INCERT

GRAND-DUCHÉ DE LUXEMBOURG

Verifying the authenticity of ePassport certificates – Practical steps…

Taking you to the PKI highway

INCERT GIE

Author: Benoit Poletti

Agenda

1. INCERT GIE overview

Who are we ?

INCERT GIE is a **Luxembourgish public agency** responsible for:

1. **Managing mutualized and dedicated PKIs**, as well as **trusted back-end infrastructures** (supporting cryptography based solutions);

2. **Managing governmental CAs** used for the production and verification of travel and secure documents (i.e. ePassport, eResidence Permit and eID card);

3. **Personalizing smart cards** as well as **PIN and PUK codes letters**; and

4. **Representing Luxembourg at standardisation committees** within specific information security domains (e.g. PKI, cryptographic algorithms and cyber security).

Recognized in Luxembourg as a **centre of expertise within PKI/cryptography domain** serving public and private sectors

2. Verifying the authenticity of ePassport certificates 1/3

Verifying the electronic authenticity of an ePassport consists, in particular, in **checking the following elements**:

1. The **Country Signing Certification Authority (CSCA) certificate** - identifying the country having issued such eDocument; and
2. The **Document Signer (DS) certificate** - identifying the signer of the eDocument issued by the CSCA.

These digital certificates need to be checked for:

1. Their **conformity** ("profile" - against ICAO technical specifications);
2. Their **correctness** (do not include malicious code); and
3. Their **origin** (coming from the country they claim to be issued by).

2. Verifying the authenticity of ePassport certificates 2/3

At the border - how does it work from a practical perspective?

@ Verification steps
&
@ Authentication steps
Are inseparable

Data (e.g. holder's name, first name, facial image, fingerprints) contained in the contactless chip

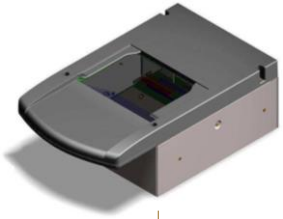
Data digitally signed by the country having issued the ePassport

1

1

Collection from the contactless chip of information required to **verify the CSCA and DS certificates of the country** having issued the ePassport

Reader



Country

For example, checking the origin of the certificates

Trusted sources of CSCA certificates

Bilateral exchanges

Schengen CSCA master list (project)

Trusted source of DS certificates

Public Key Directory managed by ICAO

2

2

Providing the CSCA and DS certificates

2

Verification of the CSCA and DS certificates

2. Verifying the authenticity of ePassport certificates 3/3

What are the risks when not **verifying** (or **not adequately verifying**) ePassport certificates?

Not verifying ePassport certificates

A **fraudulent ePassport** will be then **detected only** by **checking the existence of graphical security features** (e.g. UV, IF, microtext), with regard to **sanctions and watch lists**.

*Not **adequately** verifying ePassport certificates*

Fraudulent CSCA and DS certificates may not be **detected**.

- Already years ago, **counterfeit ePassports** from countries with **fraudulent certificates** were identified.

- **Malicious code in certificates** can **adversely impact** (crash) the system supporting the reader.

3. Increasing collaboration

To summarise:

1. **Relying** nowadays **only on graphical security features** when checking an ePassport **should not be an option anymore**.

2. **Countries** should **share digital certificates** for facilitating the **verification of the electronic authenticity** of ePassports issued.

Trusted sources of CSCA certificates

Bilateral exchanges

Schengen CSCA master list (project)

ICAO CSCA master list (Q3/Q4 2017)

Trusted source of DS certificates

Public Key Directory managed by ICAO

To conclude:

1. **Increasing collaboration** between parties (i.e. countries, private entities) **is deemed necessary** to **improve the awareness and technical capability** at border controls (or for mobile police units) of **the verification of the electronic authenticity of issued ePassports**.

Tutorial (awareness initiative) jointly produced by  and  for ICAO Public Key Directory organisation.

ePassport validation process

Example #1 of collaboration

The ePassport validation process can be explained in 4 steps.
Please click on the links in the menu on the left for some important background information and more information about each step.

