CRYPTOMATHIC
www.cryptomathic.com

Cryptomathic Certification Authority

PROFESSIONAL TRUST MANAGEMENT

In the physical world identity cards and hardwritten 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 Certification Authority (CA) is a highly secure public key infrastructure (PKI) enabling service. It issues and manages the certificates of users, service providers, applications and appliances. The Cryptomathic CA allows companies to take full control of certificate management and meets individual security requirements for using digital signatures across a wide range of applications and platforms including: eGoverment, Trusted Platform Modules (TPM), ID cards and ePassports, eBanking, Digital Rights Management (DRM) and Utilities.

Cryptomathic Certification Authority

The Cryptomathic CA professionally manages all the tasks of a Certification Authority - this includes issuing:

- Certificates for secure email (S/MIME)
- Certificates for digital signatures
- Certificates for authentication and VPN logon
- SSL/TLS server and client certificates
- Certificates for Windows smart card logon
- Trusted Computing Platform Alliance certificates
- Certificates for Country Signing CAs (ePassport/eID)

Benefits

Cryptomathic CA offers all the features expected from a PKI enabling service, 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.

Flexibility - Designed to enable customers to tailor the solution to meet their specific organisation's needs. The CA easily integrates with other PKI components.

System Architecture

The Cryptomathic Certification Authority is designed in a client-server structure, where the CA server that is managed through the (possibly remote) administration client. 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 of online 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: X509v3 and PKCS#10, certificate returned in PKCS#7 or plain X.509v3

Certificate Revocation and Renewal
- CMP, according to PKIX

Certificate Status Retrieval
- CRLs according to X.509

Cryptographic Algorithms
- ECC (NIST, Brainpool)
- RSA
- SHA-1, SHA-256, SHA-384, SHA-512

Client Side Integration
- 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 auxilliary keys are hardware protected

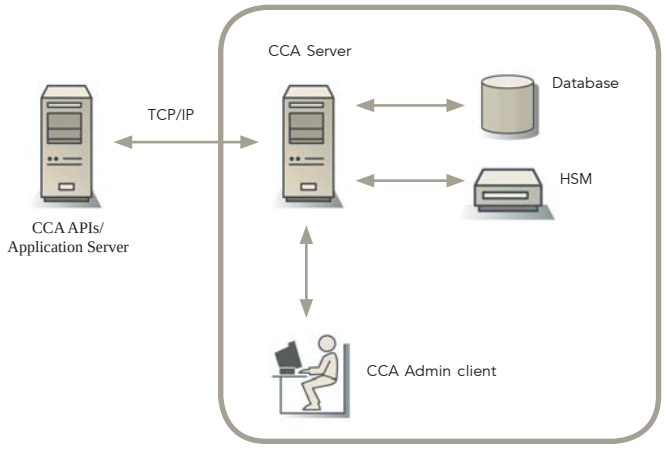
Operational Features
- Two-factor authentication for user logon
- All events are MAC protected and securely logged in the database
- Scale-out clustering for high availability and performance
- Support for multiple Hardware Security Modules (HSMs) in one server

Operating Environment
- Microsoft Windows

Hardware Security Modules
- Thales / nCipher
- SafeNet
- Utimaco
- Other PKCS#11 compliant hardware

Supported Databases
- Microsoft SQL
- Oracle

Cryptomathic CA System Overview



CRYPTOMATHIC PKI PRODUCTS

Cryptomathic's PKI products include all the applications needed to set up and maintain an 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 incude:

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

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 25 years' experience, Cryptomathic has assisted customers by providing systems for e-banking, PKI initiatives, card personalisation, ePassport, card issuing, and advanced key management through best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with its 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