SECURE IDENTITY ALLIANCE

What is PKI?

Understanding Public Key Infrastructure

25 November 2022

1. Overview

Trust in passports is essential. Public Key Infrastructure (PKI) technology gives strong evidence that information on a secure passport chip can be trusted. This helps authorities issue more secure passports, increase security and throughput at the border, increase automation and catch identity cheats. It can help airports, airlines and commercial parties to check documents and carry out KYC (Know Your Citizen or Know Your Customer). Genuine passengers are more able to demonstrate their true identity quickly. Conversely, identity cheats stand a greater chance of being discovered.

Passport fraud is a very real threat! A genuine document can be lost, stolen or borrowed and then used by someone who is not the holder (an imposter or lookalike). A criminal might try to change the photograph or other data about the holder, to turn a passport into his own travel document (a forgery). A false passport might be manufactured (a counterfeit). Someone may make a false application to obtain a passport (a Fraudulently Obtained Genuine, or FOG). Or someone may steal blank passports which have not yet been personalised with holders' details.

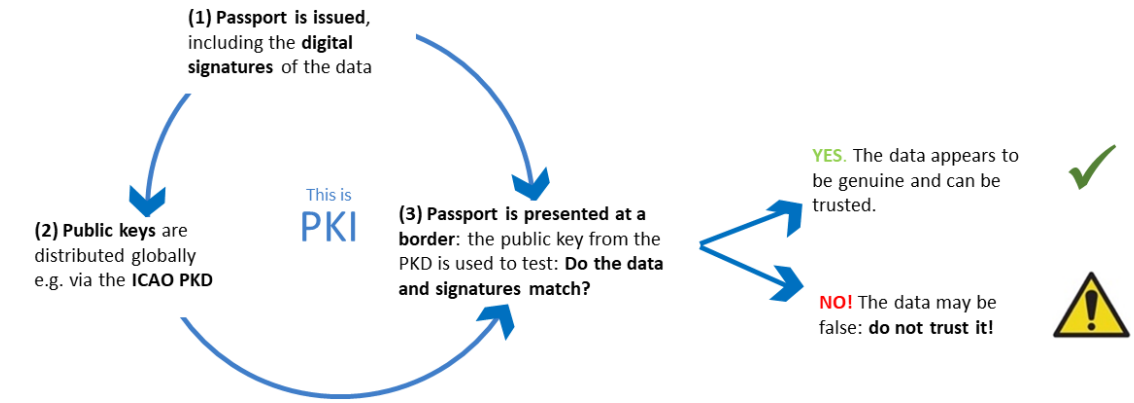
Great care is taken to defend passports from such attacks. This includes strong security in the manufacture, storage and delivery of documents; rigorous testing of new passport applications; and advanced security features in passports so that false documents are difficult to produce or use. See Passport Fraud Trends and Ways to Combat Them (SIA, 2021) and ICAO 9303, Machine Readable Travel Documents—see references.

Contents

2. How secure electronic chips improve security and convenience

Many passports and ID cards contain an electronic chip, holding key data about the document and the holder, including the holder's facial photograph. All of this data is protected by the issuer who includes a cryptographic digital signature on the chip. This signature, when verified, shows that data on the chip comes from the right source and has not been changed. Only the issuer can produce this signature, but everyone who needs to can verify that the signature and the data match. If so, it can be trusted; if not, it can't. The complete set of components is called a **Public Key Infrastructure (PKI)**. Here is a simplified, high-level description of how this works:

This is PKI



2.1. Issuing a new passport

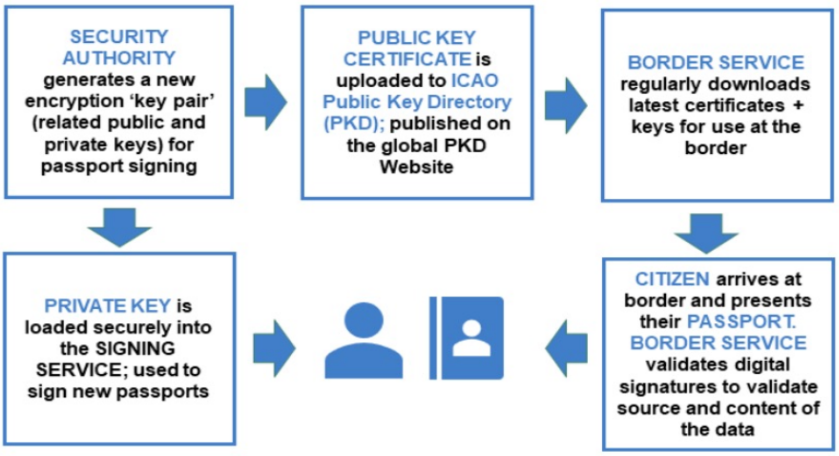
Signing data and loading it onto the secure chip

When someone applies for a passport and the application is accepted, information is prepared to appear in the physical document. A copy of the same data is made to go on the chip. A signing service then uses cryptography to generate digital signatures relating to the data. During personalisation, the information is written onto the blank passport, and the data including digital signatures are loaded securely into the chip.

2.2. Enabling authentication around the world

Publication via ICAO PKD

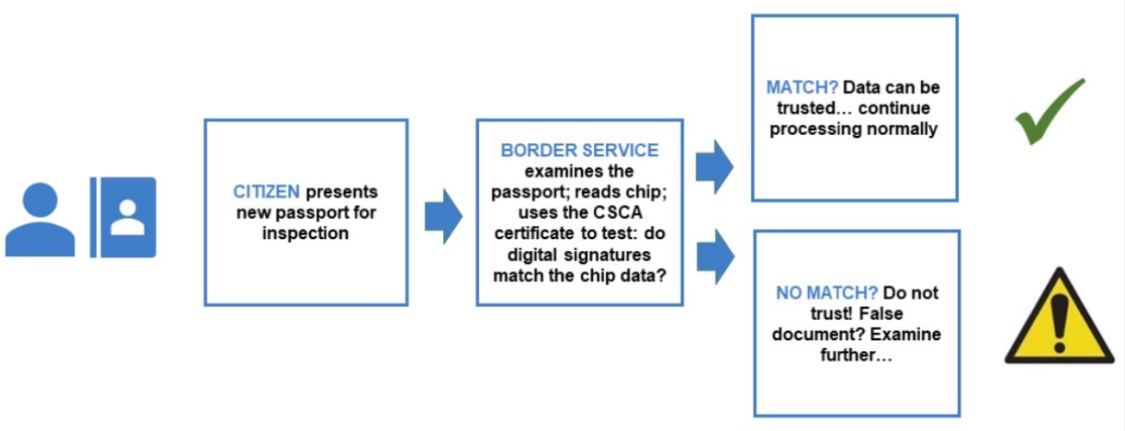
The passport issuer publishes a CSCA Country Signing Certificate, containing a public encryption key which validates signatures against the data they protect. However, that key does not let anyone generate a valid signature if data on the chip have been changed; only the issuer can generate valid signatures, using the corresponding private key. Certificates, with their public keys, can be shared via the ICAO Public Key Directory (PKD).



2.3. Authenticating the passport and chip data

Testing a passport at the border

When the passport is presented at a border the passport is inspected. Data on the chip is read and validated against the digital signatures. If the signatures do not match the data, this alerts the border service that the passport may be false and should not be trusted.



2.4. What is a digital signature?

A digital signature is an encrypted representation of some data that it protects. All of the data is processed to produce the signature. Provided security is maintained, only the genuine issuer can produce a genuine digital signature. If any of the data is changed after it is issued (such as substituting a different name or facial photo), when the signature is compared against the data it will not match, revealing that it cannot be trusted.

This assurance is achieved by a special form of encryption.

