

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 is verified against the data on the passport.

Standardization on PKI

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.

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.”

Entrust — The ePassport Standard

Entrust is the pioneer of PKI technology, which serves as the backbone for securing sensitive information on today’s ePassports. And Entrust is one of the few vendors capable of handling the scale, complexity and reliability demanded by the 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.

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.

Why Entrust?

- **Governments worldwide rely on Entrust**
 - Used by 35-plus governments to secure the largest, most complex trust environments
 - In use for the largest and most complex ePassport environments
- **Unparalleled world leader in the PKI 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

Proven. Entrust is acting as a trusted adviser 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, Ireland, Slovenia, Singapore, Taiwan and New Zealand.

Mastered. Entrust provides commercial Master List Signing capabilities that enable 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.

Integrated. Entrust provides seamless integration into the ICAO Public Key Directory (PKD), which is critical to verify the authenticity of ePassports from other countries. 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.

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.

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



Entrust BAC & EAC ePassport Solutions

Entrust has two specific ePassport security solutions: Country Signing Solution (also known as BAC) and Country Verifying Solution (also known as EAC), each of which is outlined in the following table.

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.

Entrust Country Signing Solution (BAC)	Entrust Country Verifying Solution (EAC)
Protects the digitized, personally identifiable information and the digitized photograph	Protects access to the digitized biometrics (fingerprints and/or iris scans)
Provides data integrity and passport authenticity (named "passive authentication" by ICAO)	Provides authentication between the MRTD and the inspection station to control release of the biometrics (named "terminal 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 CVCA, DV, EAC Concentrator and EAC Client are typically deployed with hardware security modules (HSMs) to store and protect PKI keys
<p>The Entrust Document Signer consists of three separate, yet tightly integrated, software components:</p> <ul style="list-style-type: none"> • 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. 	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
The CSCA and DS each use hardware security modules (HSMs) to store and protect their PKI keys	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; EAC Client and EAC Concentrator, coupled with the inspection station software and hardware, provide the mutual authentication required for EAC-enabled inspection

SECURITY
ON

Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

Entrust's identity-based solutions empower enterprises, consumers, citizens and websites in more than 5,000 organizations spanning 85 countries. This 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**, email entrust@entrust.com or visit entrust.com/epassport.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 globally

Headquarters

One Lincoln Centre
5400 LBJ Freeway, Suite 1340
Dallas, Texas 75240 USA

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

About Entrust

A trusted provider of identity-based security solutions, Entrust empowers governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL. For more information about Entrust products and services, call 888-690-2424, email entrust@entrust.com or visit www.entrust.com.

Entrust[®] 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 2012 Entrust. All rights reserved.