No Issuance without Inspection

Millions of eMRTDs are in circulation today and billions of dollars have been invested in the issuance of the credentials to mitigate threats of undetected forgery, impersonation, fraud and other criminal activity. Unfortunately, proper inspection infrastructure is often expensive to deploy and maintain. And costs don’t end at the initial investment — expert IT staff are required for ongoing operation and maintenance.

Optional Integration

For governments with limited expertise and budget, Entrust provides the necessary components for proper document inspection — all from a single, proven vendor. Importantly, Entrust can streamline integration with both the ICAO PKD as well as domestic no-fly lists.

Streamlined Border Control

Entrust simplifies the complex architecture associated with validating eMRTDs by providing a solution that cross-references the revocation information from the International Civil Aviation Organization’s (ICAO) public key directory (PKD) and secures the transmission of validation material.

Encrypted Data Transmission

To ensure the secure exchange of documents and certificates, Entrust also properly encrypts all transmissions — providing a trusted infrastructure and protecting the integrity of all exchanged data. If transmissions are susceptible to attack, false or altered data can result in the incorrect acceptance of a fraudulent eMRTD and jeopardize the entire global security infrastructure.

Solution Benefits

- Gain a proven solution for inspection of first- and second-generation eMRTDs
- Leverage optional integration to ICAO PKD, domestic no-fly lists
- Comply with all ICAO standards, including BAC and EAC
- Based on Entrust’s proven PKI technology
- Improve ROI with comprehensive service that includes infrastructure, facilities, integration and expertise
- Deploy via flexible hosted or on-premise models
Entrust ePassport Solutions
Document Inspection

Entrust ePassport Inspection

**Comprehensive**
Entrust PKI solutions simplify all aspects of properly inspecting first- and second-generation eMRTDs. From complex integration to secure transmission, Entrust offers governments a proven solution for authenticating eMRTDs and strengthening overall border security.

**Cost-Effective**
From required integration to expert IT staff, the Entrust border security solution is the most cost-effective approach for accurately inspecting today’s advanced eMRTDs.

**Standards-Compliant**
Technology is compliant with all ICAO standards, including Basic Access Control (BAC) and Extended Access Control (EAC).

**Government-Grade**
Proven Entrust ePassport solutions have been deployed in 15 countries, who collectively have issued more than half of the world’s ePassports in use today. Entrust solutions are also used by more than 45 countries and more than 60 U.S. federal agencies.

<table>
<thead>
<tr>
<th>ICAO Public Key Directory</th>
<th>Domestic No-Fly Lists</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participating in ICAO’s PKD is critical to verify the authenticity of ePassports from other countries. And, conversely, other countries can help identify fraudulent ePassports being issued in another country’s name.</td>
<td>Entrust can also establish integration with a border agency’s own domestic no-fly lists. This helps keep individuals of interest from crossing borders without additional investigation, improving border security for all countries.</td>
</tr>
</tbody>
</table>
The First Generation: Basic Access Control

The initial generation of ePassports uses Basic Access Control (BAC), which features passive and optional active authentication, and is in production in many parts of the world.

The European Union member countries were required to issue ePassports containing facial images secured via BAC by August 2006. The U.S. mandated the same for the Visa Waiver Program countries by October 2006.

This functionality, based on X.509 PKI (CSCA), provides verification that the document was signed by the legitimate issuing authority and the data stored on the chip has not been changed since issuance.

The Evolution: Extended Access Control

Countries are now evolving their ePassport programs to a second-generation framework that includes capabilities for Extended Access Control (EAC).

Entrust is participating in related standards bodies and has released security solutions to meet the certificate management requirements of EAC (CVCA PKI).

Through terminal and chip authentication, EAC aims to increase the security of MRTDs through enhanced protection of biometric data (e.g., iris scan and/or fingerprint) stored on the contactless chip in the ePassport.
**Standardization on PKI**

In order to facilitate interoperability across countries, ICAO has helped drive global standards for ePassport implementation. Since ePassports contain sensitive personal information, security and integrity are critical.

Public key infrastructure, or PKI, is an integral technology for the security and verification infrastructure for ePassports.

Entrust provides leadership for the security of these important and sensitive documents through software solutions that reduce fraud by verifying the integrity of the personal and biometric data contained on the chip imbedded in the ePassport.

The use of digital certificates and PKI provides flexibility and extensibility, enabling a wide variety of security functions to assist government agencies as they face the challenge of secure travel document issuance. The PKI capabilities used for an ePassport deployment also may be leveraged for other citizen identity documents such as national ID cards or travel visas.

Entrust’s solutions, together with an ePassport vendor’s front-end passport issuance software and back-end border control readers and software, provide the front-to-back ePassport “trust framework.”