



International Civil Aviation Organization

Sixth Symposium and Exhibition
on ICAO MRTDs, Biometrics
and Security Standards

ICAO Headquarters, Montréal, Canada
1 - 4 November 2010



Joining the PKD – why?

Experiences of Switzerland

State of Play Switzerland

The first generation e-passport is being issued since 4 September 2006

- Name, first name
- Passport number
- Date and place of issue, expiry date
-



+
from 1 March 2010

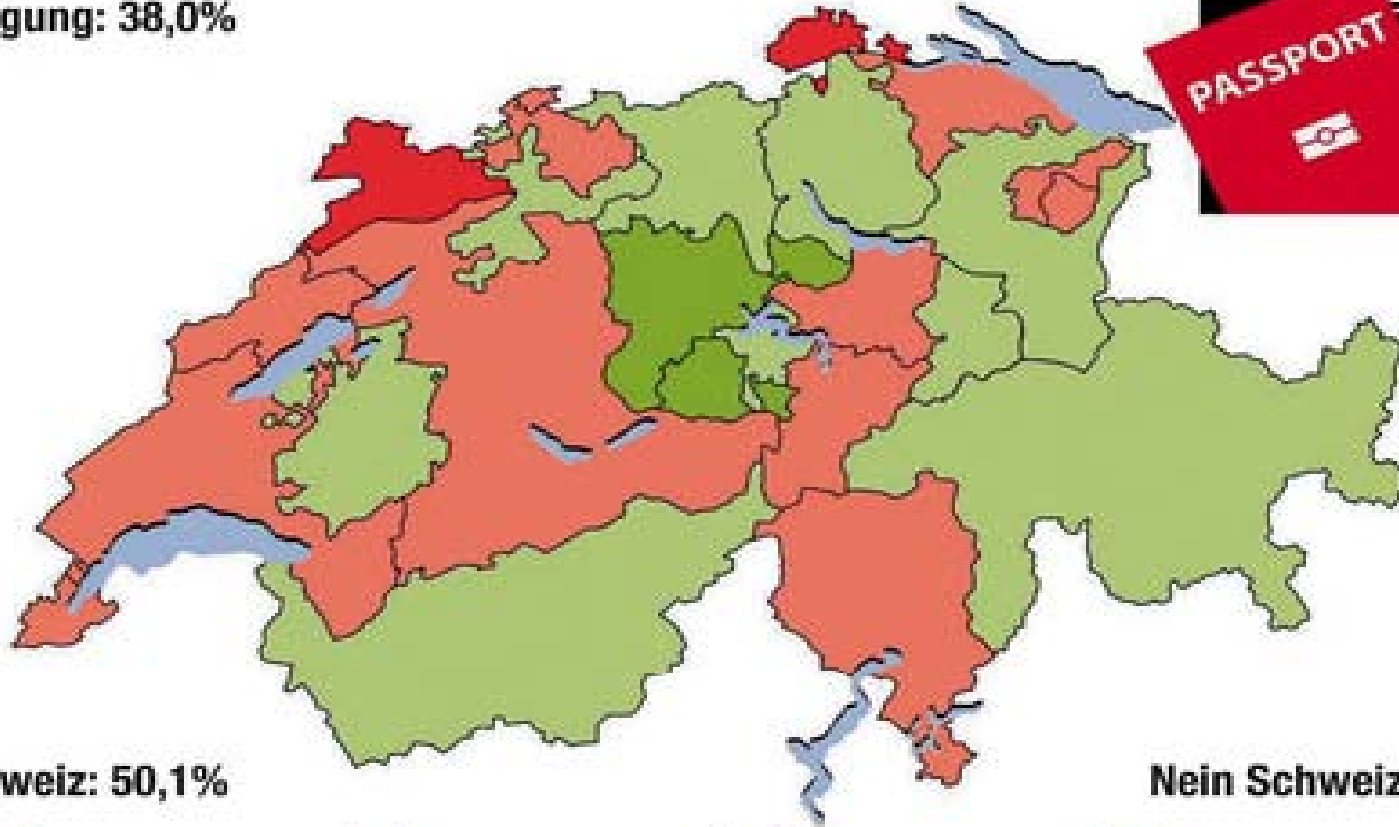


Public Vote on e-passports

Eidg. Abstimmung – Biometrischer Pass

Beteiligung: 38,0%

PASSPORT



Ja Schweiz: 50,1%

Nein Schweiz: 49,9%

Ja  unter 45%

 45–49,9%

 50–54,9%

 55% und mehr



Why are certificates necessary?

