



# < Let's Talk

## Entrust ePassport Solutions

### Extensible Solutions for Today and Tomorrow

Security concerns, developing technologies and emerging standards have led governments worldwide to pursue the issuance of more sophisticated machine-readable travel documents (MRTD) to their citizens. Commonly known as “ePassports,” these documents contain a chip that stores information that can be verified against the data on the passport.

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

PKI has become 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 key values of digital certificates and PKI are 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 can 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.”

### Interoperable. Reliable. Proven.

Entrust is the pioneer of PKI technology, which serves as the backbone for securing sensitive information on today’s ePassports. We believe that Entrust is the only vendor capable of handling the scale, complexity and reliability demanded by the new Extended Access Control (EAC) framework.

**Interoperable.** Entrust strives to maintain and expand technology integration and interoperability with many of the leading vendors that provide additional hardware and software components used in MRTD issuance and verification.

### Why Entrust?

- Governments worldwide rely on Entrust
  - Used by 35-plus governments to secure extensive trust environments
  - In use for the largest and most complex ePassport environments
- Unparalleled world leader in the PKI technology underpinning ePassports
  - 15-year track record helping customers achieve scalable, critical PKI in complex, cross-border environments
  - Only PKI solution that enables governments to upgrade security seamlessly
  - Extensive partnerships with the world’s leading ePassport and technology vendors
  - Active player in international standards development
- Only vendor capable of handling the scale, complexity and reliability demanded by EAC
  - Solution manages certificates throughout EAC architecture and provides security for their distribution
  - Flexible four-tier (CVCA, DVCA, Concentrator and IS Workstations) EAC solution with advanced management features and GUI that simplify the display of complex EAC environmental relationships

**Reliable.** Entrust’s PKI technology is dependable, and is currently used by more than 35 governments to secure the largest, most complex trust environments across the world. Entrust has a 15-year track record helping customers achieve critical, scalable PKI in complex, cross-border environments.

**Proven.** Entrust is acting as a trusted advisor to many countries as they pursue ePassport projects. Our software is currently in production use in some of the largest and most complex ePassport environments in the world, including the United States, Canada, New Zealand Ireland, Slovenia, Singapore, and Taiwan.

### ePassports: The First Generation

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 of ePassports: Extended Access Control

Countries are now evolving their ePassport programs to a second-generation framework that includes capabilities for Extended Access Control (EAC). EU member countries are required to add fingerprint and/or iris pattern data to MRTDs with the biometric information protected through the EAC scheme. Entrust is participating in related standards bodies and has released security solutions to meet the certificate management requirements of Extended Access Control (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.

### Entrust BAC and EAC ePassport Solutions

Specifically, Entrust has two ePassport security solutions: **Country Signing Solution (also known as BAC)** and **Country Verifying Solution (also known as EAC)**, each of which is briefly described below.

	Basic Access Control (BAC)	Extended Access Control (EAC)
<p><b>Primary Benefits of First- and Second-Generation ePassports</b></p>	<ul style="list-style-type: none"> <li>• RFID chip contains electronic version of printed contents</li> <li>• Encrypted transfer of data (30- to 60-bit)</li> <li>• Chip contents digitally signed by passport office; cannot forge legitimate signature</li> <li>• Border control can compare printed contents, electronic version and appearance of person</li> <li>• Potential for machine-matching of facial photo</li> </ul>	<ul style="list-style-type: none"> <li>• Inclusion of advanced biometric data (e.g., fingerprints, iris scans) that are highly resistant to impersonation (low false-acceptance rate)</li> <li>• Stronger encryption of data in transfer (128-bit)</li> <li>• Chip contents cannot be duplicated or “cloned”</li> <li>• ePassport reader terminal authenticates itself to the ePassport</li> <li>• RFID chip will only release advanced biometrics to trusted readers</li> <li>• Improved international verification approach</li> </ul>

### Entrust Country Signing Solution

- Protects the digitized, personally identifiable information and the digitized photograph;
- Provides data integrity and passport authenticity (named “passive authentication” by ICAO);
- Consists of an X.509 certificate-based PKI certification authority (CA) termed the Country Signing Certificate Authority (CSCA), as well as a Document Signer (DS) that digitally signs each ePassport;
- The Entrust Document Signer consists of three separate, yet tightly integrated, software components:
  - The Signature Delivery Service (SDS), which exposes a Web service interface as the integration point between external personalization and printing systems, and the signing function of the DS;
  - The Verification Server (VS), which acts as a credentialing end-point from a PKI perspective and performs the signing operation on the passport data;
  - The Offline Token Creation Utility (OTCU), which allows for submission and fulfillment of certificate signing requests from the DS to the CA in situations where the CA is operated offline and/or there is no network connectivity between the CA and DS.
- The CSCA and DS each use hardware security modules (HSMs) to store and protect their PKI keys.

