Entrust Datacard™

Entrust ePassport Solutions

Issuance & Inspection Technology for ePassports

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.

Interoperable, scalable and validated by third-party testing, Entrust ePassport solutions provide the necessary capabilities — whether via a hosted or in-house model — for the proper issuance and inspection of today's advanced ePassports.

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.

Trusted Worldwide

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.

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.

Mastering the Process

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.

+1-888-690-2424

entrust@entrust.com
entrust.com/ePassport

@EntrustDatacard
+entrust
/EntrustVideo
/EntrustSecurity

DOWNLOAD
THIS
DATA SHEET

Solution Benefits

- Used by 35-plus governments to secure the largest, most complex trust environments
- 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
- 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

Trusted Document Issuance & Inspection

Based on trusted PKI technology, Entrust provides solutions for first- and second-generation ePassports. In fact, ePassport technology is based on two current standards: Basic Access Control (BAC) and Extended Access Control (EAC).

Entrust offers 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, IS Concentrator and IS Client are typically deployed with hardware security modules (HSMs) to store and protect PKI keys
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	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; IS Client and IS Concentrator, coupled with the inspection station software and hardware, provide the mutual authentication required for EAC-enabled inspection

Secure Issuance

Whether for simple BAC ePassports or a more advanced EAC framework, Entrust provides the proven solutions to properly and securely issue ePassports for multimillion-user populations. Entrust is a 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 EAC framework.

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."

Advanced Inspection

Advanced ePassport travel documents aren't effective unless properly inspected. Entrust provides the necessary components for proper document inspection — from a single, proven vendor — and can include integration with both the International Civil Aviation Organization (ICAO) PKD as well as domestic no-fly lists.

By leveraging proven hosted or in-house public key nfrastructure (PKI) technology, Entrust provides border control agencies the ability to properly read and verify first- and second-generation eMRTDs. For organizations who opt for the hosted service, this approach simplifies deployment by removing the need for dedicated hardware, facilities and expertise.

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.

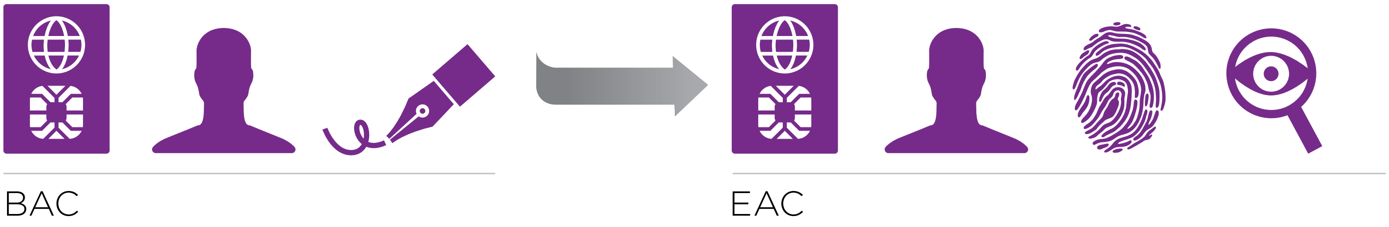
This functionality, based on X.509 PKI (CSCA), provides verification that the document was signed by the legitimate issuing authority and the data stored on the chip has not been changed since issuance.

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	○ 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	○ 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

About Entrust Datacard
Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

Entrust Datacard™