# Entrust ePassport Solutions

Get the reliability, scalability, and level of automation required to support complex border ecosystems, with Entrust's ePassport solutions.

## OVERVIEW

### Issuance and Inspection Technology for ePassports

Security concerns, developing technologies, and emerging standards have led governments worldwide to pursue issuing more sophisticated electronic Machine-Readable Travel Documents (eMRTDs) to their citizens. Commonly known as "ePassports," these documents contain a chip that stores information that is verified against the data page of the passport.

Interoperable, scalable, and validated by third-party testing, our ePassport trust infrastructure is very comprehensive. In fact, Entrust® is one of very few vendors capable of delivering the reliability, scalability, and level of automation required to support border ecosystems that are experiencing unprecedented traveler volumes.

## KEY FEATURES

### Continously enhancing our solution

Entrust continues to enhance our solutions to meet emerging travel standards, improve infrastructure reliability, and increase trust at the border.

- Versatile solutions for managing citizen ePassport, e-ID, and mobile ID
- Common Criteria certified to EAL 4+ augmented
- Automated certificate lifecycle management
- Fully integrated PKI and document-issuance architecture
- Fully automated national and international certificate management and distribution

## THE OPPORTUNITY

### The Complete ePassport Solution

With trusted PKI technology, we provide solutions for first- and second- generation eMRTDs, commonly referred to as Basic Access Control (BAC) and Extended Access Control (EAC). We are pioneers of Passport/ePassport delivery, with market-leading solutions for:

- Identity vetting and document-issuance workflow software
- Physical production of ePassports on high-performance laser, ink, and dye transfer-based print/personalization systems
- PKI to support integrity and authenticity features within eMRTDs and Digital Travel Credentials (DTC)
- Authentication and validation of ePassports for automated border control systems

Supported components include: CSCA, CVCA, DV, DS, MLS, DLS, NPKD, ICAO PKD upload/download, IS/Concentrator architecture, including DTC issuance and/or derivation from standard eMRTD.

# Entrust ePassport Solution

## HIGHLIGHTS

### Scaled eMRTD validation for border control

As the globalization of travel and international trade continues to grow, the need for countries to secure their borders and prove the authenticity and validity of eMRTDs has never been more important.

In order for border control systems to be able to validate eMRTDs, they need access to validation certificates for credentials for all countries anticipated at the border.

Entrust provides a national PKD solution and ICAO PKD interoperability that enables automation of the access, lifecycle management and distribution of validation materials to border control.

| **Country Signing Solution**<br>Basic Access Control (BAC) | **Country Verifying Solution**<br>Extended Access Control (EAC) |
|---|---|
| Protects the digitized version of the eMRTD data on the contactless RFID chip. Provides digital signature protection to ensure integrity and authenticity of chip data (Passive Authentication or PA). | Protects access to digitized biometrics (fingerprints and/or iris scans), which, as Personal Identifiable Information (PII), is considered especially sensitive and requires strongly authenticated access control. |
| Authentication for chip access while originally employing BAC is not standardized on the cryptographically stronger Supplemental Access Control (SAC) using Password-Authenticated Connection Establishment (PACE). | Provides authentication between the eMRTD and the inspection station to control release of the biometrics (Terminal Authentication or TA). |
| Consists of:<br>• An X.509 certificate-based PKI certification authority (Country Signing Certificate Authority or CSCA).<br>• Document Signer (DS) that digitally signs each ePassport.<br>Our DS employs a component architecture that allows it to be deployed securely in centralized, distributed, or hybrid models to support the varied needs of national issuing authorities. | Consists of:<br>• An ISO 7816 certificate-based PKI CA (Country Verifying Certificate Authority or CVCA).<br>• A sub-CA (Document Verifier or DV) that provides lifecycle management of keys and certificates for border control systems via inspection system APIs.<br>Our PKI is dual-rooted to support both X.509 and ISO 7816 PKI standards from a single platform. |
| Solution includes additional optional DSs to support:<br>• Master List Signing (MLS)<br>• Deviation List Signing (DLS) services<br>• Digital Travel Credential (DTC) signing | The Single Point of Contact (SPOC) is deployed to secure international certificate management capabilities to support cross-jurisdictional interrogation of eMRTDs for biometric validation. |
| The National Public Key Directory (NPKD) solution handles lifecycle management of certificate validation materials received from the ICAO PKD or exchanged bilaterally with foreign states.<br><br>Our NPKD is designed for scale and can completely automate the retrieval validation and distribution of validation materials to border control points. | The CVCA, DV, IS Concentrator, and IS Client provide national and international lifecycle management of TA keys and are typically deployed with hardware security modules (HSMs) to store and protect PKI keys. |

**Learn more at**
**entrust.com**



ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
**info@entrust.com**