

Cryptomathic CardInk ID Data Preparation System

Electronic Passports

The move from OCR¹-only passports to electronically readable passports, known as ePassports is well underway on a worldwide scale. The national authorities responsible for passport issuing and border control management are implementing new and complicated technology. They are facing time pressure from the international community to convert to ePassport.

CardInk ID is a data preparation system for generating the logical data structure (LDS) for ePassports. With LDS, the ePassport data is structured in a standardised way designed to pave the migration path and meet future requirements imposed through the ICAO ePassport standard. CardInk ID ensures secure data generation and cryptographic key management based on the citizens' record files.

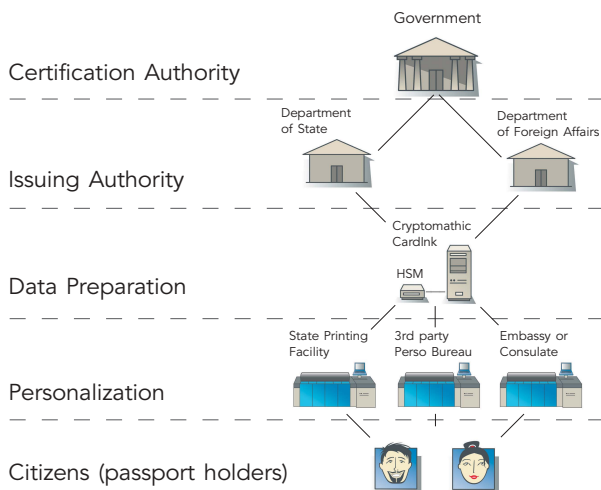
System Architecture

CardInk ID is the third generation data preparation system from Cryptomathic. It has been developed in close cooperation with major industrial nations and service suppliers to meet market demands.

CardInk ID is used by the passport issuer and integrates with chip management systems. The host feeds data to CardInk ID which in turn prepares ePassport data i.e. LDS data in TLV (Tag Length Value) format. CardInk ID output files conform to a wide range of personalization systems.

¹Optical Character Reading

e-Passports Issuing



Cryptomathic CardInk ID

Flexible – CardInk ID is suitable for passport production. The system offers: security, stability, low-maintenance and will suit almost any migration and issuing strategy. CardInk ID interfaces with chip management systems for full automation (using a DLL or an API). This results in fast production, thus making LDS data preparation an easy passport issuing task. CardInk ID works with a wide range of HSMs (Hardware Security Modules) integrating with passport issuers' existing production environments.

Cost-efficient – CardInk ID is the most versatile LDS data preparation solution available imposing no limitation on the number of passports issued, ensuring a high return on investment. The system is easily set up, allowing issuers to instantly issue ePassports across a number of issuing locations.

Key Management – The core objective of CardInk ID is to allow for versatile management of cryptographic keys related to LDS data preparation. CardInk ID contains a complete key management system with functionality for communication and key exchange with external systems. All keys are handled in HSMs and CardInk ID provides secure import / export facilities. This applies to all aspects of ePassport including; key encryption keys, transport keys, document signing keys, certificate management (including PKI interoperability), as well as management of administrative keys for disaster recovery, and appropriate separation of duties through management of system users.



Technical Specifications

Supported Authentication Schemes

- Passive Authentication (digital signatures)
- Active Authentication (individual keys for each passport)

Platforms

- RFID ISO/IEC 14443

Formats Supported

- ICAO ePassport LDS (Logical Data Structure)

Supported Cryptographic Standards for LDS

- RSA algorithm PKCS#1
- ECDSA
- SHA-1
- 3DES, AES
- X.509 certificates

System Architecture

- Multiple servers
- Multiple HSMs
- System Integration API for automated production

Security Architecture

- PKCS#8, PKCS#12 protected net work communication
- Access control via smart cards
- Secure environment using HSMs
- HSM programming for active authentication schemes
- Secure audit log of all events (in HSM)

Operating Environment

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

Database

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

Hardware Security Modules

- Eracom Protectserver Orange CSA 8000 (validated to FIPS 140-1 level 3)
- nCipher nShield F3 (validated to FIPS 140-2 level 3)

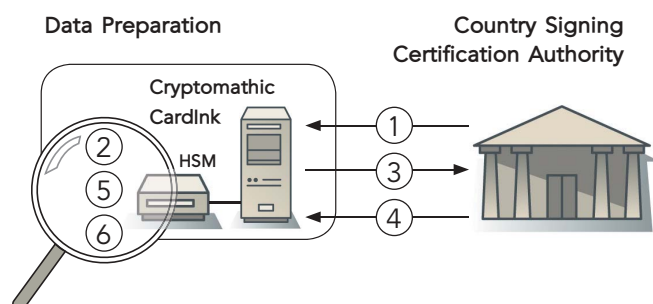
Other HSMs

- PKCS#11 interface
- HSM specific firmware

Performance Monitoring

- Customisable integration into Microsoft Windows Performance Monitor

Certificate Management



CardInk Key Management:

1. Import of CSCA self signed certificates
2. Generation of Document Signer RSA key pairs
3. Export of Document Signer RSA public key to CSCA
4. Import of Document Signer certificate signed by CSCA
5. Creation and signing of Document Security Objects at run time (using the Document Signer private key)
6. Optional import of Document Signer private keys

The ICAO PKI scheme consists of a classic certificate hierarchy with a Country Signing CA as the highest authority.

Document Signer Certificates belong to the Document Signers that represent the second level in the hierarchy and are the ones that sign each passport using their private RSA keys.

The signed data in a passport (the Document Security Object) contains the mandatory hash values of the LDS content. Thereby, the authenticity of each passport can be verified at border control level.

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 almost 20 years of experience, we have assisted our customers by providing systems for e-banking, PKI initiatives, card personalization, 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.

www.cryptomathic.com

