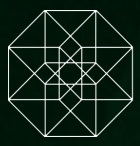


CRYPTOMATHiC

# EMV CA

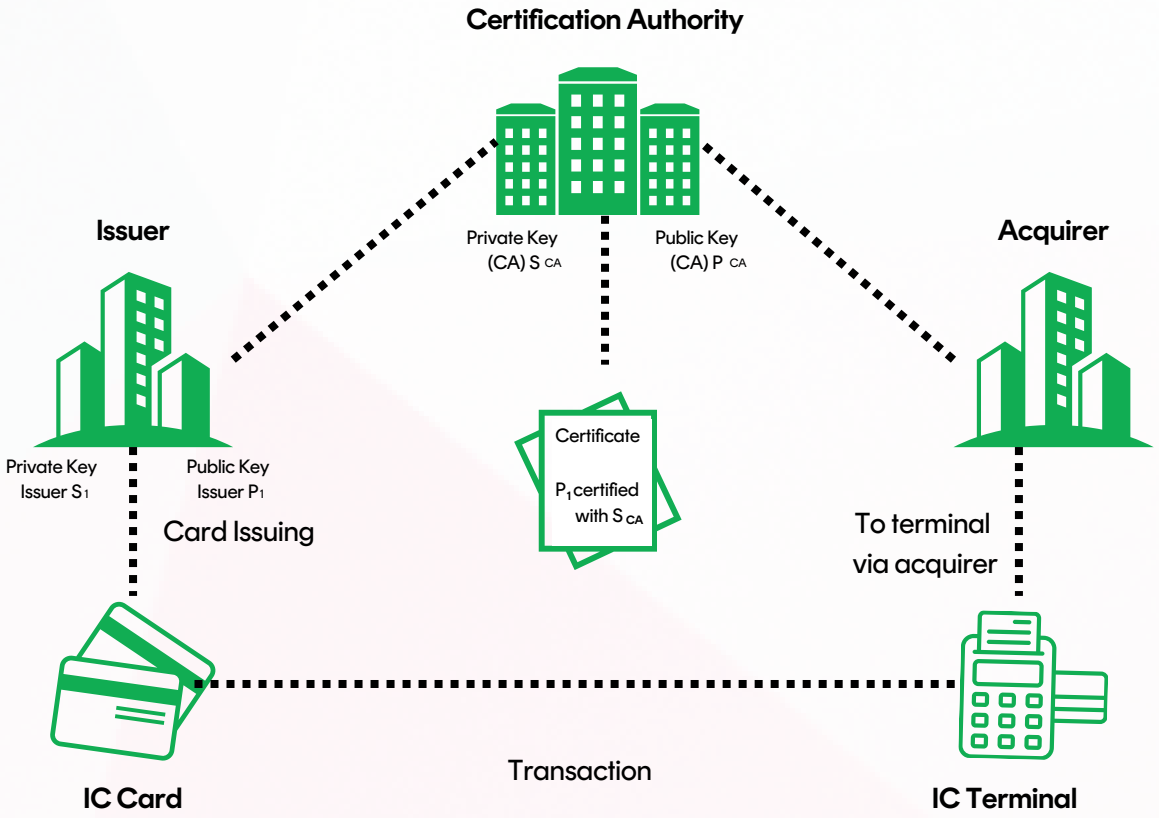
## A Regional EMV Solution

Product Sheet

# EMV AND PKI

EMV is the payment system standard widely used across the globe, with billions of credit and debit cards issued since its initial roll-out. Nowadays, cards can be found in various forms, physical or virtual, and allow many transaction types with card-present (being contact, contactless), or with card-not-present on the Internet. In the context of card-present transaction, contact or contactless, the payment card presented at the point-of-sale terminal (POS) must be authenticated to make sure of its authenticity. EMV defines two different types of card authentication mechanisms, one being on-line when the transaction can be sent to the issuer, and one being offline when the transaction must be processed locally without a direct communication with the issuer. The EMV off-line card authentication process is based on Public Key Infrastructure (PKI), such requiring an EMV Certification Authority.

EMV Certification Authority is the root of trust to payment schemes, under which issuers and acquirers are certified, acting as a trusted third party. A payment scheme can be a major international player such as MasterCard and Visa, or it can be regional or country wide, such as national debit schemes, which are found in many countries all over the world. Cryptomathic EMV CA is the product of choice on which payment schemes rely for establishing and managing their root of trust.



