CRYPTOMATHIC
www.cryptomathic.com

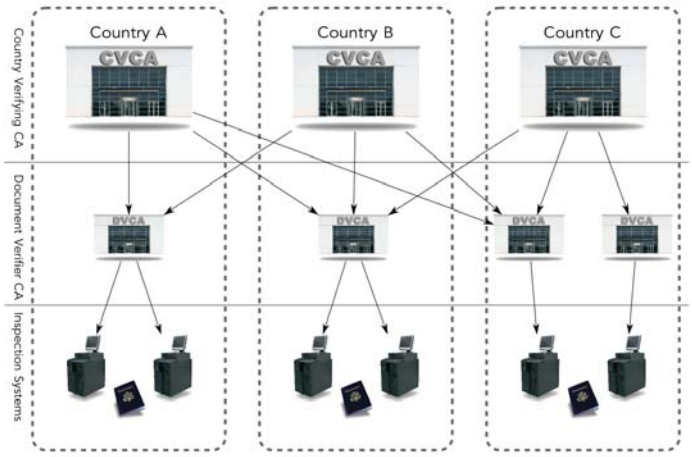
Cryptomathic CVCA/DVCA

EPASSPORT EAC INSPECTION PKI

Extended Access Control

Implementing Extended Access Control (EAC) for machine readable travel documents means a paradigm shift from the *right to inspect* to the *privilege to inspect*. EAC depends not just on the existing ePassport infrastructure, but also on a second inspection Public Key Infrastructure (PKI). The inspection PKI allows countries to certify each other to read sensitive fingerprint data from EAC ePassports, and assists in country management of inspection systems.

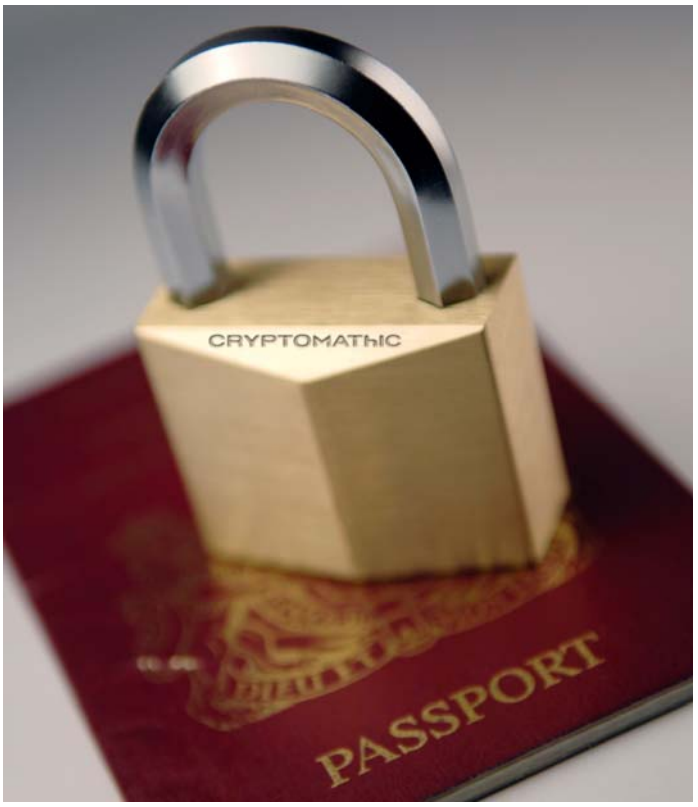
Cryptomathic CVCA/DVCA is a special purpose certificate authority designed specifically for EAC ePassport data formats and workflows. It provides functionality for both Country Verifying Certificate Authorities (CVCAs) and Document Verifier Certificate Authorities (DVCAs) as outlined below.



Cross certification of inspection systems

The Inspection PKI

For nations rolling out "second generation" EAC passports, each issuing country establishes its own PKI, and needs to authorise the accepting countries to read sensitive data from its passports. The inspection PKI consists of infrastructure components that process certificate requests, verify the identity of new applications, and then issue time-limited certificates granting permission to inspect. The resulting certificate chain is checked by the ePassport. The components consist of:



CVCA (Country Verifying Certification Authority):
Each country that wants to take part in an EAC environment needs to establish a CVCA. The CVCA authorizes Document Verifier Certification Authorities by issuing Document Verifier certificates.

DVCA (Document Verifier Certification Authority):
Will receive certificates from CVCAs in all countries willing to grant access to the passports they have issued. The DVCA itself will then issue certificates to all of the country's Inspection Systems.

CRYPTOMATHIC CVCA/DVCA

Standards Compliant and Easy to Use

Cryptomathic CVCA/DVCA is a single product which can be used either in the role of the CVCA or the DVCA for issuing Card Verifiable certificates in all levels of the trust hierarchy in accordance with the EU-led EAC protocol, BSI Technical Report 03110. Day-to-day operation of the CA is supported through the secure and user-friendly administrative remote client, which features a modern graphical user interface. Work-flow driven processes are used for configuration and certificate policy management, country management, inspection system registration, in addition to certificate issuance and key update protocols. Synchronous and asynchronous dual control of operations and two-factor logon mechanisms permit state-of-the-art security

TECHNICAL SPECIFICATIONS

Supported Protocols

- EU Extended Access Control
- BIG Working Group CVCA interoperability protocols
- Terminal Authentication

Security Architecture

- Two factor auth. for user logon
- Secure environment using HSMs
- HSM specific firmware for key generation
- Secure audit log of all events (in HSM)

Hardware Security Modules

- SafeNet ProtectServer (FIPS 140-1 level 3)
- nCipher nShield (FIPS 140-2 level 3)
- IBM 4764 (FIPS 140-2 level 4)
- Software emulated HSM

Standards

- ICAO ePassport LDS (Logical Data Structure)
- BSI TR03110 EAC
- MULTOS / GlobalPlatform

Operating Environment

- Microsoft Windows: W2K Server and Windows 2003
- Microsoft Windows Service

Supported Cryptographic Standards

- RSA
- ECDSA and ECDH
- SHA family
- Card-Verifiable (CV) certificates

Database

- Oracle version 9i or higher
- MS SQL Server 7 and 2000
- OBDC compliant databases

without damaging usability, even if operators are not present at the same time and place for performing system operations.

System Integration

Verifying systems easily integrate with the Country Verifying CA through the automated certification interface for high-volume or frequent certificate issuance for inspection systems. Once the request is registered, approval can be granted in manual, timed or automatic modes, reducing manpower resource requirements. The CA can issue certificates in an entirely manual mode as well, suitable for air-gapped environments.

Client-authentication ensures that the certificates are only issued to trusted clients, and strict enforcement of certificate policies guarantee that keys being certified are endowed with the correct inspection privileges.

Secure Server

Central features of the Cryptomathic CVCA are Role-Based Access Control (RBAC) for operators, both administrative and operator use, and a high performance and scalable architecture to meet the requirements of modern production systems in terms of availability and fail-over. The system maintains a digitally signed audit log to allow monitoring of system critical activities and reporting in the event of possible attacks on the system. Cryptomathic's security speciality is to use advanced custom developed Hardware Security Module (HSM) firmware, to ensure that private key material is properly managed and protected by HSMs even in the event of server compromise (see technical specification for details on availability). These facilities operate in conjunction with the industry standard PKCS#11 interface.

Cryptomathic ePassport Suite:

Cryptomathic offers a wide range of products, solutions and consultancy for ePassport (for more details, see our website):

- ID Issuer (Data Signing CA & Data Preparation)
- Inspection System
- ID Inspector Server / SDK / Mobile ISKM / DevTool

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 20 years of 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.