2.5. PKI depends on public key encryption

PKI relies on a smart form of encryption that uses a **pair** of encryption keys. One is the **public key** and can be shared with anyone; the other is the **private key** which has to be kept secret. These are used as follows:

- The issuer uses the secret **private key** to make the digital signatures for the chip—this is called “signing” the data.
- The **public key** is used to verify that the digital signatures correctly match the data on the chip and comes from the authentic source. However, this key cannot be used to create authentic signatures, for example to sign false data.
- Two-key encryption like this is called **public key encryption**, and the complete end-to-end infrastructure is known as a **public key infrastructure (PKI)**.
- The **ICAO Public Key Directory (PKD)** is a convenient and secure means of publishing all necessary public keys within their certificates. This is an efficient one-stop shop for passport issuers and border services to exchange the data they need to share, though not all certificates are distributed this way.
- Each issuer operates a highly secure **Country Signing Certificate Authority (CSCA)** which holds the “master” signing keys for a country, to validate up to 5 years of document signing. The CSCA is the **root of trust** in the system and issues signed **public key certificates** (containing the public key) to the ICAO PKD or others.

2.6. Definitions

ICAO Symbol for a passport containing a secure chip

PKI Some important descriptions for PKI have been set out in these documents or by these contributors:

- **ICAO 9303**—global specification for passports including secure chips, by ICAO.
- **Technical Guidelines** on inspection, from ICAO and the German Federal IT Security Agency (BSI).
- **Protection Profile**—required security features to protect secure chips in passports / eMRTDs.
- **Extended Access Control (EAC)**—extends ICAO 9303 to protect access to biometrics of the holder are included on the chip. An EU version is mandated for EU passports and ID cards, containing two fingerprint images of the holder.
- **Algorithms for public key encryption**—the first commercial public key algorithm was **RSA** (Rivest, Shamir and Adleman); more recently, **Elliptic Curve**.

This completes a high-level description of passport PKI. More detail follows:

- Making PKI effective
- Communicating with the secure chip
- The Logical Data Structure (LDS) within the chip
- Certificate management
- Emerging issues, including Digital Travel Credentials (DTC) and Visible Digital Seal (VDS)
- Final words
- Glossary and references

3. Making PKI effective

As already explained, Public Key Infrastructure (PKI) technology assures authorities that information on a secure ePassport chip can be trusted, while making the authentication process smoother and more efficient. That said, it's important to understand that **passport PKI only works well if it is correctly and securely implemented**.

Proper implementation of PKI includes:

- Good understanding of the complex technology and communications infrastructure for PKI, end-to-end, in the design and operation of the system, complying with ICAO 9303 and other relevant standards and good practice.
- Strong IT security, including protecting against unauthorised access and cyberattacks, protecting private keys and critical functionality in Hardware Security Modules (HSMs).
- Good teamwork between stakeholders, including management and technical; and issuance and authentication. Non-expert stakeholders need the opportunity to understand key aspects of PKI in accessible terms so they can make informed decisions—bridging the gap between specialists and non-specialists.
- Membership of ICAO PKD and ensuring that new public keys are uploaded and shared in time to reach border services before corresponding private keys are used to sign new passports.
- Active management to acquire all public key certificates possible.

3.1. Talking to the Chip

Communicating with the secure electronic chip in an e-passport uses Near-Field Communication (NFC), which is a low-powered radio signal used when a payment machine talks to a contactless card. Several steps should be followed to read and authenticate an e-passport securely:

(1) Establish contact with the chip. A reader can use two mechanisms to access the chip: the original, **Basic Access Control (BAC)** is being replaced over time by **Password Authenticated Connection Establishment (PACE)**. PACE-only documents have been allowed since 2018 so today's passport readers need to be able to read both. The term **Supplemental Access Control (SAC)** refers to using PACE when both parties can do so, or BAC if not.