Headline in St. Galler Tagblatt – 19 August 2009:
(Daily Swiss newspaper)

**“Passport can be copied and altered
in 12 minutes”**

“New ID cards are supposed to be
'unforgeable' - but it took our expert 12
minutes to clone one, and programme it with
false data” (6 August 2009, Daily Mail (UK))



Our responses to these fears

- E-passports are secure.
- Altered e-passports will be detected by a properly set up border control operation, that validates the signatures.
- The electronically stored biometric data (including the certificates) are an additional measure against document fraud by allowing a reliable 1:1 match.
- **Switzerland participates in the ICAO-PKD.**




Objectives of Switzerland

- Assure the balance between the need for additional security and customer/citizens needs.
- Generate a big as possible benefit from e-passports.
- Offer the citizens an added value for the money invested, i. e. automated fast, reliable border controls.



Some arguments for not joining

- It's too expensive! 
- Bilateral exchange works good enough
- It's not necessary – DS certificates are (mostly) on the chip
- It's too complicated – we must first introduce e-passports



Reasons to join

- Switzerland invested about € 20 millions to introduce the 2nd generation e-passport.

ICAO-PKD registration fee: USD 56'000

ICAO-PKD annual fee (technical participation + ICAO budget contribution): USD 60'150

Costs will go down when more countries join.

Figures according to: Document B-Fin/35 PKD Fee Schedule 13.9.2010)

- Swiss passports shall be validated rapidly worldwide allowing our citizens to travel hassle free. How much is this worth to you, how much is the trust in your passport worth?



