



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement  
Bundesamt für Polizei fedpol

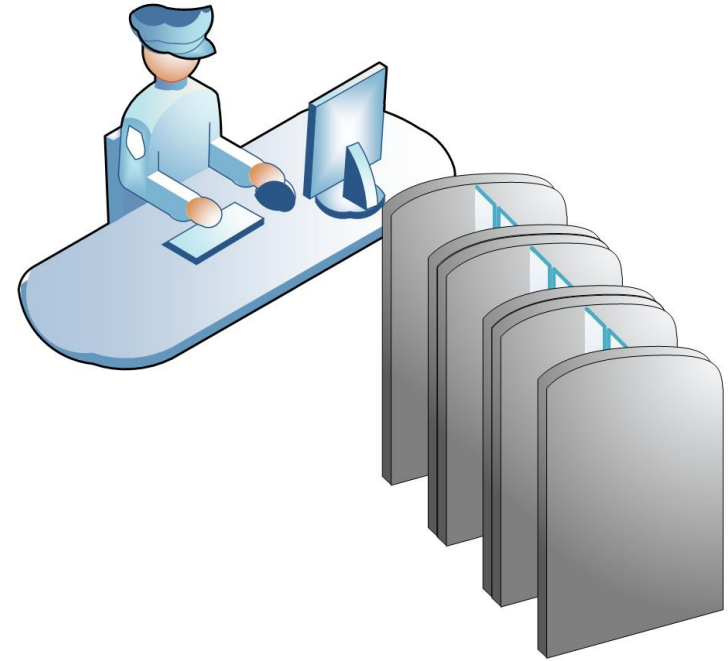
# eMRTD

## Explanation of the Swiss PKI

Titus Abele & Benjamin Mouchet

## In the field

- Is it genuine?
- Has it been altered?
- Does it belong to the holder?

