MOBILE-ID
Anytime, Anywhere

# TRUSTED HUB

## ePASSPORT APPLIANCE

**Common Criteria Certified PKI**

Trusted Hub ePassport Appliance provides a modular framework that delivers all of the components required to issue, protect and validate ePassports as well as an SDK that can enable border control to inspect ePassports and digitized passport holder biometrics.

Electronic passports are electronic machine-readable travel documents with many security features, Public Key Infrastructure provides the key components to deliver electronic security to the solution. The International Civil Aviation Organization (ICAO) and the European Union introduced standards to provide security to these documents, this has helped to deliver superior border security to countries globally.

## Modular Deployment Options

Trusted Hub ePassport Appliance is built on the modular architecture of the Trusted Hub Appliance platform, Trusted Hub ePassport Appliance can be deployed to meet the requirements of Basic Access Control, Extended Access Control or both.

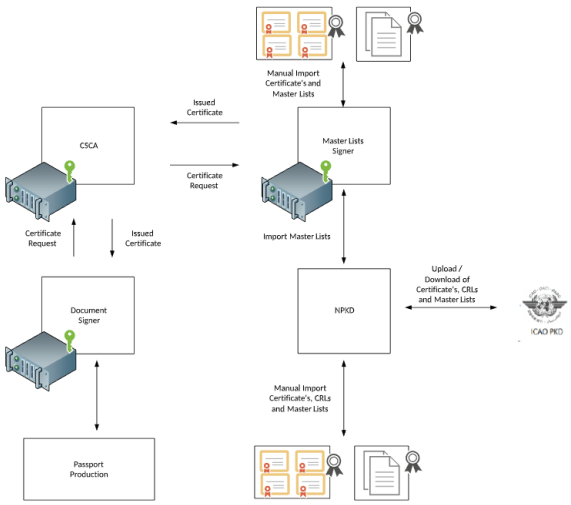
### Mobile-ID Basic Access Control PKI

#### Core CSCA Infrastructure

- Country Signing Certification Authority (CSCA)
- National Public Key Directory
- Master List Signer

#### Passport Production Infrastructure

- Document Signing Service




### Mobile-ID Extended Access Control PKI

#### Core Infrastructure

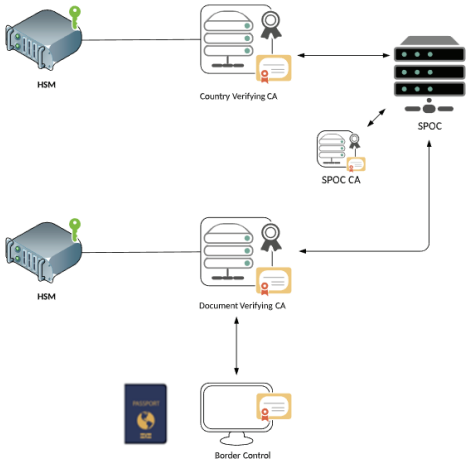
- Country Verifying CA (CVCA)
- Document Verifier (DV)

#### Border Control

- Inspection System SDK

#### International Certificate Management

- Single Point of Contact (SPOC) CA
- Single Point of Contact (SPOC)



## Mobile-ID SPOC

Mobile-ID's Single Point of Contact (SPOC) module enables countries to securely exchange certificates and certificate requests automatically for their EAC PKI with their international counterparts to enable secure and authorised access to citizen biometrics stored within the ePassport.

## Mobile-ID National Public Key Directory Server

National Public Key Directory (NPKD) provides fully automated download and upload to the ICAO PKD and offers countries the ability to manually import BAC validation materials obtained through diplomatic exchange or that have been downloaded from ICAO.

## Mobile-ID Master List Signer

Master List Signer is an optional component that digitally signs a list of CSCA certificates, this provides a secure list of trust anchors at border control as well as supporting a secure distribution mechanism for CSCA certificates via the ICAO PKD.

## Key features for Trusted Hub ePassport Appliance

### Certificate Format Support
- X.509 and ISO 7816
- ICAO 9303 and EU Standards Compliant

### Automated Certificate Lifecycle Management
- BSI TR-03129 Compliant
- Certificate Management over CMS
- ICAO PKD Download/Upload
- International Certificate exchange via SPOC

### Easy to Deploy
- Dual Rooted PKI to support combined BAC and EAC Deployment
- Component based flexibly deployment
- FIPS 140-2 and Common Criteria EAL 4 Evaluated
- Inspection System SDK toaid border control

### Operating System Support
- Microsoft Windows Server 2016/2019
- Linux CentOS, RedHat, Suse & Fedora

### Database Support
- Microsoft SQL Server 2019/2017/2016
- Oracle 18c/11gR2
- PostgreSQL 11.x/10.x/98.x
- MySQL 8.x
- Percona 5.7.x

### Hardware Security Module Support
- Thales Luna HSM Family
- Entrust Datacard nCipher nShield Family
- Utimaco CryptoServer Family

### Trusted Hub Security Features
- Secure Web console with strong 2FA of operators
- Fine grain access control and role management
- Detailed HMAC logs of all operator actions and API calls
- Automated/manual system integrity checking
- Flexible Dual control features
- Monitoring and alerting features using SNMP

## Standards Based Trust Infrastructure

Trusted Hub ePassport Appliance is fully compliant with:
- ICAO 9303 7th Edition Part 12 – Public Key Infrastructure for MRTDs
- BSI TR-03139 v2.2 – Common Certificate Policy for Extended Access Control Infrastructure
- BSI TR-03129 – Protocols for the Management of Certificates and CRLs
- BSI TR-03110 – Advanced Security Mechanisms for MRTDs
- CSN 36 9791 – Country Verifying Certification Authority Key Management Protocol for SPOC