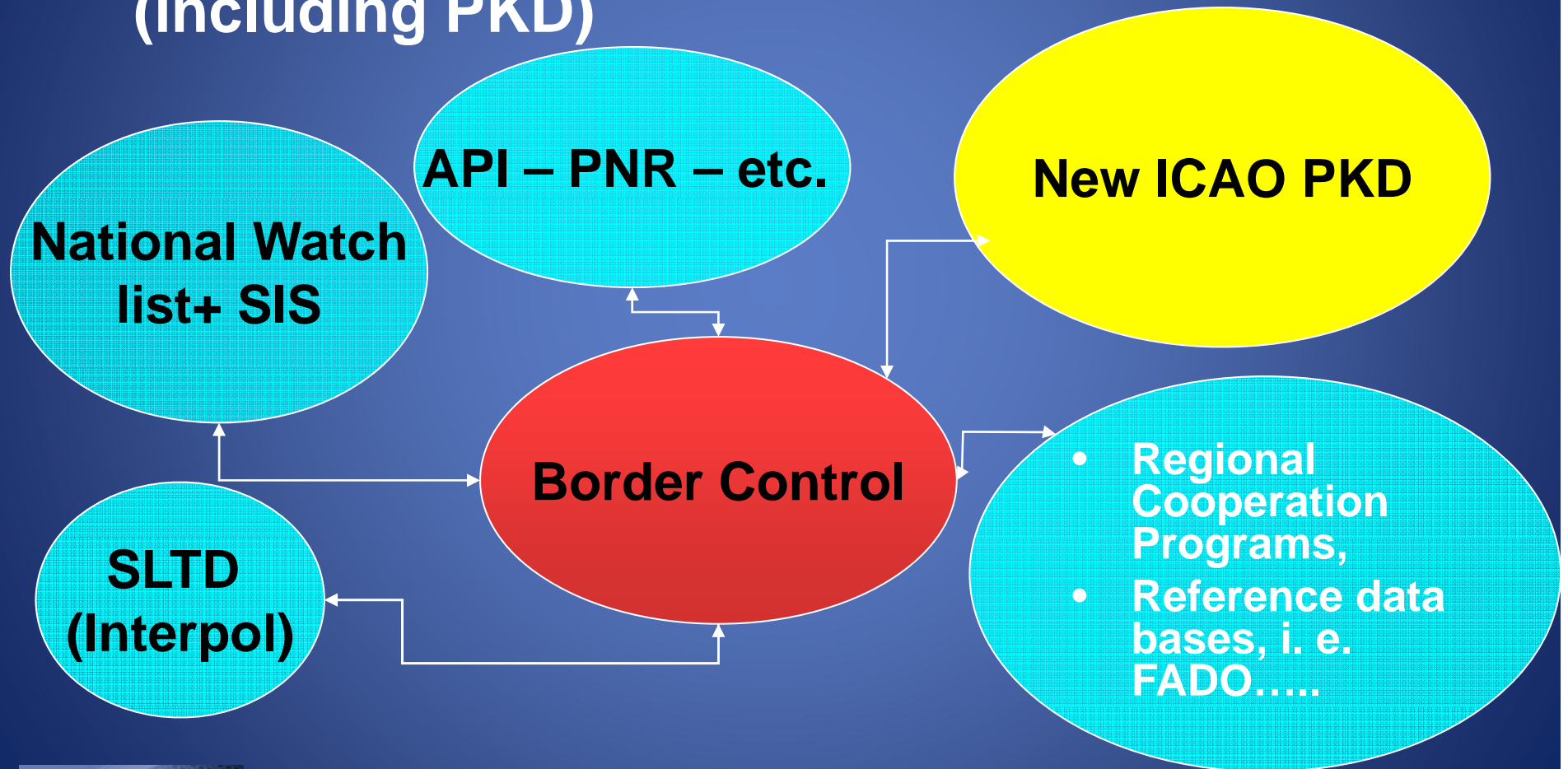
Reasons to join

- If not done at the same time, participation at the ICAO-PKD should be the immediate next goal of a country after introducing e-passports.
- The need to exchange certificates is the logical step forward from the well known specimen exchange (you must know what you're looking for, when inspecting a travel document).
- A reliable certificate exchange is a requirement for the use of automated border controls.