# EMV CA

The Cryptomathic EMV CA allows managing all CA and Issuer certificate functions including:

- Creation of multiple EMV CAs
- Lifecycle management of EMV CA root keys and associated CA certificates
- Export of CA certificates for distribution to acquirers
- Export of CA Certificate Revocation List (CA CRL)
- Lifecycle management of Issuer certificates
- Export of Issuer's Certificate Revocation Lists (Issuer CRL)

## Benefits

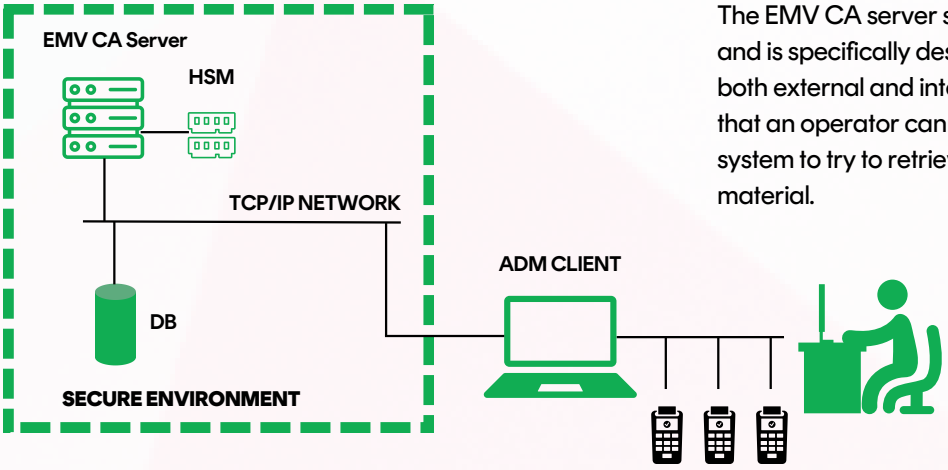
**Multiple CAs –** Running several logical Certification Authorities concurrently accommodates different CA hierarchies required by Trust Service Providers or countries/regions operating multiple schemes.

**Compliance –** EMV CA follows the best practices and security guidelines defined by the EMV standard. It also supports the issuer certificate formats from Visa and Mastercard, among others.

**Security** – role-based access control with segregation of duties and dual control are implemented. All sensitive cryptographic operations performed in FIPS-certified hardware security modules (HSMs).

# SYSTEM ARCHITECTURE

The main component of Cryptomathic EMV CA is the CA server, managed through the administration client, providing a user friendly graphical user interface. The EMV CA server accesses the data base and the HSM and accepts only AES encrypted connections on the client communication port, which is configured during initialization.




The EMV CA server supports multiple HSMs and is specifically designed to protect against both external and internal attacks. This means that an operator cannot force changes in the system to try to retrieve valuable key material.

# TECHNICAL SPECIFICATIONS

### Certificate Format

- EMV MasterCard
- EMV Visa
- Regional certificates can be supported upon request

### Security Features

- All CA private keys protected in FIPS 140-2 level3 HSM
- Integrity protected audit log.
- Server clustering for high availability and redundancy
- Role-based access control with 2FA
- Dual control on all sensitive operations.

### Operating Environment

- Microsoft Windows

### Supported Database

- Microsoft SQL

### Hardware Security Module

- Entrust nShield

# EMV PRODUCTS

Cryptomathic has a wealth of experience working with EMV. Whether it's protecting card holder data(e.g. acquirer network security), issuing EMV cards or advising on how to balance security and cost, banks and financial service providers all over the world rely on Cryptomathic to ensure that their EMV projects run smoothly.

Cryptomathic's EMV offerings include a range of products needed for issuing as well as accepting EMV cards:

- Data preparation
- Card management system
- PIN Management
- EMV Key management system
- EMV card authorization

### Features

**Interoperable –** All EMV products comply with business standards and are tested for interoperability, e.g. scheme logical security inspections. This ensures that the applications fit into existing infrastructures.
**Scalable and Stable –** Designed with scalability and stability in mind, the EMV products fit both current and future requirements.
**Proven –** Financial institutions and banking service providers rely on Cryptomathic's EMV products to protect their business.
**Flexible –** The EMV products are designed for easy integration with existing banking systems.
**Secure –** Built by world-class security experts, Cryptomathic's EMV products offer premium security.
**Hardware Crypto Enabled –** For physical security, compliance and increased performance all the EMV products support hardware security modules.

# ABOUT US

Cryptomathic is a global leader in data security and encryption solutions. Governments, industry leaders and cloud service providers around the world trust us to address their security challenges, reduce risk and meet complex compliance requirements.

Our solutions encrypt and fortify data, transactions and applications across a wide range of industries. By trusting Cryptomathic, enterprise businesses and governments achieve cryptographic-agility and truly adaptive digital security..

**www.cryptomathic.com**

**enquiry@cryptomathic.com**

**+45 8676 2288**