These steps **read** the data on the chip, but they **do not check whether the data and chip are genuine** (i.e., whether the e-passport can be trusted). Experts agree with ICAO recommendations that further steps (2) and (3) to authenticate the document are essential.

(2) Authenticate the DATA on the chip. After connecting to the chip, the reader verifies that the digital signatures correctly match the data on the chip. A correct match is essential as it proves that the data has come from the right originator and has not been amended, so can be trusted. This step is called **Passive Authentication (PA)**.

PA involves two levels of signing and authentication. **Document signing keys** are used to sign individual passports but are typically used only for a limited number of times before being retired. The document signing certificate stating the public key for a passport is included in the chip, and this certificate is signed by the **country signing key,** which is used to sign document signing certificates, for a maximum of 5 years.

Certificate Revocation Certificates (CRLs) and **Deviation Lists** are used by a passport issuer to notify all countries of technical errors or certificates that should not be relied on (for example, because security has been compromised). The issuer notifies ICAO of CRLs and Deviation lists so they can be included in the Public Key Directory (PKD). This ensures that Passive Authentication does not place trust in invalid data.

Master Lists (ML) can be included in the PKD which declare which public keys a country considers valid. This is useful source for making a consistency check but represents one country's view rather than ICAO's.

(3) Authenticate the CHIP. Another test is carried out to check that good (valid) data has not been copied (cloned) onto a false chip. This test is called **Chip Authentication (CA)**, or an earlier version, **Active Authentication (AA)**.

After (2) and (3) have been successfully completed, the passport reader now has evidence that the **chip** and its **data** can be trusted.

(4) EU fingerprints access. EU passports contain two fingerprint images of the document holder, to enable a simple and effective check on identity if necessary. This is subject to rigorous privacy control called **Extended Access Control (EAC)**. The process to verify this permission and unlock access to the fingerprints is **Terminal Authentication (TA)**. EAC requires the reading country to have authority from the country issuing the document: permission is exchanged via a **Single Point Of Contact (SPOC)** in each country.

3.2. Logical Data Structure (LDS)

Data is stored on a secure passport chip (an eMRTD) in a defined structure called the Logical Data Structure (LDS) including up to 16 Data Groups (DGs), as defined in ICAO 9303. The LDS definition includes:

- DG1 holds a copy of the Machine Readable Zone (MRZ);
- DG2 the facial image of the holder;
- DG3 fingerprints;
- DG4 eyes / iris; and
- the Document Security Object (SO_D) holds the digital signatures.

3.3. Certificate management

It is important that every country actively maintains its reference library of all the current public key certificates it needs to authenticate eMRTDs. This can for example involve regular checking of the ICAO PKD; following up certificates that are expiring, if relevant asking a source country to provide its successor public key certificates; making consistency checks of others' certificate library as declared in their Master List.

The ICAO Public Key Directory (PKD) enables participating countries (88 in November 2022) to share their respective public keys to facilitate easier controls around the world.

A recent initiative of ICAO is to make the public keys available to commercial entities in the private sector (e.g., banks, insurance and travel companies) so more entities would be able to verify data contained in ePassport chips. This generates facilitation and trust.

3.4. Emerging issues

Digital Travel Credentials (DTC)

ICAO are coordinating efforts to introduce a future form of the passport which will include a virtual component: the Digital Travel Credential (DTC). It could become possible for travellers to send the contents of their DTC electronically to the border services at their destination in advance; and it may be possible for a mobile phone to become an accepted form of passport in the future. The data structure of a DTC is similar to that of a standard ePassport, so it can also be verified using the PKD.

Visible Digital Seal (VDS)

This security solution uses PKI to sign and authenticate data on printed or visually represented documents such as a visa. VDS uses a QR 2D barcode. The barcode, when used to encode visa information, contains data such as the visa number, date of issue and the holder's name and passport number; plus a digital signature. A barcode like this cannot hold as much data as a passport chip. The barcode is read optically by the reader device, and then the signature is verified as for a passport chip. The relevant public key(s) are needed to verify a VDS, either from the ICAO PKD, or an alternative secure source. See references. New EU visas will include a VDS.

