

# Cryptomathic Certification Authority

## Professional Trust Management

In the physical world identity cards and handwritten signatures are the means with which we build trust and seal agreements. In the electronic world these means are replaced by certificates and digital signatures.

The Cryptomathic CA professionally manages all the Certification Authority's tasks – this includes issuing:

- Certificates for secure e-mail (S/MIME)
- Certificates for digital signatures in Web browsers
- Certificates for authentication and VPN logon
- SSL/TLS server and client certificates
- Certificates for Windows 2000 smart card logon
- Trusted Computing Platform Alliance certificates

## Benefits

Cryptomathic CA offers all the features expected from professional trust management software, including:

**Multiple CAs** – Running several logical Certification Authorities concurrently, the CA server easily accommodates the CA hierarchies of Trust Service Providers and large enterprises.

**Scale-out Clustering** – Assures high availability and performance and allows servers to be added or removed from a running system.

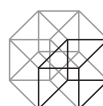
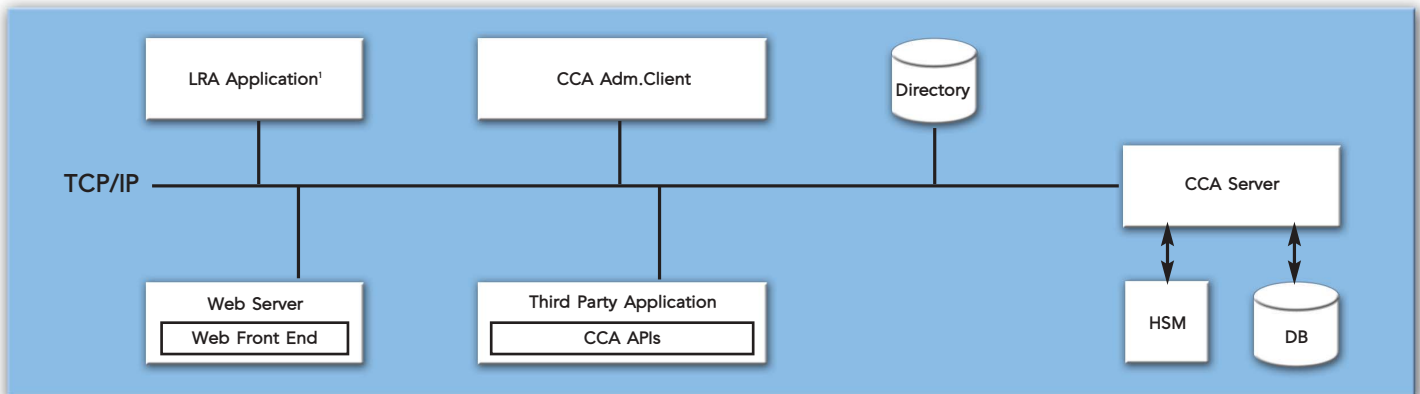
**Hardware Security Modules** – Support for a number of FIPS-certified hardware security modules.



## Architecture

The main component of Cryptomathic CA is the CA server that is managed through the (possibly remote) administration client. The Local Registration Authority (LRA) application<sup>1</sup> allows local identification and registration of end users, whereas the Web Front End provides instant integration with Microsoft Explorer for certificate issuing and installation. In addition, two APIs are provided for facilitating custom applications to interface directly with the CA server. The LRA API enables registration of end users and management of these registrations, and the PKIX API offers functionality for on-line certificate issuing, updating and revocation. Moreover, the PKIX API supplies a combined registration and certification protocol for bulk certification. Off-line certificate issuing (e.g. for CA certificates) is facilitated through the administration client.

<sup>1</sup>Available from version 3.4



## Technical Specifications

### Certificate Format

- X509v3

### Certificate Requests

- PKCS #10, certificate returned in PKCS #7 structure
- SPKAC, certificate returned in PKCS #7 structure
- CRMF, request/response according to PKIX-CMP
- Central bulk issuing
- Off-line: X.509v3 and PKCS #10, certificate returned in PKCS #7 or plain X.509v3

### Certificate Revocation and Renewal

- CMP, according to PKIX

### Certificate Status Retrieval

- Instant certificates
- CRLs according to X.509v2

### Cryptographic Specification

- Certification of RSA keys of 512 bits or longer

- RSA 1024-4096 bit CA keys, limit set by hardware security module<sup>2</sup>

### Client Side Integration

- Web pages for certificate issuing and pick up, support for any CSP
- ActiveX component for LRA administration
- API for certificate management, available in ANSI C and as Windows DLL

### Server Side Integration

- ANSI C API for CA administration, also available as Windows DLL
- API for LRA administration, available in ANSI C and as Windows DLL

### Key Management

- All CA keys are hardware protected
- All auxiliary keys are hardware protected

### Operational Features

- All events are MAC protected and securely logged in the database
- Scale-out clustering for high availability and performance

### Operating Environment

- CA server runs as Windows NT/2000 service
- Administration client – Windows NT/2000 applications

### Supported Hardware Security Modules

- nCipher nShield F2 and F3
- IBM 4758
- Chrysalis-ITS Luna SA and Luna CA<sup>3</sup>
- Any PKCS #11 compliant hardware

### Supported Databases

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

### Supported Directories

- SUN™ ONE Directory Server (formerly iPlanet Directory Server)
- Novell eDirectory
- MS Active Directory
- Any LDAP compliant directory

<sup>2</sup>In version 3.3 at most 2048 bit.

<sup>3</sup>Available from version 3.4

## 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 data 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 fill in the interest card on our web site:

[www.cryptomathic.com](http://www.cryptomathic.com)



**CRYPTOMATHIC**  
e-Security for Better Business