CRYPTOMATHIC
www.cryptomathic.com

Cryptomathic ID Issuer

SECURE LDS GENERATION

Electronic Identification Documents

Electronic identity and travel documents are becoming the most widely implemented means of identification across the globe. These include documents such as national ID cards, electronic passports and driver's licences.

Electronic Passports

The move from paper based passports to electronically readable passports is underway on a worldwide scale. National authorities responsible for passport issuing and border control management are implementing new and sophisticated technologies. Whilst many countries face time pressure from the international community to adopt electronic passports (ePassports), the European Union is pressing forward with the addition of fingerprint data, protected by Extended Access Control (EAC). Cryptomathic ID Issuer is a system that securely generates the Logical Data Structure (LDS) for ePassports, and associated key material. The ePassport LDS structures biometric and biographical data in a standardised way designed to pave the migration path and meet future requirements imposed through the ICAO (International Civil Aviation Organization) ePassport standard. ID Issuer can interface with both enrolment systems and personalization systems to ensure secure data generation and cryptographic key management throughout the issuance process.

ID Issuer is a third generation system, building on Cryptomathic's extensive experience in EMV data preparation and Public Key Infrastructure. It has been developed in close cooperation with major industrial nations and service suppliers to meet market demands. The passport issuer can integrate ID Issuer with an ePassport enrolment system so that data is digitally signed as soon as an application is approved, and returned in personalization-ready data files. Alternatively ID Issuer can prepare data for personalization in real time and be integrated into production software. ID Issuer output formats conform to a wide range of personalization systems, and uses Hardware Security Modules (HSMs) to provide the highest level of security for document signing keys. In the case of Active Authentication and EAC, the HSMs also securely generate cryptographic keys for each ePassport.

Cryptomathic ID Issuer

Future Proof – ID Issuer is specially designed for passport production, but can be integrated in a variety of ways to prepare ICAO compliant data for use in other multi-application settings (e.g. national ID cards). It can support Basic Access Control (BAC) data generation, EAC data generation, and "EAC with BAC data" modes. The system offers: security, stability, low maintenance and will suit almost any migration and issuing strategy.

Cost-efficient – ID Issuer is the most versatile LDS data generation solution available. It imposes no limits on the number of passports issued, ensuring a high return on investment. The system is easy to set up and integrate against, allowing issuers to rapidly prepare data for ePassports to be used across multiple issuing locations.

Key Management – A central objective of ID Issuer is to simplify key management for cryptographic keys related to LDS data generation, whilst retaining versatility. ID Issuer contains a complete key management system with functionality for communication and key exchange with external systems. All keys are handled in HSMs and ID Issuer provides secure import / export facilities. This applies to all aspects of ePassport including:

TECHNICAL SPECIFICATIONS

Supported Protocols
- BAC
  - Passive Authentication
  - Active Authentication
- EAC
  - Chip Authentication
  - Terminal Authentication
- SAC
- PACE

Platforms
- Microsoft Windows Server 2008

Formats Supported
- ICAO ePassport LDS (Logical Data Structure)
- BSI TR03110 EAC
- CBEFF

Supported Cryptographic Standards
- RSA algorithm PKCS#1
- ECDSA and ECDH
- Diffie-Hellman
- SHA family
- 3DES
- X.509 certificates

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

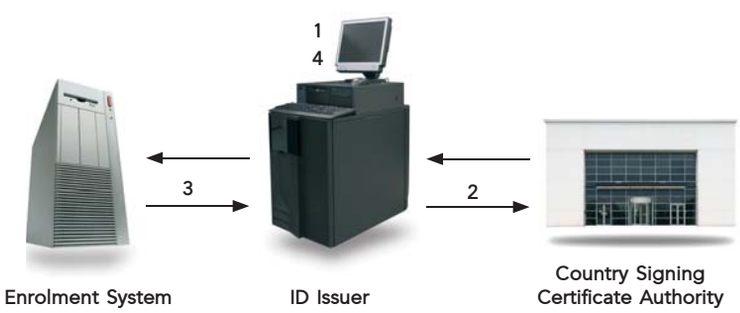
Security Architecture
- PKCS#8, PKCS#12 encrypted network communication
- Two factor authentication for user logon
- Secure environment using HSMs
- Specific HSM firmware for key generation
- Secure audit log of all events (in HSM)

Operating Environment
- Microsoft Windows

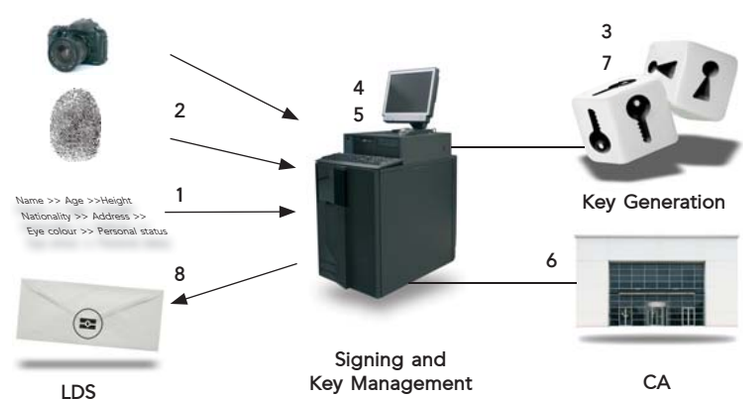
Database
- Oracle
- Microsoft SQL Server

Hardware Security Modules
- Safenet
- Thales / nCipher
- IBM

Other HSMs
- PKCS#11 interface
- HSM specific firmware



ID Issuer Setup
1. Generation of Document Signer RSA keypair
2. Certification of Document Signer key by CSCA
3. Normal Operation via integration API
4. DS Key Management as required (import etc.)



ID Issuer Operation
1. Construct MRZ and Data Group 1
2. Construct Biometric image blocks (face & fingerprint)
3. Generate ePassport keypair with HSM and make DG14 (AA/EAC only)
4. Construct additional data groups as required
5. Hash data groups, and create Document Security Object
6. Digitally sign Document Security Object with DS key
7. Re-encrypt ePassport private key (AA/EAC only)
8. Return formatted LDS and chip data

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 more than 25 years' 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.

Learn more at cryptomathic.com