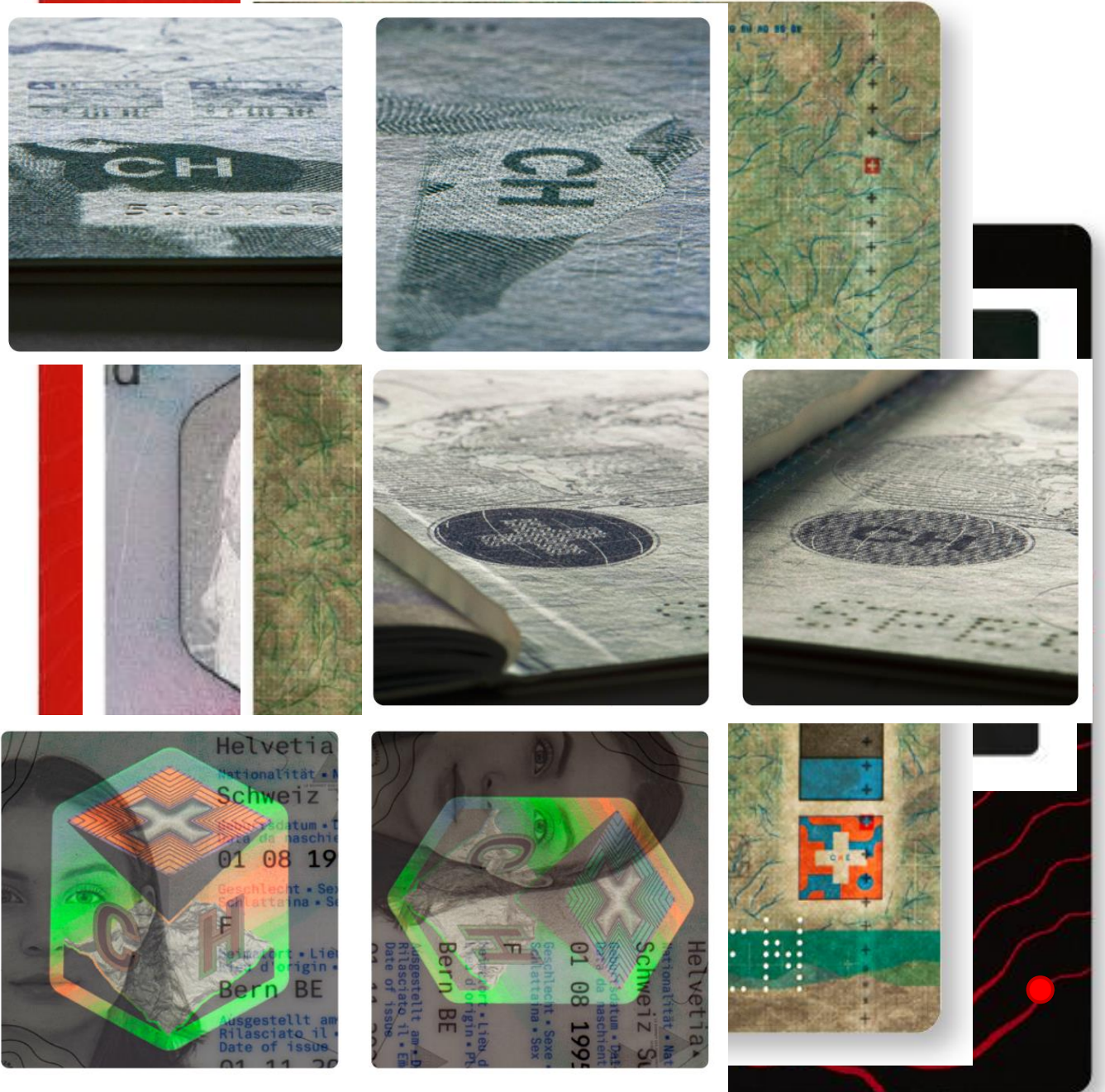


*With electronic travel documents (eMRTDs), we answer the same questions by adding cryptography to the visual inspection.*

# eMRTD – the Booklet

## Physical optical elements

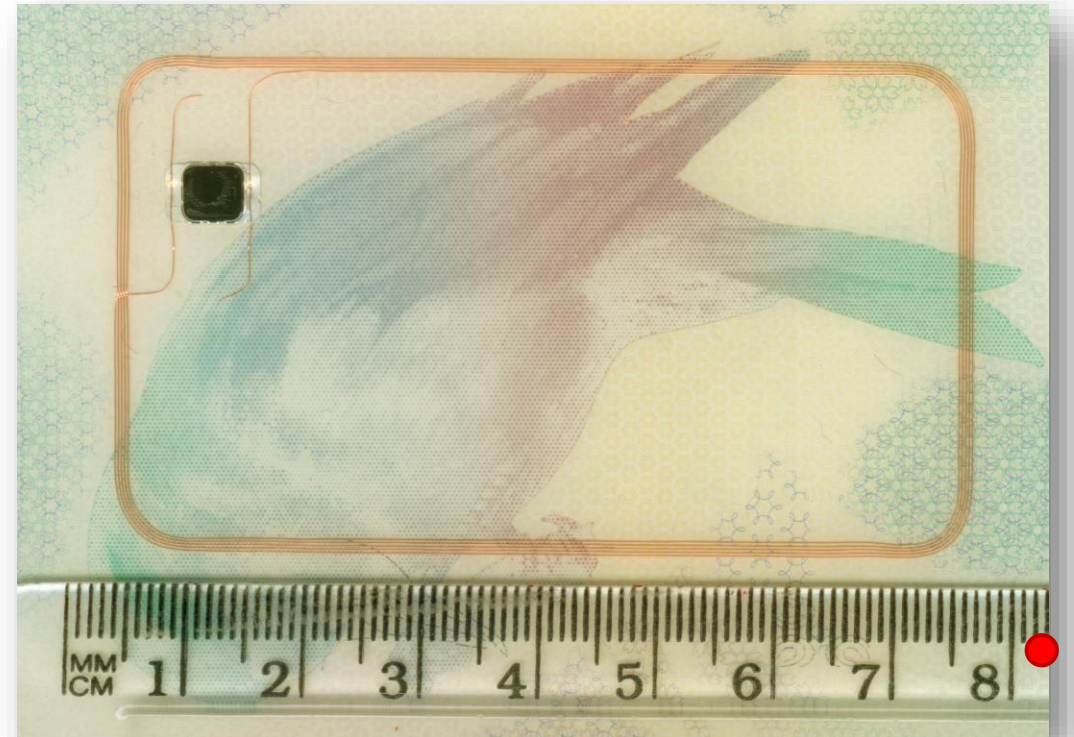
- UV features
- Embossing
- OVI®
- Window Lock
- Watermark
- Etc.



# eMRTD – the Chip

Digital mathematical elements - Data Groups such as

- **DG1** – Personal data (MRZ information)
- **DG2** – Facial image
- **DG3** – Fingerprints
- **DG14** – Chip authentication info
- ...
- **SOD** – Security Object