### Entrust Country Verifying Solution

- Protects access to the digitized biometrics (fingerprints and/or iris scans);
- Provides authentication between the MRTD and the inspection station to control release of the biometrics (named “terminal authentication” by ICAO)

- Consists of a card-verifiable, certificate-based PKI CA termed the Country Verifying Certificate Authority (CVCA); a sub-CA known as a Document Verifier (DV) that provides keys; and certificates to issuance and border control systems. For passport validation at issuance and in border control environments, distributed (workstation) and centralized (server) software components fully automate key and certificate management for EAC-enabled inspection. The EAC Client and EAC Concentrator, coupled with the inspection station software and hardware, provide the mutual authentication required for EAC-enabled inspection;
- The CVCA, DV, EAC Concentrator and EAC Client are typically deployed with hardware security modules (HSMs) to store and protect PKI keys.

By managing the full lifecycles of certificate-based digital identities, Entrust Authority PKI serves as the core of Entrust’s ePassport solution. Entrust’s proven PKI enables encryption, digital signature and authentication capabilities to be consistently and transparently applied across a broad range of applications and platforms.

To date, countries wishing to establish trust for purposes of validating others’ first-generation (Basic Access Control) eMRTDs have manually exchanged Country Signing CA (CSCA) certificates through diplomatic channels — an inefficient, time-consuming process.

To encourage more rapid adoption of first-generation eMRTDs, as well as ease issues with boot-strapping cross-jurisdiction trust, the ICAO defined the Master List Signer (MLS). While not replacing the need for countries to independently establish the veracity of country CSCA certificates, the MLS provides a mechanism to support trust decisions.



# < Let's Talk

A Master List is created by a country that has established trust in a number of foreign CSCA certificates by placing those certificates on a list and digitally signing that list with a Master List Signing credential issued by its own Country Signing CA. The country then uploads the list to the ICAO public key directory (PKD) where it can be downloaded by any member nation.

A country that has placed a given CSCA certificate on its Master List does not, in itself, mean that another country can trust its veracity, but it does show that the Master List Issuer has established that trust. Retrieval of a CSCA certificate from a number of Master Lists raises the assurance that trust can be established.

Entrust ePassport Solutions and the Entrust Credentialing Service provide a commercial Master List Signing capability that enables countries to efficiently manage the Master List Signing process. Entrust also uses a domestically deployed Master List to provide a domestically rooted trust mechanism for secure automated distribution of eMRTD validation material to inspection systems.

## PKI for Citizen Identification

Government organizations looking to provide citizen identification and authentication to government services face a number of challenges related to accessibility, usability, security and privacy. Entrust has worked with numerous government organizations across the world to extend secure government services to citizens while keeping private information secure.

This model provides greater and more convenient access, increases trust for the citizen while reducing costs and increasing efficiency for the government. A variety of approaches to citizen authentication can be used, including citizen ID cards, ePassports, digital certificates or strong authentication. Entrust offers a flexible set of authentication solutions designed to meet a variety of citizen ID and e-authentication requirements.

## About Entrust

Entrust provides identity-based security solutions that empower enterprises, consumers, citizens and Web sites in more than 4,000 organizations spanning 60 countries. Entrust's identity-based approach offers the right balance between affordability, expertise and service. For strong authentication, fraud detection, digital certificates, SSL and PKI, call 888-690-2424, e-mail [entrust@entrust.com](mailto:entrust@entrust.com) or visit [www.entrust.com](http://www.entrust.com).

**Entrust**<sup>®</sup> Securing Digital Identities & Information

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc. or Entrust Limited in certain countries. All other company names, product names and logos are trademarks or registered trademarks of their respective owners. © Copyright 2010 Entrust. All rights reserved.

## Discover Entrust

Expertise in identity-based security has been a hallmark of Entrust since we began developing best-in-breed solutions more than 15 years ago. We are proud of the value Entrust provides to government customers across the world. Entrust would be pleased to share our experiences and lessons learned related to ePassport and citizen identification.

## Contact Us

North America: 1-888-690-2424  
EMEA: +44 (0) 118 953 3000  
E-mail: [entrust@entrust.com](mailto:entrust@entrust.com)

## Try EAC & SPOC

Entrust has established an EAC demonstration and SPOC Interop Facility Web site.

To register for access to the site, please visit:  
<https://www.entrust.com/forms/eac-demo/index.htm>