Two VDS standards have been defined: (1) the original version, in ICAO standard 9303 Part 13, used for visas and emergency travel documents; and (2) VDS-NC V1.3, used for vaccination / health certificates and for Digital Travel Authorisations (DTAs). These two are similar, but with some technical differences and additions. (NC stands for Non-Constrained.)

EU COVID Certificates (EUCC)

The PKI model used for these certificates has been successfully used at European level as part of the definition of QR Codes used to confirm vaccination, test results and recovery from COVID.

ICAO PKD can include certificates that can support verification of EUCC, VDS, VDS-NC and other health proof formats, as for ePassports and other ICAO-complaint electronic travel documents.

EU Identity and Travel Documents

The EU has strengthened European ID Cards and certain Residence Documents, bringing these into line with European Passports and Residence Permits which implement ICAO 9303 plus the EU requirements for fingerprint images (EAC, above). This is contained in EU Regulation 2019/1157, in force from 2 August 2021.

3.5. Is my encryption strong enough?

Computer power increases substantially over time (known as Moore's Law), so what is considered 'beyond computation feasibility' to break an encryption key today—therefore what is strong enough to resist attack now—may become unsafe in the future, requiring key lengths to be increased and, from time to time, stronger encryption algorithms to be introduced. **Quantum computing** may radically increase computer power beyond the existing trend. New forms of encryption are being examined to safeguard trust in the era of quantum computing in the future.

3.6. Final words

To emphasise the core message of this paper:

- The PKI model based on ICAO 9303 described here can give **trust** that data stored in the ePassport or eMRTD chip is genuine when it is presented at a border or elsewhere.
- To achieve that, the solution must be implemented **securely**, throughout, in what is a highly complex environment, requiring the full engagement of experts.

3.7. Glossary

AA	Active Authentication, an earlier version of CA
BAC	Basic Access Control (to communicate with the chip)
CA	Chip Authentication (verifies a chip is genuine, not a clone)
CAN	Card Access Number printed on an eMRTD, used in PACE
CSCA	Country Signing Certificate Authority, the root of trust in a country's PKI
DG	Data Group within the LDS, for example DG-1 (MRZ), DG-2 (face image), DG-3 (fingerprints)
DTA	Digital Travel Authorisation
DTC	Digital Travel Credential
EAC	Extended Access Control (uses TA)
eMRTD	electronic Machine Readable Travel Document (conforms to ICAO 9303)
EUCC	EU COVID Certificates
FOG	Fraudulently Obtained Genuine document such as a passport
HSM	Hardware Security Module (secure store for critical data, e.g. keys)
KYC	Know Your Citizen, or Know Your Customer
LDS	Logical Data Structure—how data is structured within the chip (see DG)
ML	Master List—the set of public keys believed correct by one country issuing the ML
MRZ	Machine Readable Zone—2 or 3 lines of data printed on the title page of an eMRTD, used in BAC
NFC	Near-Field Communication (low-powered communication from the reader to chip)
PA	Passive Authentication (verifies that data on a chip matches the digital signatures)
PACE	Password Authenticated Connection Establishment (improved form of BAC)
PKD	Public Key Directory
PKI	Public Key Infrastructure
PP	Protection Profile—security specification for an eMRTD chip
QR	A format of 2-D barcode (QR = Quick Response). See VDS.
SAC	Supplemental Access Control: uses PACE; or if not possible, BAC
SO_D	Document Security Object—holds digital signatures within the LDS
SPOC	Single Point Of Contact for exchange of EAC/TA permission between EU countries
TA	Terminal Authentication (used in EAC to unlock access to fingerprints)
VDS	Visible Digital Seal: uses a QR barcode with a digital signature for authentication

3.8. References

Passport Fraud Trends and Ways to Combat Them, Secure Identity Alliance, 2021 https://secureidentityalliance.org/ressources/blog/entry/passport-fraud-trends-and-ways-to-combat-them

