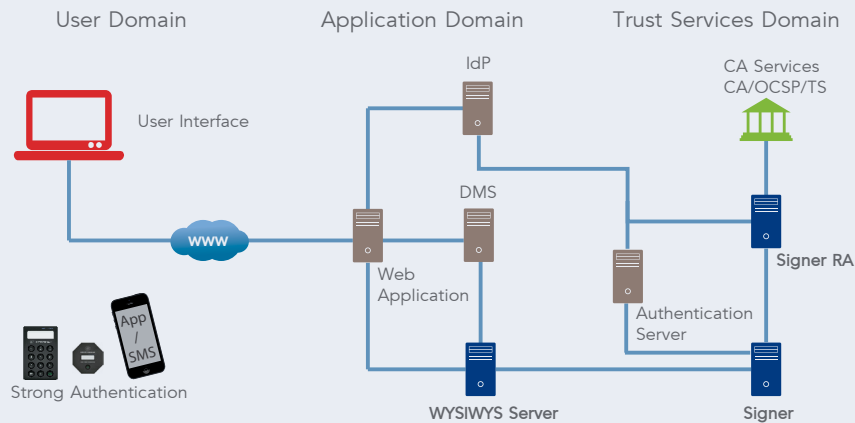
External integration points:

- User registration
- Signature process
- Authentication services
- DMS services

Technical Architecture

Cryptomathic Signer is deployed in a 3-tier environment

- ▼ User domain - The user in possession of laptop, tablet or mobile phone and uses a browser for zero footprint signing. An application installed locally can also be deployed for specific cases.

- ▼ Business Application Provider domain - The application provider manages the business workflow and prepares the data to be signed.

- ▼ Trust Centre domain - The trust centre ensures that the signing server is operated securely and manages the processes to ensure the users are provisioned with keys and certificates.

Compliance and Standards

Legislative framework:

- EU regulation No 910/2014 (eIDAS)
- Swiss ZertES (incl. VZertES and TAV)
- Other, e.g. Monetary Authority of Singapore

ETSI and CEN standards:

- ETSI EN 319 411-2
- ETSI EN 319 142-1
- ETSI EN 319 132-2
- CEN TS 419 241-1
- CEN PP 419 241-2
- CEN PP 419 221-5

Authentication standards:

- SAML v2
- OpenID Connect

RFC standards:

- RFC 3161
- RFC 6960
- RFC 2986

Financial industry standards:

- Payment Services Directive (PSD2)
- Guidance on private banking controls from Monetary Authority of Singapore

Certification:

- Pending QSCD certification / Common Criteria EAL 4+ against PP 419 241-2
- Use of CC certified HSMs

Email enquiry@cryptomathic.com for more information

Cryptomathic Signer: Pioneering remote e-signing

Already in 1998 Cryptomathic invented the notion of What You See Is What You Sign (WYSIWYS) and in 2001 Cryptomathic introduced the concept of secure remote digital signatures to the world. Cryptomathic Signer is the most advanced and secure remote signing solution; the patented technology globally supports millions of transactions and signed documents every month.

Signer Case Study - Luxtrust

Central signing service

More than 500k residents in Luxembourg can now securely access a variety of web applications like eBanking and public services, as well as digitally sign legally binding transactions and official documents from an online PC or mobile device, anywhere in the world. With just one LuxTrust certificate, users can remotely access and sign multiple online forms from any organisation connected to the service.

Signer Case Study - UBS

UBS increases efficiency and security using Qualified Electronic Signatures

As one of the world's largest banks, UBS is transforming its services through digitization by offering clients remote electronic signatures that provide the same legal value as a handwritten signature while adding convenience and efficiency.

ABOUT CRYPTOMATHIC

Cryptomathic is one of the world's leading providers of specialised security solutions to businesses across a range of industry sectors, including finance, smart card, digital rights management and government. With over 30 years' experience, Cryptomathic provides customers with systems for e-banking, PKI initiatives, ePassport, card issuing and advanced cryptography and key management utilizing best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise, customisation capabilities and unique market knowledge. Together with an established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

Learn more at cryptomathic.com