



## SIGNING AS A SERVICE

### Digital Signatures in a Service Oriented Architecture

Digital signatures make it possible to trust and act upon electronic transactions as if they were printed on paper and signed by a trusted business partner. A prerequisite for the signature to be of value is that the private key used for signing is properly protected and controlled by its sole owner. This has traditionally conflicted with ease-of-use. With Cryptomathic Signer this is no longer the case.

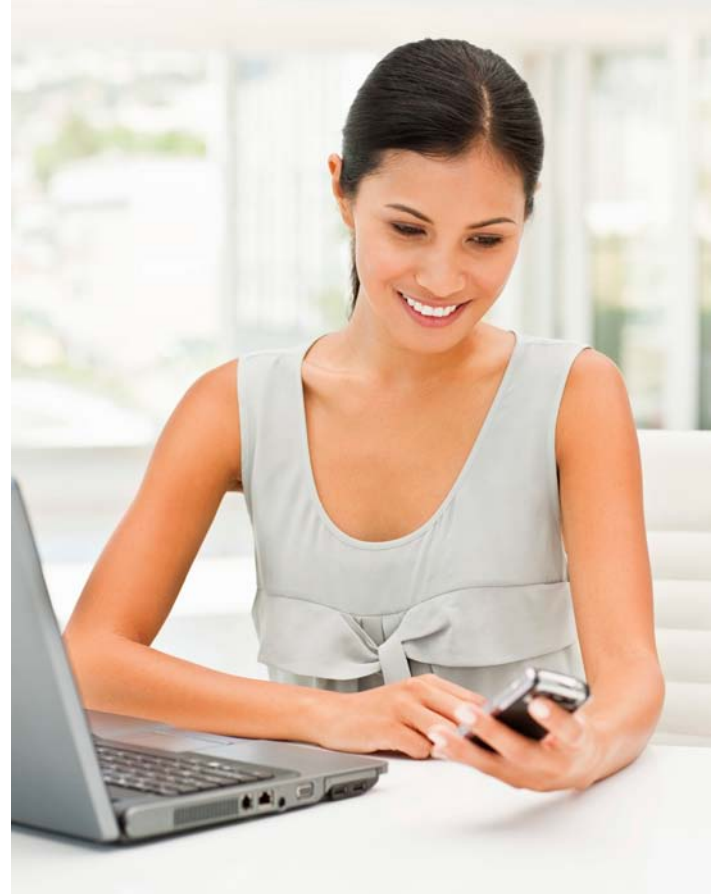
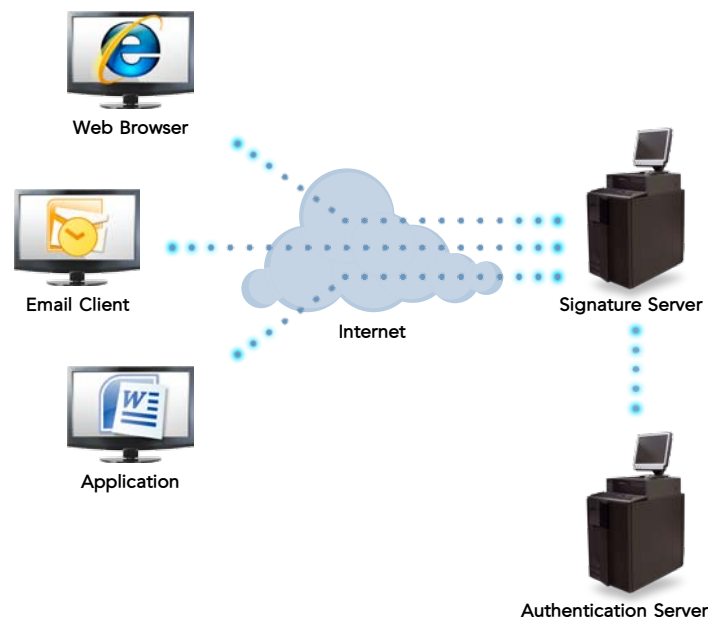
### Central Signing Service

The Cryptomathic patented method which the Signer is based upon is a service based architecture where an infrastructure offering secure signature services is made available as a service to the Business community.