ICAO: Basic Concepts of MRTD and EMRTD—Two-page factsheet
https://www.icao.int/meetings/tag-mrtd/tagmrtd22/tag-mrtd-22_wp24.pdf

ICAO Doc 9303, Machine Readable Travel Documents, 8th edition 2021, contents
https://www.icao.int/publications/pages/publication.aspx?docnum=9303

ICAO Doc 9303, Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs
https://www.icao.int/publications/Documents/9303_p2_cons_en.pdf

ICAO Doc 9303, Part 11: Security Mechanisms for MRTDs
https://www.icao.int/publications/documents/9303_p11_cons_en.pdf

ICAO Doc 9303, Part 12: Public Key Infrastructure for eMRTDs
https://www.icao.int/publications/Documents/9303_p12_cons_en.pdf

ICAO Doc 9303, Part 13: Visible Digital Seals
https://www.icao.int/publications/Documents/9303_p13_cons_en.pdf

ICAO Master Lists, ePassport and Health
https://www.icao.int/Security/FAL/PKD/Pages/icao-master-list.aspx

German Federal Office for IT Security (BSI): BSI TR-03135 Machine Authentication of MRTDs for Public Sector Applications
https://www.bsi.bund.de/EN/Service-Navi/Publications/TechnicalGuidelines/TR03135/TechnicalGuidelines_03135_node.html

EU Digital COVID Certificate
EU Digital COVID Certificate | European Commission (europa.eu)

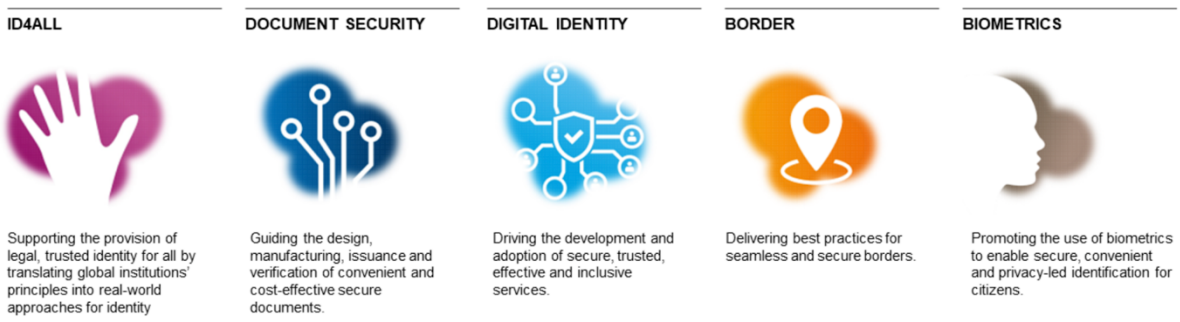
Keesing Technologies Platform: What is PKI? June 2022
Part 1: https://platform.keesingtechnologies.com/understanding-public-key-infrastructure-part-1/
Part 2: https://platform.keesingtechnologies.com/understanding-public-key-infrastructure-part-2/

3.9. About this paper

This paper was produced by the Document Security Working Group of the Secure Identity Alliance (SIA), Chair: Joachim Caillosse. The Lead Author is Frank Smith, SIA Associate Member. Thanks for all comments and contributions for the paper including those from colleagues outside the SIA. The paper was first published on Keesing Platform in two parts: Part 1 and Part 2, June 2022.

The SIA is an expert and globally recognised not-for-profit organisation. We bring together public, private and non-government organisations to foster international collaboration, help shape policy, provide technical guidance and share best practice in the implementation of identity programmes. Underpinning our work is the belief that unlocking the full power of identity is critical to enable people, economy and society to thrive.

Our workgroup programmes offer expert advice and pragmatic guidance, addressing issues throughout the identity journey



Shaping the future of identity

https://secureidentityalliance.org/