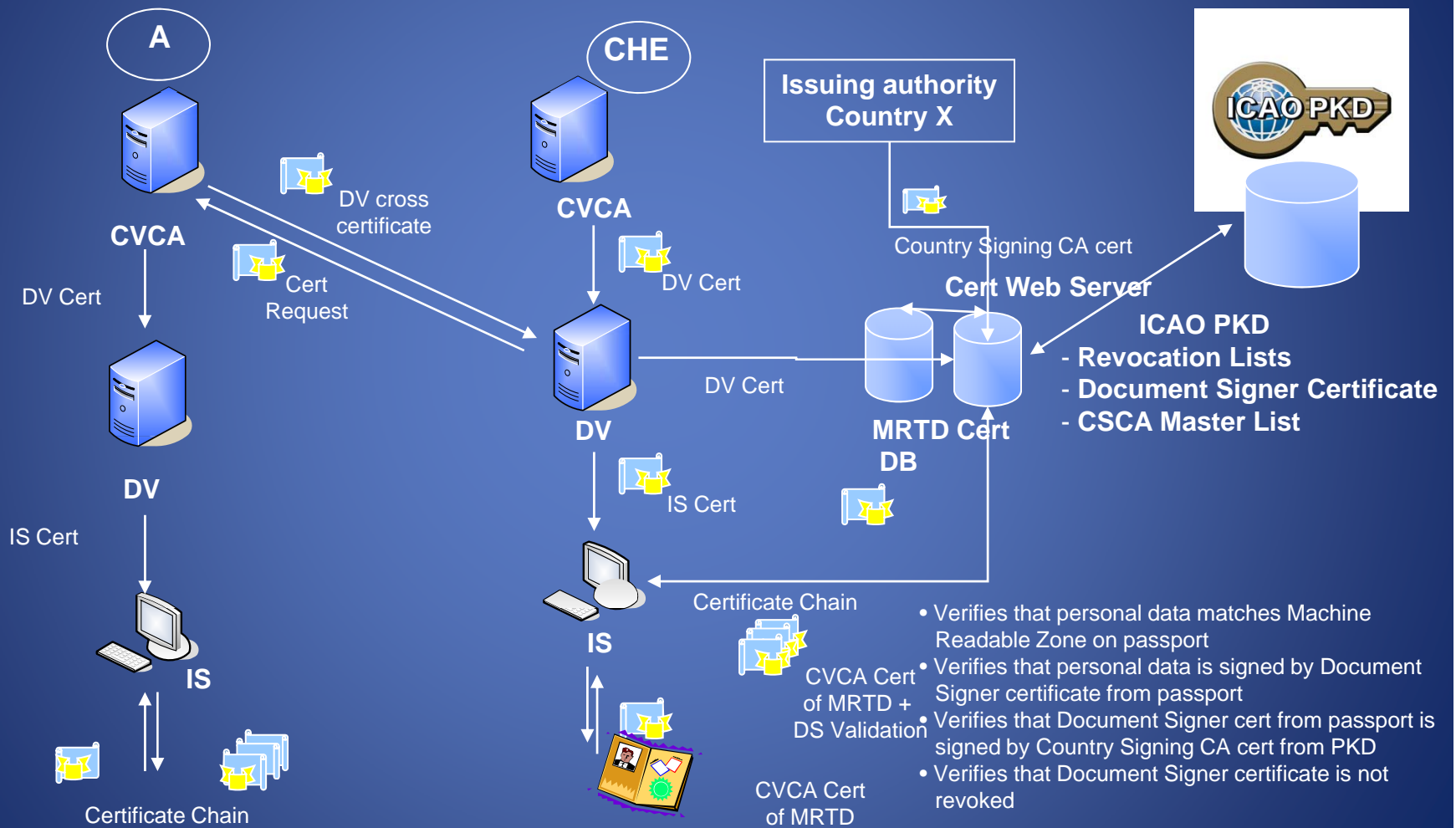


Border Control

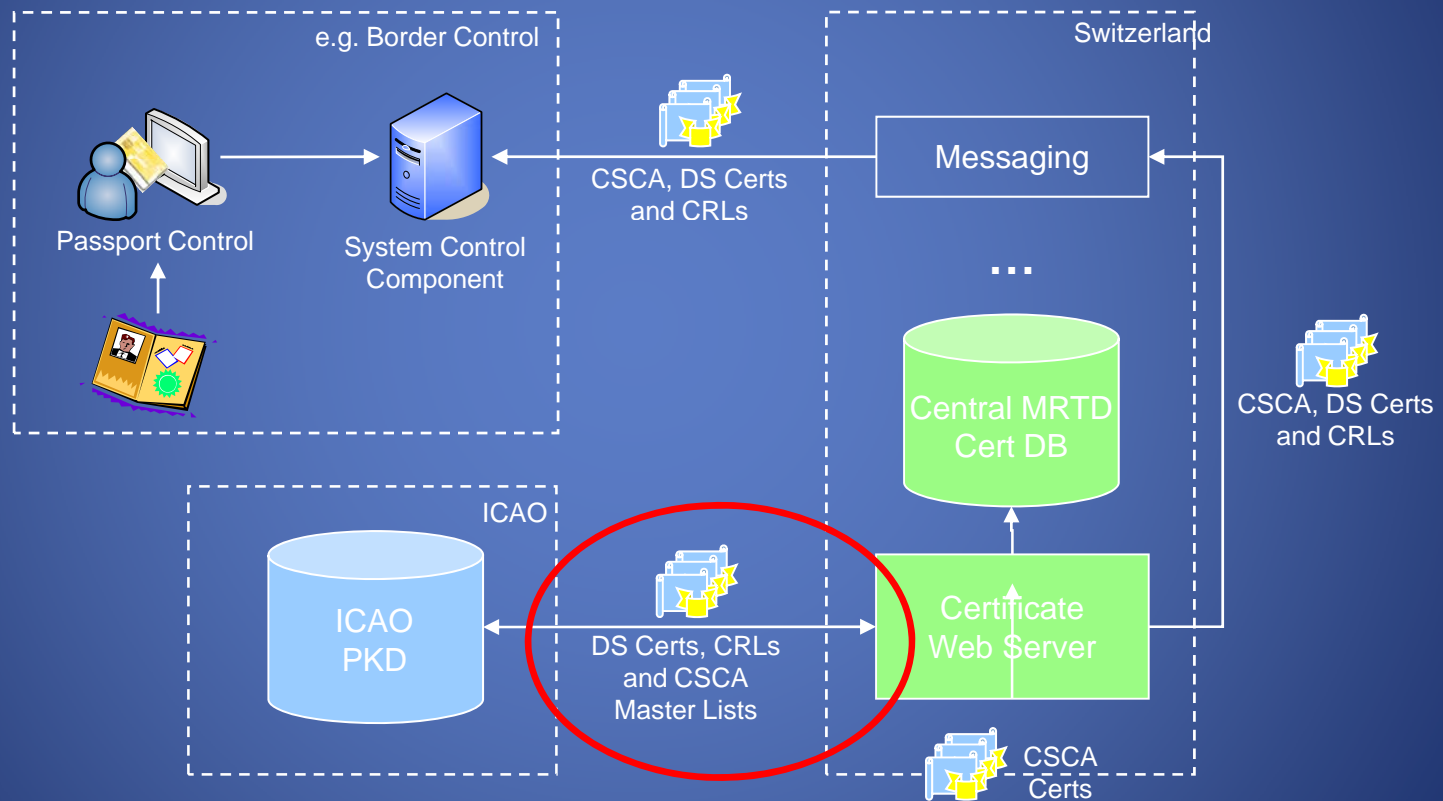
- Information is vital
(including PKD)



PKI/PKD Set-Up Switzerland



PKD-Set up details



Processes to be defined

- Download of foreign DS
- Download foreign CRLs
- Download foreign CSCA Master List
- Upload of national DS, CRLs and CSCA Master Lists
- Creation of Master Lists



