



## 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.

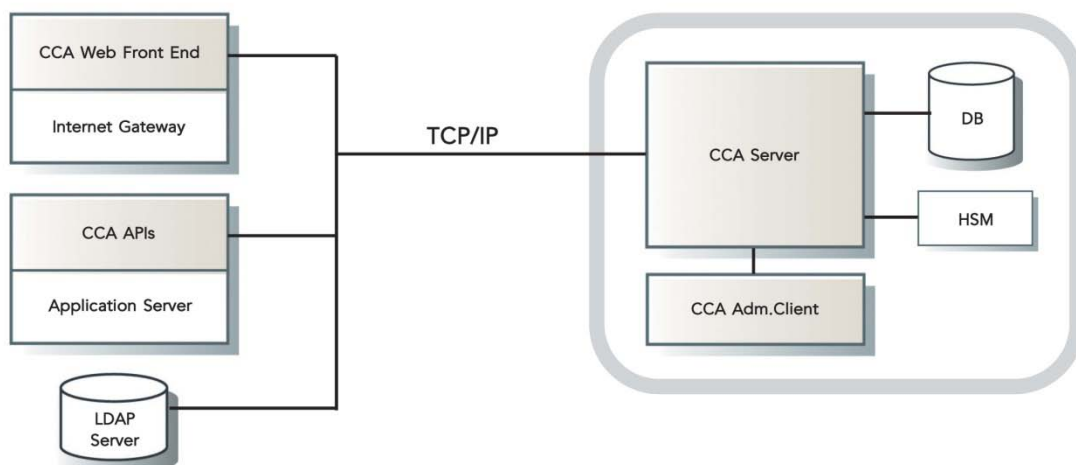
**Scale-out Clustering** – Assures high availability and performance and allows servers to be added or removed from a running system.

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



### Cryptomathic Certification Authority

The main component of Cryptomathic CA is the CA server that is managed through the (possibly remote) administration client. The system comes with a Web Front End which provides instant integration with Microsoft Explorer for certificate issuing and installation. In addition, a number of APIs are provided for facilitating custom applications to interface directly with the CA server. The APIs enable management of end user registration, and offer functionality for on-line certificate issuing, updating and revocation. Moreover, they supply a combined registration and certification protocol for bulk certification. Off-line certificate issuing (e.g. for CA certificates) is facilitated through the administration client.



# TECHNICAL SPECIFICATIONS

## Certificate Format

- X.509v3

## 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 PKCA #10, certificate returned in PKCS #7 or plain X.509v3

## Certificate Revocation and Renewal

- CMP, according to PKIS

## Certificate Status Retrieval

- Instant certificates
- CRLs according to X.509v2

## Cryptographic Algorithms

- RSA, SHA-1

## Client Side Integration

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

## Server Side Integration

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

## Key Management

- All CA and 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
- Support for multiple Hardware Security Modules (HSMs) in one server

## Operating Environment

- Microsoft Windows

## Hardware Security Modules

- Thales / nCipher
- IBM
- SafeNet
- Other PKCS #11 compliant hardware

## Supported Databases

- Microsoft SQL
- Oracle

## Supported Directories

- SUN ONE Directory Server
- Microsoft Active Directory Application Mode (ADAM)
- Other LDAP compliant directories

## Cryptomathic PKI Products

Cryptomathic's PKI products include all the applications needed to set up and maintain a trust community, also known as a Public Key Infrastructure (PKI).

Our PKI solutions can be implemented as individual products, or in combination with other products in the range. All of our PKI products will fit easily into an existing infrastructure.

Products within the PKI range include:

- Certification Authority
- CVCA & DVCA
- High Speed Inspection
- OCSP Responder
- Time Stamping Authority
- Primelink Toolkits

Cryptomathic's PKI Products are:

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

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

**Flexible** – Designed for easy integration with existing systems.

**Secure** – Cryptomathic's PKI products offer premium security

**Hardware Crypto Enabled** – For physical security and even better performance all the PKI products support Hardware Security Modules (HSMs)

## 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 over 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)