

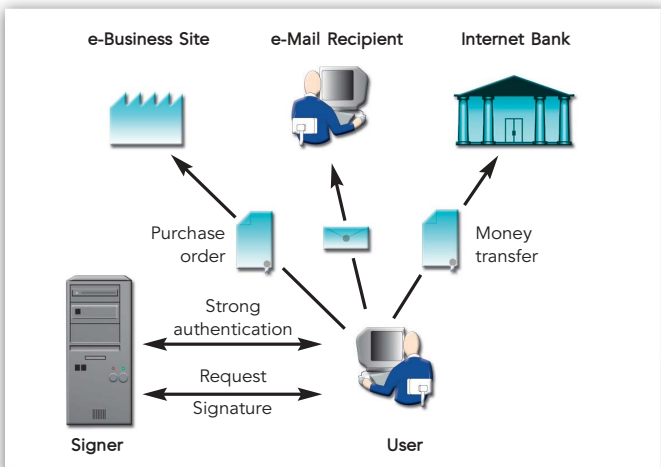
## Digital Signatures made Easy

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, however, is that the private keys used for signing are properly protected, which traditionally has conflicted with ease-of-use. With Cryptomathic Signer this is no longer the case.

### Central Signing

Cryptomathic Signer is a central server, which stores the user's private key in a secure database and generates digital signatures on the user's request. The user can request a signature at any time via the Internet, e.g. from a Web browser or an e-mail client.

This means that the physical security of the private key is no longer the user's responsibility, as it is not stored on the user's PC or hardware token. However, two-factor authentication ensures that the private key remains under the user's sole control, and he can use it from any device connected to the Internet.



*Signer can sign and decrypt e-mails and allows the roaming user to apply his digital signature to e-Business and Internet banking transactions. The actual contents are never revealed to Signer.*

### Benefits

Compared to traditional key storage solutions, i.e. software and smart cards, Cryptomathic Signer offers:

**Enhanced Key Protection** - The private keys are generated in and never leave the server's high security environment.

**Enhanced Security** - The private key is protected by the user's password at all times, which means that not even the Signer service provider can access the key.

**Mobility** - Signer can always be reached via the Internet and does not require installation of software at the client side.

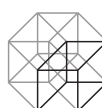
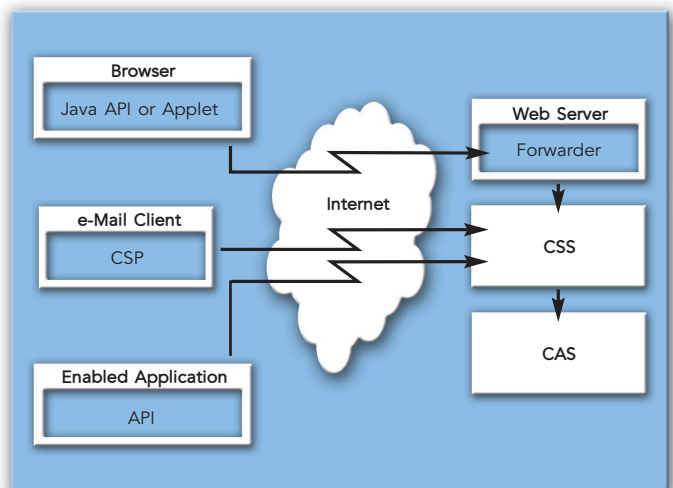
**Central Key Management** - Simplifies otherwise complex tasks like key renewal and policy enforcement.

### Architecture

Cryptomathic Signer consists of two servers: A signature server and an authentication server as well as management tools for these. Both servers can be clustered for high availability and performance.

To interface with the servers, Cryptomathic provides APIs in ANSI-C and Java, and a standardised PKCS#11 and MS-CryptoAPI Crypto Service Provider (CSP) for instant integration with Netscape Communicator and Microsoft Outlook/Outlook Express.

The figure below illustrates how the end-user's application communicates with the Cryptomathic Signature Server (CSS) via the Internet. The Cryptomathic Authentication Server (CAS) is invoked by CSS to authenticate the user's request. CAS supports several methods for strong authentication.



