PKD – Luxemburgish national implementation

INCERT GIE

Where PKI meets trust services, travel documents & cyber security

Author: Clement Gorlt

Agenda

1	**INCERT GIE overview**

2	**PKD structure**

3	**Luxembourgish national implementation**

4	**Questions / Answers**

1. INCERT GIE overview

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

1. **Managing governmental CAs** used for the production and verification of Luxembourgish travel and secure documents (e.g. ePassport, eID card);

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

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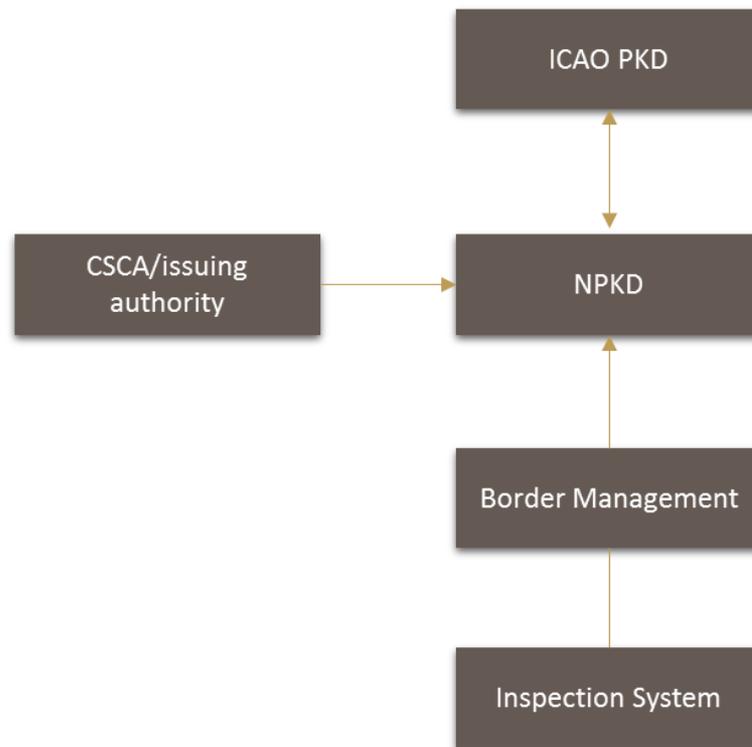
Recognized in Luxembourg as a **centre of expertise within PKI/cryptography domain** serving public and private sectors

2. PKD structure

ICAO defined the NPKD as the replicate of the remote PKD server at Montréal

It should be updated with PKD content regularly and serve as national focal point to access PKD information (and thus reduce the overhead on the central server).

INCERT GIE – PKD – Luxembourgish national implementation V1.0   Classification: Unclassified   © 2017 INCERT GIE

3. Luxembourgish national implementation

As for the migration to Veridos vendor, we had to create new NPKD to prepare for migration.

For time constraint, we focus on the very minimum:

The NPKD was composed of

- A server

- A default Linux operating system

- An open-source LDAP package for Linux (called openldap; the whole structure was copied from ICAO PKD)

- Few scripts to perform default functionalities like

  - PKD download twice a day,

  - Certificate and CRL upload (to be called manually by our operator to upload content),

  - And also an LDAP Backup script

3. Luxembourgish national implementation

Once the migration was over, we extend it a bit:

- New LDAP branch for all CSCA trusted by Luxembourg (that do not come from PKD)
- New script for assessing CRL present and look for more recent one if they are available in internet (through CDP)

Next improvement area, is to look at accessing Interpol SLTD from our NPKD, to allow border to retrieve all necessary information be it Certificates for ePassports validation or document verification against watchlist.
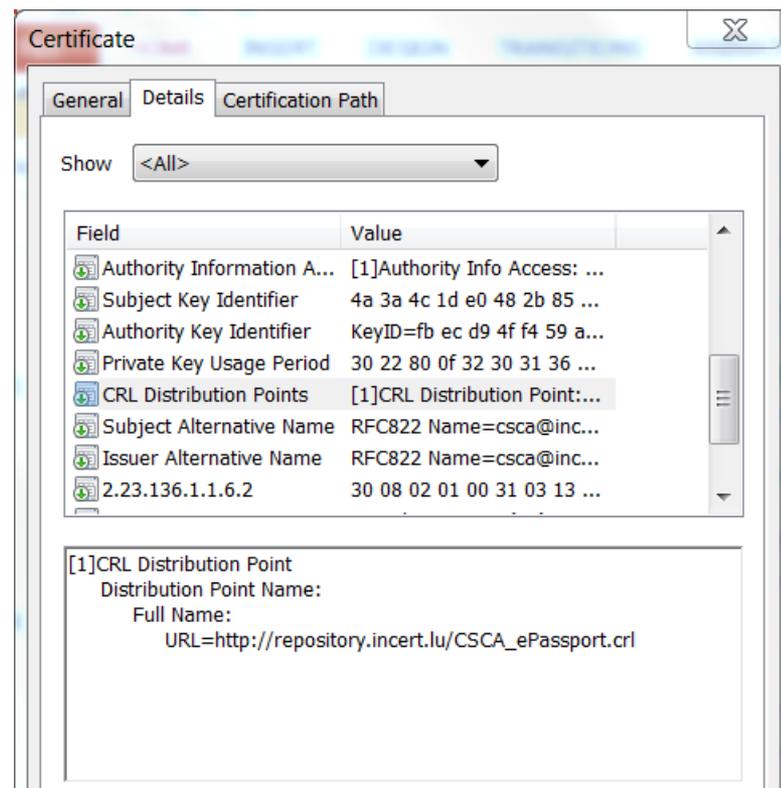
3. Luxembourgish national implementation

Summary:

- If kept to the official role, setting up a NPKD can be really straight forward and not complicated.

- The fees are recurrent each year and need to be integrated into the long-term budget

- PKD implementation and maintenance can be done with « normal » IT people (and most of the tasks can be automated) in opposition to PKI for ePassport issuance, which require potentially more PKI operator profile than IT ones.

Classification: Unclassified   © 2017 INCERT GIE

4. Questions / Answers

Any question?

Clément GORLT

INCΞRT

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