Already available at the following URL:

INCERT https://www.incert.lu/upload/PKD/index.html#/

Available soon (Q2/Q3 2017) at the ICAO web site:
http://www.icao.int/Pages/default.aspx

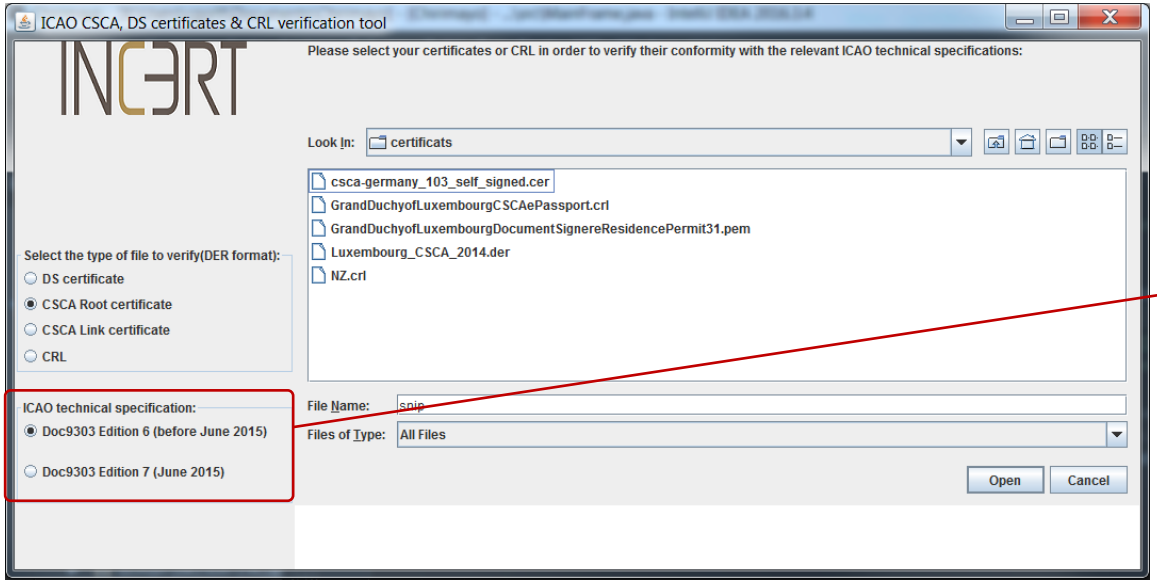
3. Increasing collaboration

Application (technical capability) produced by  to serve the community.

As a reminder, CSCA and DS certificates need to be checked for:

1. Their **conformity** ("profile" against ICAO technical specifications);
2. Their **correctness** (do not include malicious code); and
3. Their **origin** (coming from the country they claim to be issued by).

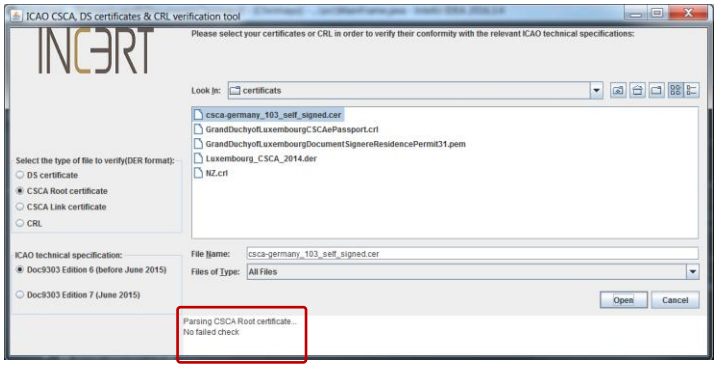
Example #2



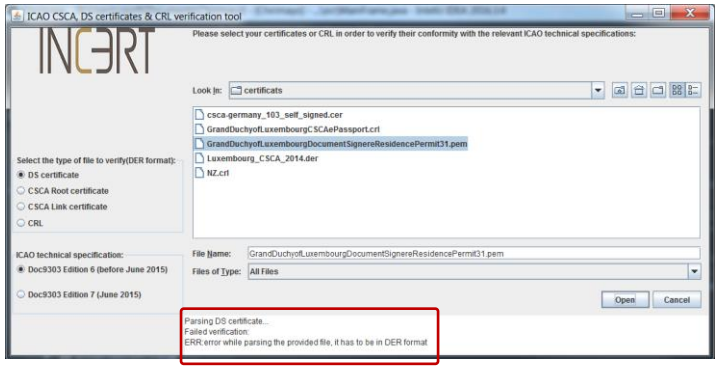
Current version of the application addresses **item #1**.

3. Increasing collaboration

Portable application developed in Java that can be adapted on workstations or mobiles.



Conformity check successful.



Conformity check unsuccessful.

Application "roadmap"

1. **Correctness** (Q3 2017); and
2. **Origin** (Q4 2017).

Still some work to be done, any support from relevant, collaborative parties (i.e. countries, private entities) is welcome!

Open-source application (freely) available at the following URL:

INCERT https://github.com/incert/ICAO-CSCA-DS-verification-tool

4. Questions / Answers

Any question?

Benoit POLETTI
Directeur
INCERT GIE
Address: IVY Building, 13-15 Parc d'activités, L-8308 Capellen, Grand-Duchy of Luxembourg
Office: +352 273 267 1
Fax: +352 273 267 32
Email: contact@incert.lu