

**CRYPTOMATHiC**

# **OBSIDIAN CA**

Turn-key EMV Certificate Authority for  
national and private payment schemes

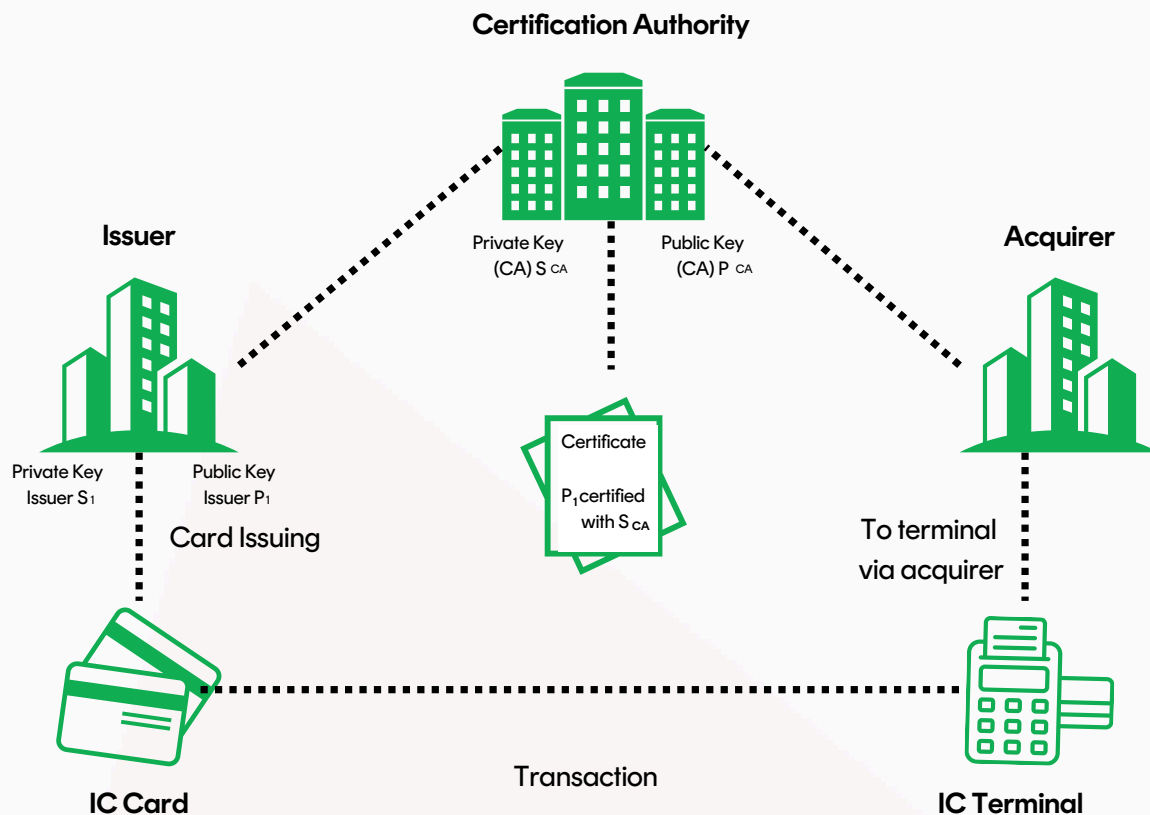
Product Sheet

# EMV CERTIFICATE AUTHORITY

International card networks typically charge a high interchange fee per transaction. National schemes running their own EMV infrastructure removes dependency from the large international payment schemes, and achieve payment sovereignty by using domestic rails. At the heart of every domestic scheme sits an EMV Certification Authority (CA)—the cryptographic “root of trust” that signs issuers public key certificates so transactions remain fraud-proof even when processed offline at the POS.

Cryptomathic’s Obsidian CA is the product of choice on which payment schemes rely for establishing and managing their root of trust. It is the market-proven platform behind more than 15 national debit systems and 250 million cards world-wide. It lets your scheme:

- Stand up a fully accredited CA in under 90 days.
- Run multiple card programs on one cluster, with FIPS 140-2 HSM protection and <5 s RPO.
- Reduce per-transaction network fees.



# OBSIDIAN CA



Cryptomathic's ObsidianCA 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

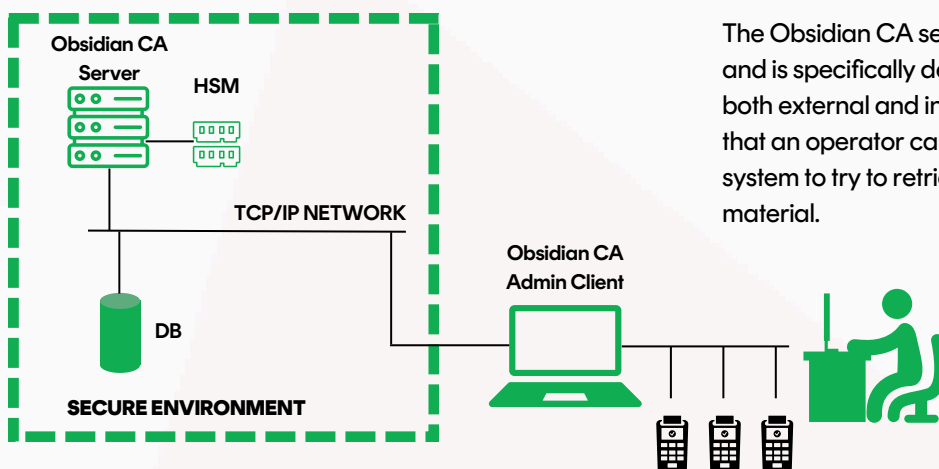
**Cost efficient** – Running several logical Certification Authorities concurrently accommodates different CA hierarchies required by countries/regions operating multiple schemes.

**Compliant** – ObsidianCA follows the best practices and security guidelines defined by the EMV standard. It supports different certificate requests formats including the ones from Visa and Mastercard, among others.

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

## SYSTEM ARCHITECTURE

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



# TECHNICAL SPECIFICATIONS



## Certificate Format

- MasterCard
- Visa
- Regional schemes

## Security Features

- All CA private keys protected in FIPS 140-2 level 3 HSM
- Integrity protected audit log.
- Server clustering for high availability and redundancy
- Role-based access control with 2FA
- Dual control on all sensitive operations.

## Hardware Security Module

- Utimaco uTrustAnchor
- Entrust nShield 5c
- Additional vendor plug-ins available upon request.

## Supported Database

- Microsoft SQL

## Operating Environment

- Microsoft Windows

# PAYMENT PRODUCTS

## Cryptomathic experience in payment

**150 million+ EMV®** Chip cards are issued annually with data generated by Cryptomathic solutions.

**500+ financial institutions globally trust us** to secure their EMV® card data, including Barclays, S2M and Swedbank.

## Payment offering include a range of products

**Obsidian platform**, for EMV data-prep, EMV authorization and PIN Management.

**CardInk**, EMV data-prep and key management system.

**CrystalKey360**, key management for payment.

**MASC (Mobile Application Security Core)**, in-app mobile security for mobile banking apps, wallets and SoftPOS applications.

## 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](http://www.cryptomathic.com)**

**[enquiry@cryptomathic.com](mailto:enquiry@cryptomathic.com)**

**+45 8676 2288**