# eMRTD PKI

## Machine-Readable Travel Document PKI

Enables certificate generation and management to authenticate electronic documents and secure access to biometric data stored in the identity document's chip in compliance with ICAO standards.

### A reliable and flexible PKI

The purpose of the eMRTD PKI system is to provide a set of components allowing deployment in various configurations, depending on countries' standard application and management policies.

In its most comprehensive setup, the system provides a PKI complying with ICAO and EU-EAC standards, supporting both document signing and verification. Components can also be delivered individually to offer flexible integration or migration within an identity ecosystem.

### IN Groupe's eMRTD PKI includes two sub-PKIs:

- International Civil Aviation Organization PKI (ICAO PKI): Part of a passport management system, it ensures secure management of ICAO-compliant travel documents.
- Extended Access Control PKI (EAC PKI): An enhanced security infrastructure based on ICAO standards with additional EU recommendations—its purpose is to safeguard sensitive information stored in the document, such as fingerprints and iris data.

### Main components

IN Groupe's eMRTD PKI, or System-One PKI, includes major components such as:

- CSCA (Country Signing Certification Authority): The root certification authority (CA) for travel documents.
- NPKD (National Public Key Directory): Provides connection capabilities with the ICAO Public Key Directory (PKD) to enable secure exchanges with member countries.
- CVCA (Country Verifying Certification Authority): The root CA for a document verification system.
- I3S (ICAO Inspection System): The end point of the verification system, allowing terminals to read an eMRTD chip and access data protected under EAC.

The eMRTD PKI solution is deployed with hardware security modules (HSMs) that generate, keep, and protect the cryptographic keys.

Standalone solutions, such as IN Groupe's NPKD and I3S, can be integrated independently. IN Groupe's eMRTD PKI solution can be used in combination with Document Personalization System (IDPS) for document issuance and quality control.

## Key Benefits

**Compliant**

Conformity with ICAO 9303 and BSI latest standards, ensuring interoperability and security.

**Flexible**

Mature solution deployed in more than ten countries for over ten years.

**Durable**

Offers tailored solutions as part of a complete document personalization system or as stand-alone modules, meeting the unique needs of each customer.



# IN Groupe's eMRTD PKI includes two sub-PKIs:

## ICAO PKI

**CSCA**
The Country Signing Certification Authority is the root CA for travel document signatures. It receives certificate requests from the Document Signer (DS) and issues Document Signer Certificates as well as Certification Revocation Lists (CRLs).

**DS**
The Document Signer (DS) is the provider of signing services for document production. The DS generates certificate requests for validation by the CSCA.

**Additional optional services:**
BCS: The Bar Code Signer for non-chip-based documents
MLS: The Master List Signer module
DLS: The Deviation List Signer

**IN Groupe National PKD**
The National Public Key Directory centralises national and international certificates and acts as the interface between the ICAO PKD and a country's offline eMRTD ICAO PKI. It enables the secure exchange of certificates and allows border control systems to verify the authenticity of foreign ICAO-compliant travel documents.

## EAC PKI

**CVCA**
The Country Verifying Certification Authority is the root CA for a document verification system. It produces certificates for the Document Verifier (DV).

**DV**
The Document Verifier is a second-level CA with authority delegated by the CVCA of its own country. It signs Terminal Certificates, possibly transferring access privileges to the Inspection System (IS).

**IS**
The Inspection System is the end point used by the verification system at border control to perform multiple checks. It can also be used to enable complete document quality control.

**SPOC**
The Single Point of Contact interface allows the secure exchange of digital credentials required to access sensitive biometric data in EAC documents, from the document issuing country to the controlling country.

## CUTTING-EDGE TECHNOLOGY

**Security:** FIPS 140-2 level 3, HSM compatibility, data encryption, TLS-secured connection.

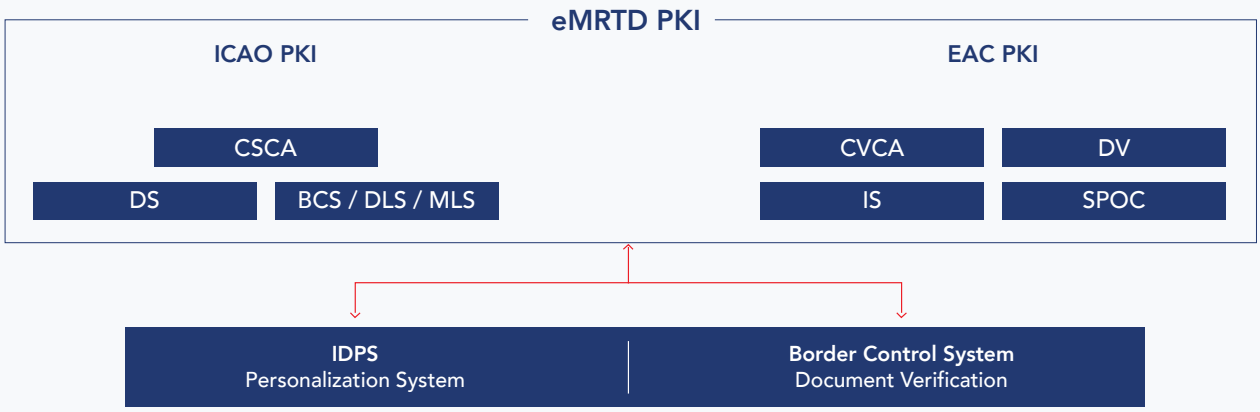
**Cryptography:** Most advanced algorithm (RSA up to 4096, ECDSA up to 512)

**Interface/APIs:** Web services applications, SOAP APIs

**User management and access control:** Active directory, role-based access control

**Standard compliancy:** ICAO Doc 9303 Ed 8, BSI TR-03110

**Field-proven:** Mature solution deployed in more than ten countries




April 2026
Copyright © 2026 IN Groupe. All rights reserved.
**www.ingroupe.com**