Download foreign DS



Certificate Web Server



ICAO PKD



Central MRTD
Cert DB

1. Connection with LDAP over SSL

2. Connection established

3. LDAP search request for all DS Certs for 1 country

4. Return all DS Certs for this country

5. Get all existing DS Certs for this country

6. Return all existing DS Certs for this country

7. Check for new and removed DS Certs

8. If new DS Certs, get issuing CSCA Certs and corresponding CRLs

9. Return CSCA Certs and CRLs

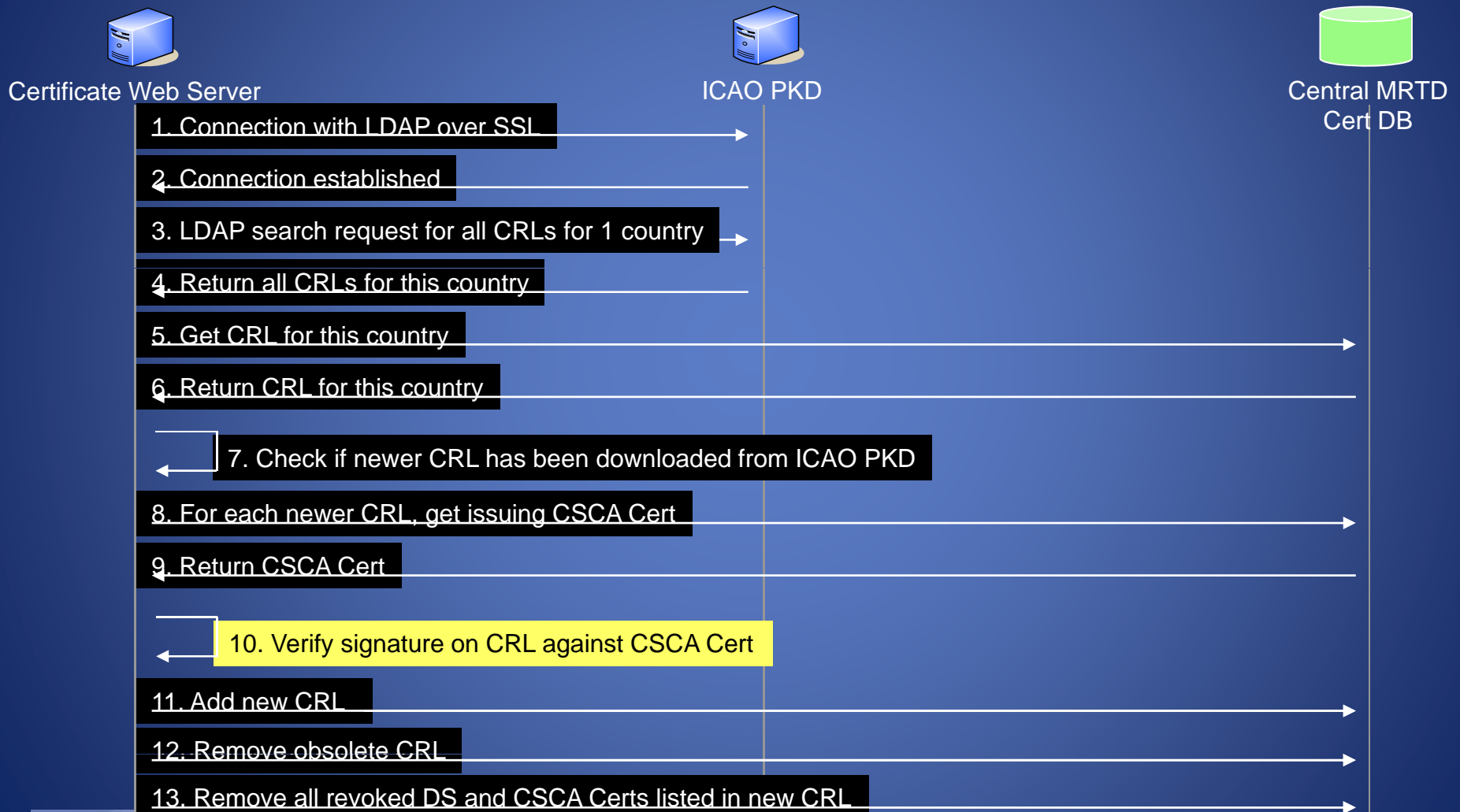
10. Verify DS Certs against CSCA Certs, validate DS Cert and CSCA Cert against CRL