Our approach is to centralise the storage and management of private signing keys at trusted 3rd parties with highly secure environments and strict procedures in order to maintain a data centre which is both logically and physically protected. The user retains full control over his/her private signing key using 2-Factor Authentication techniques.

The Cryptomathic Signer is delivered with everything it takes to integrate with any application either on the web or your local workstation PC.

A convenient way to provide such signature services is for the web application provider to develop an application using a thin client in order to fulfil the commonly desired zero-footprint requirement. In practice, this is made available as a Java applet running in a web browser. This applet can of course be customised to follow a given workflow with interactive features such as *What You See Is What You Sign* (WYSIWYS) functionality.



### Cryptomathic Signer

Compared to traditional methods for signing electronic documents, i.e. software and smart cards, Cryptomathic Signer offers:

- **Convenience:** Because a mere 2FA token (virtual or physical) and an internet connection are the sole requirements for the end-user. Full mobility is offered to the end-user who needs not care about technical issues such as key storage, lifecycle management or middleware installation. The application provider can customise his workflow and application taking advantage of the authentication and signing services provided by the Cryptomathic Signer.
- **Security:** Thanks to a secure protocol, the fact that the key storage is protected in a tamper evident environment and the strict administration procedures enforced at trust provider sites, it is possible to reach an SSCD level and provide Qualified Electronic Signature (QES) services to key owners.
- **Cost-efficiency:** No other solution available on the market offers such a combination of value added authentication and signing services directly usable in B2C environments. The total cost per user remains way below legacy SSCD devices.

## TECHNICAL SPECIFICATIONS

### Signature Formats Supported

- PKCS#1, PKCS#7
- ISO 9796-1

### Authentication Methods Supported

- OATH HOTP (for event based One Button Tokens)
- OATH TOTP (for time based One Button Tokens)
- OATH OCRA (for challenge/response based Tokens)
- Dynamic One Time Passwords delivered via SMS
- Stored one-time passwords, e.g. password cards or TAN lists
- EMV card based authentication: MasterCard CAP and Visa DPA
- Static and partial passwords

### Integration with Certificate Authority (X509v3 based)

- Integration with third party CAs using standards such as PKCS#10

### Integration with Web Application Provider

- Dedicated Cryptomathic Signer applet
- Java based SDK for authentication and signing purposes
- ANSI C API, also available as Windows DLL

### Integration with Client Workstations

- Microsoft CryptoAPI, integrates as crypto service provider (CSP)
- PKCS#11

### Operating Environment

- Microsoft Windows

### Database

- Microsoft SQL Server
- Oracle

### Hardware Security Modules

- IBM
- SafeNet
- Thales / nCipher

## OPERATIONAL SECURITY FEATURES

- All events are securely logged in the database
- Protected database, all relevant data is MAC protected and critical data (such as user's private keys) is encrypted under the HSM Master Key
- Access control for operators based on smart cards or any of the supported means for strong authentication
- Strong encryption of network communication
- Dual control for system administration
- Separation of administrator duties

## ADDITIONAL FEATURES

- Performance monitoring tool
- Scale-out clustering for high availability and performance
- Support multiple issuers
- Strong separation of the Authentication and signature servers
- Compliance against European Law for electronic signature
- Easily scalable
- Designed for large volume usage
- Architecture for high availability

Qualified electronic signatures

Digital signatures without smart cards

Authentication method independent

Multi applications & channels



## ABOUT CRYPTOMATHIC

Cryptomathic is one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including finance, smart card, digital rights management and government. With more than 20 years' experience, Cryptomathic provides customers with systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing

and advanced key management utilizing best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise 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](http://cryptomathic.com)