

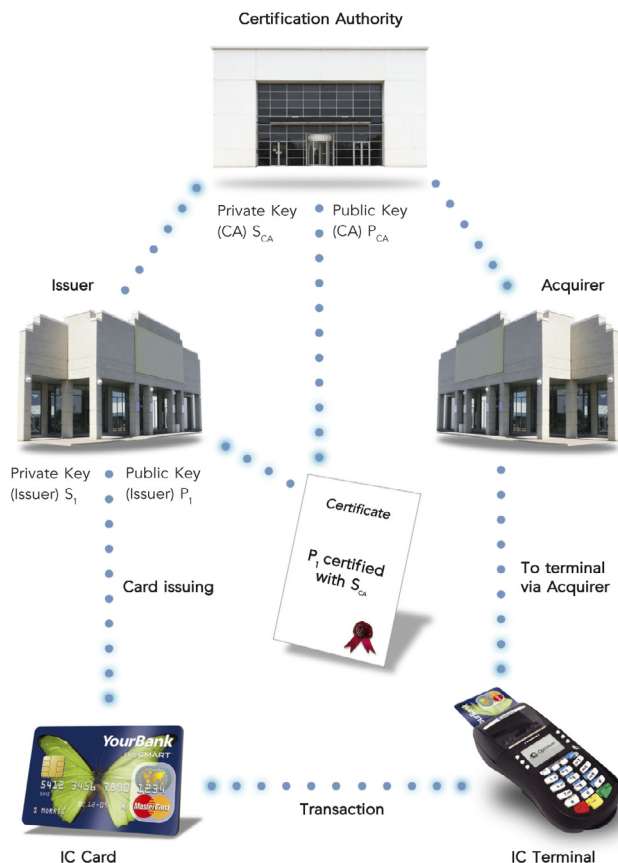
EMV AND PKI

A Regional EMV Solution

The EMV standard is designed to provide an interoperability framework for payment cards. This covers many transaction types including credit, debit, contactless and mobile. Payment cards have been around for many years in various forms. The latest cards have become more sophisticated and now contain a microchip, which can store a wealth of information, including security information used for authentication and encryption.

EMV card authentication is based on PKI (Public Key Infrastructure) but unlike traditional PKI, which is based on a standard called X.509, EMV is a standard of its own. Even though EMV is a proprietary standard it is widely used across the globe, with billions of EMV smart cards issued since its initial roll-out.

EMV Certification Authorities are central to the payment card framework, under which issuers and acquirers are certified by the payment schemes, 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. Each payment scheme requires an EMV Certification Authority and the Cryptomathic EMV CA provides that exact functionality.



EMV CA

The Cryptomathic EMV CA professionally manages all the Issuer's and Certification Authority's tasks including:

- Lifecycle management of EMV Issuer CA (scheme issuers') certificates
- Issue certificates
- Export certificates
- Revoke certificates
- Certification authority CRL (Certificate Revocation List)
- Issuer CRL (Certificate Revocation List)

Benefits

Cryptomathic EMV 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. This means that a regional EMV CA running the Cryptomathic solution could support multiple CA functions – one for each country or sub-region.

Secure User Administration – No single user can get exclusive access to the system. The system operates dual controls where users log-on using smart cards with defined roles as Administrator, Operator or Auditor.

Hardware Security Modules – Performs all sensitive cryptographic operations 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

Certificate Requests

- VISA and MasterCard self signed certificate formats

Certificate Revocation and Renewal

- EMV

Operational Features

- All events are MAC protected and securely logged in the database
- Clustering for high availability and performance
- Support for multiple hardware security modules (HSMs)

Key Management

- All CA keys are hardware protected

Hardware Security Module

- Thales / nCipher

Operating Environment

- Microsoft Windows

Supported Database

- Microsoft SQL Server

CRYPTOMATHIC'S EMV PRODUCTS

Cryptomathic has a wealth of experience working with EMV. Whether it is 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 applications needed for issuing as well as accepting EMV cards:

- Data preparation (EMV)
- Card personalization software
- Card management system (CMS)
- Crypto management and transaction authorization platform (CSG)
- EMV Certification Authority
- Centralized lifecycle key management system (CKMS)
- EMV card authentication server (CAP authentication)

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 CRYPTOMATHIC

Cryptomathic is a global provider of secure server solutions to businesses across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile. With over 30 years' experience, we provide systems for Authentication & Signing, EMV and Crypto & Key Management through best-of-breed security solutions and services.

We pride ourselves on strong technical expertise and unique market knowledge, with 2/3 of employees working in R&D, including an international team of security experts and a number of world renowned cryptographers. At the leading edge of security provision within its key markets, Cryptomathic closely supports its global customer base with many multinationals as longstanding clients.