11. Add new DS Certs

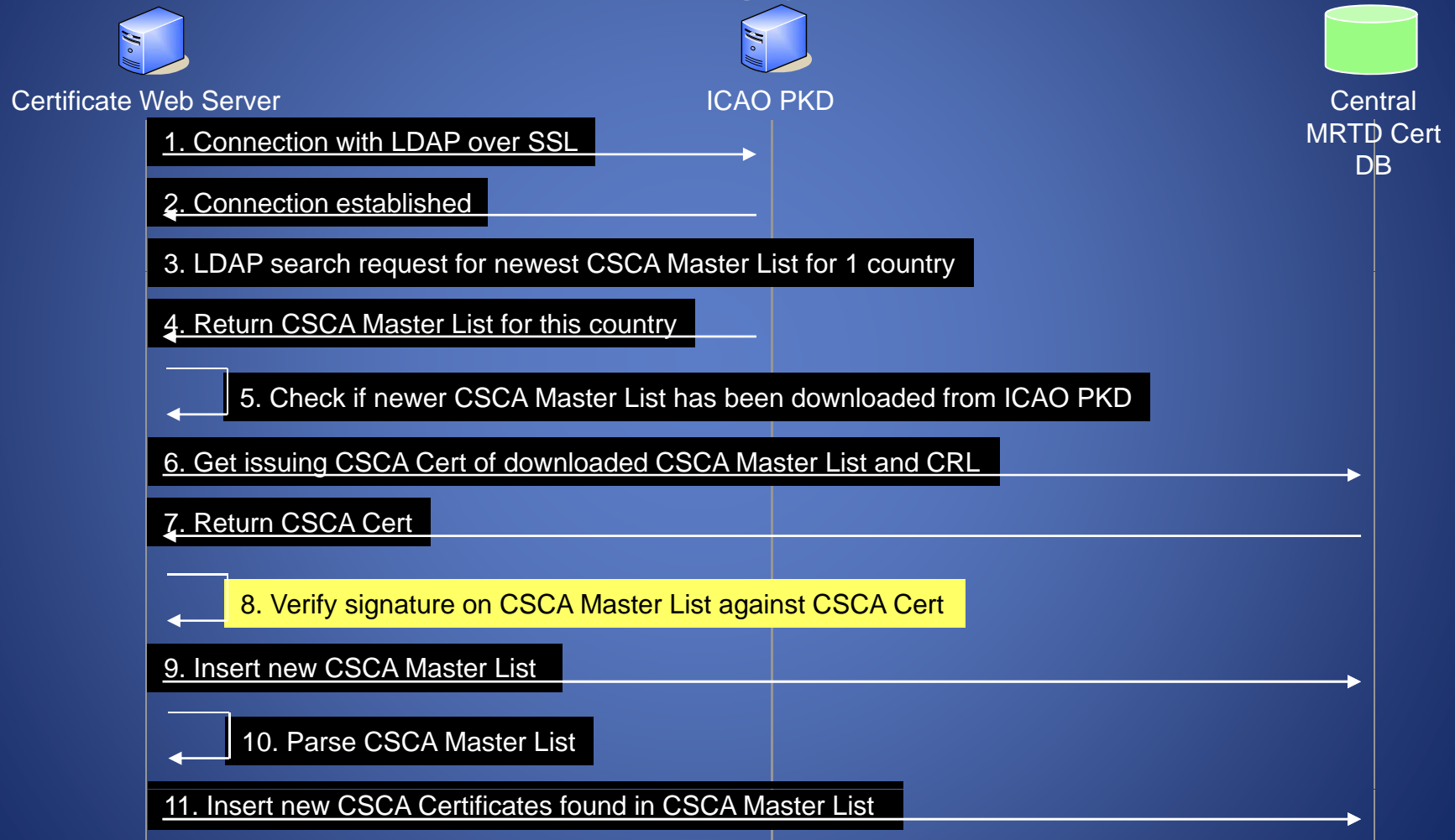
12. Remove obsolete DS Certs



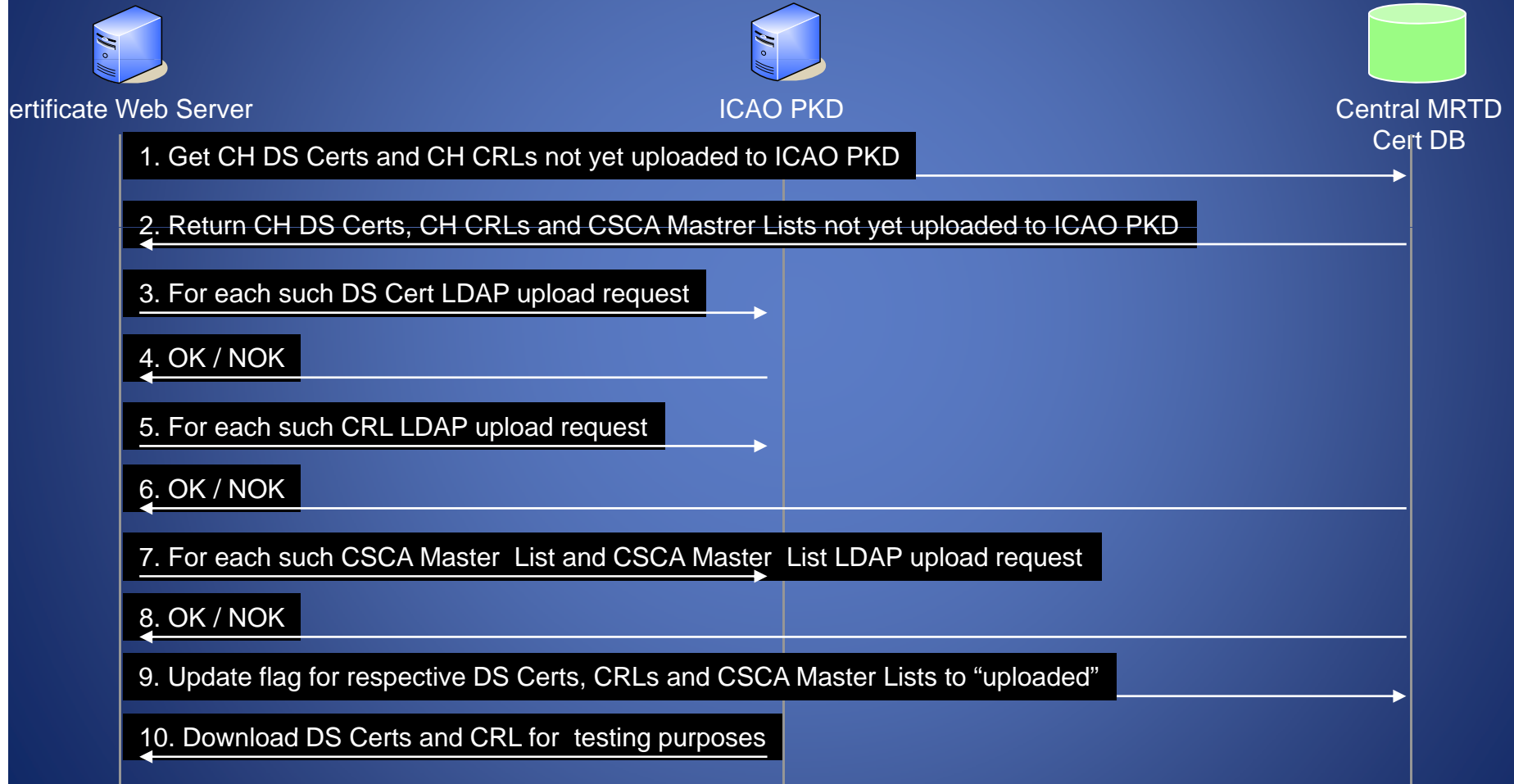
Download foreign CRLs



Download foreign CSCA Master List



Upload of national DS, CRLs and CSCA Master Lists



Creation of Master Lists



2 Users



Certificate Web Server

1. Flag CSCA Certs to be added to CH CSCA Master List and Master List Light (persistent in DB)

2. Export CH CSCA Master List ZIP File

3. Select all CSCA Certs flagged for CSCA Master List from DB

4. Assemble ZIP File holding all such CSCA Certs

5. Sign ZIP with HSM as CMS Signed-Data object

6. Return ZIP File holding all CSCA Certs to be included in CH CSCA Master List



Summary

The Swiss Central MRTD Cert DB serves as repository for all certificates available.

Procedures must be well defined and secured, especially import of CSCA Certificates.

Most down- and upload procedures can be highly automated, apart from CSCA Certificate import.



What do you have to do?

- Find out who is responsible
- Check legislation and budget
- Different organizations in different states (try to make it as simple as possible)
- e-Passport/PKD was mostly considered an issuers tasks, that is not true
- Contact ICAO or any PKD Board Member or PKD Participant if you have questions



Lessons learned

- Operational responsibilities must be defined early
- It's helpful if one authority is responsible for passports, PKI, PKD, i. e. the issuer, and takes the lead
- It will take time, please some spare time
- There will be surprises – sorry no guarantee



Who's next?



Questions?

Federal Office of Police

Chief Division Identity Documents and
Special Tasks

Roman Vanek

schweizerpass@fedpol.admin.ch

Further information:

www.schweizerpass.ch