## Technical Specifications

### Supported Use

- Web content signing, e.g. form signing
- Signed and encrypted e-mail (Netscape Messenger, MS Outlook, and MS Outlook Express)
- Digital signatures and encryption in other enabled applications

### Supported Means for Authentication

- Authentication tokens: RSA SecureID®\* and Vasco DigiPass®
- Dynamic one-time passwords delivered by SMS
- Stored one-time passwords, e.g. password cards
- EMV card based authentication with Xiring Xi-Sign
- Open integration interface for other devices\*

### Cryptographic Specification

- RSA 512-2048 bit public/private keys

### Returned Signature Formats

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

### Certificate Format

- X509v3

### Registration Requests to CA

- Native support for Cryptomathic CA 3.0 and later
- Open interface to support other CAs\*

### Certificate Requests to CA

- PKCS #10

### Client Side Integration

- PKCS#11
- Microsoft CryptoAPI, integrates as crypto service provider (CSP)
- Low footprint applet (~30KB download size)
- Java API
- ANSI C API, also available as Windows DLL

### Server Side Integration

- ANSI C API, also available as Windows DLL

### Key Management

- All keys are hardware protected
- Keys are managed in encrypted form in the database

### Operational Security Features

- All events are securely logged in the database
- Protected database, all relevant data

are MAC protected and critical data are encrypted

- Access control for operators based on smart cards or any of the supported means for strong authentication
- Strong encryption of network communication

### Additional Features

- Performance monitoring tool
- Scale-out clustering for high availability and performance

### Operating Environment

- Signature server runs as Windows NT/2000 service
- Authentication server as Windows NT/2000 service
- Administration clients in Java (require Java 2 Runtime Environment)
- Performance monitoring via Windows NT/2000 performance monitor

### Supported Cryptographic Hardware

- nCipher nShieldF2/nShieldF3
- IBM 4758\*

### Supported Databases

- Oracle 8 and 9
- Microsoft SQL Server 7 and 2000

\* Available from version 2.2

## Cryptomathic's Trust Products

Cryptomathic's family of trust products includes all the applications needed to set up and maintain a trust community, also known as a Public Key Infrastructure (PKI). Cryptomathic's trust products range from the central Certification Authority (CA), with supporting applications for registration of users and distribution of certificates, to components for time stamping and remote signature generation, which may be added as required.

With Cryptomathic's trust products you can include the benefits of digital signatures and reliable authentication in a business application for internal or external use, offer trust services as a service provider, or even set up a public Certification or Time Stamping Authority. The simple, yet flexible, license forms and pricing models make Cryptomathic's trust products an attractive choice for solutions of any scope or size.

**Interoperable** – The trust products comply with business standards and are tested for interoperability. This ensures that the applications fit into existing infrastructures.

**Scalable and stable** – Designed with scalability and stability in mind, the trust products fit both current and future requirements.

**Proven** – Large enterprises and banks as well as financial and government institutions rely on Cryptomathic's trust products to protect their business.

**Flexible** – The trust products are designed for easy integration with existing business systems. In addition, our e-Security tools allow you to enable new and legacy applications to handle digital signatures.

**Secure** – Built by world-class security experts, Cryptomathic's trust products offer premium security.

**Hardware Crypto Enabled** – For physical security and even better performance all the trust products support hardware security modules.

## About Cryptomathic

With more than 15 years of experience, Cryptomathic is one of the world's leading providers of e-Security. We can assist you in securing your business by providing best-of-breed e-Security software products and services as well as consultancy and education.

Our range of software products covers e-Security tools for professional application development, trust products as well as personalization preparation for smart cards.

Cryptomathic's world-class experts offer e-Security consultancy at strategic level, for solution architecture, and integration.

We offer a complete modular education program, where you can learn what you need to know about e-Security – both on a general and product specific level.

We serve our customers through our head office in Denmark and our European subsidiaries. For more information, please mail us at [signer@cryptomathic.com](mailto:signer@cryptomathic.com) or visit our web site: [www.cryptomathic.com](http://www.cryptomathic.com)



**CRYPTOMATHIC**  
e-Security for Better Business