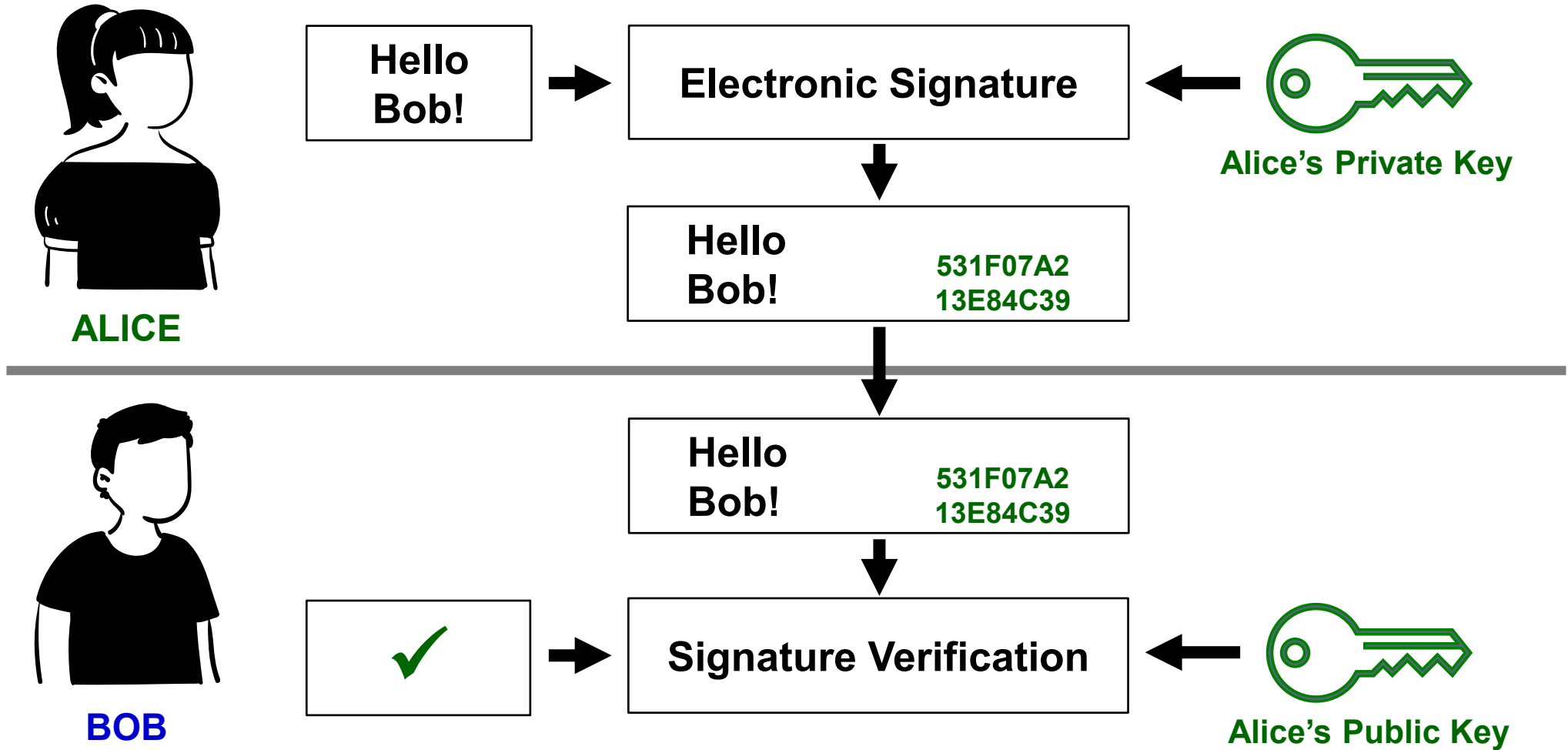


# Why is a signature not enough

“A valid signature proves that the data hasn’t been changed and identifies the signing key - but it does not prove that the signer is trusted or authorized.”

1. The PKI provides proof
2. The chip stores proof
3. The controller checks proof

# A quick note on cryptography and signatures





Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement  
**Bundesamt für Polizei fedpol**





# The Swiss Chocolate Analogy: why public keys are meant to be shared

| Swiss Chocolate        | eMRTD PKI              | Who knows it      |
|------------------------|------------------------|-------------------|
| The secret recipe      | Private key            | Only Switzerland  |
| The chocolate box      | Signed passport data   | Travels the world |
| The unmistakable taste | Public key certificate | <b>Everyone</b>   |

***Only Switzerland can make it. Anyone can recognise it.***

- One taste tells you it's genuine and hasn't been altered.

***Knowing the taste doesn't reveal the recipe, but if nobody knows the taste, nobody can tell real from fake.***

- Sharing your certificates via the ICAO PKD costs you little and protects your citizens' passports.

# The Swiss Chocolate Analogy, Part 2: The *premium* box (EAC)

**The setup:** Every Swiss chocolate box has a sealed inner compartment holding the finest truffles (*fingerprints*). Tasting the outside is open to all. Opening the inner compartment requires a pass issued by Switzerland.

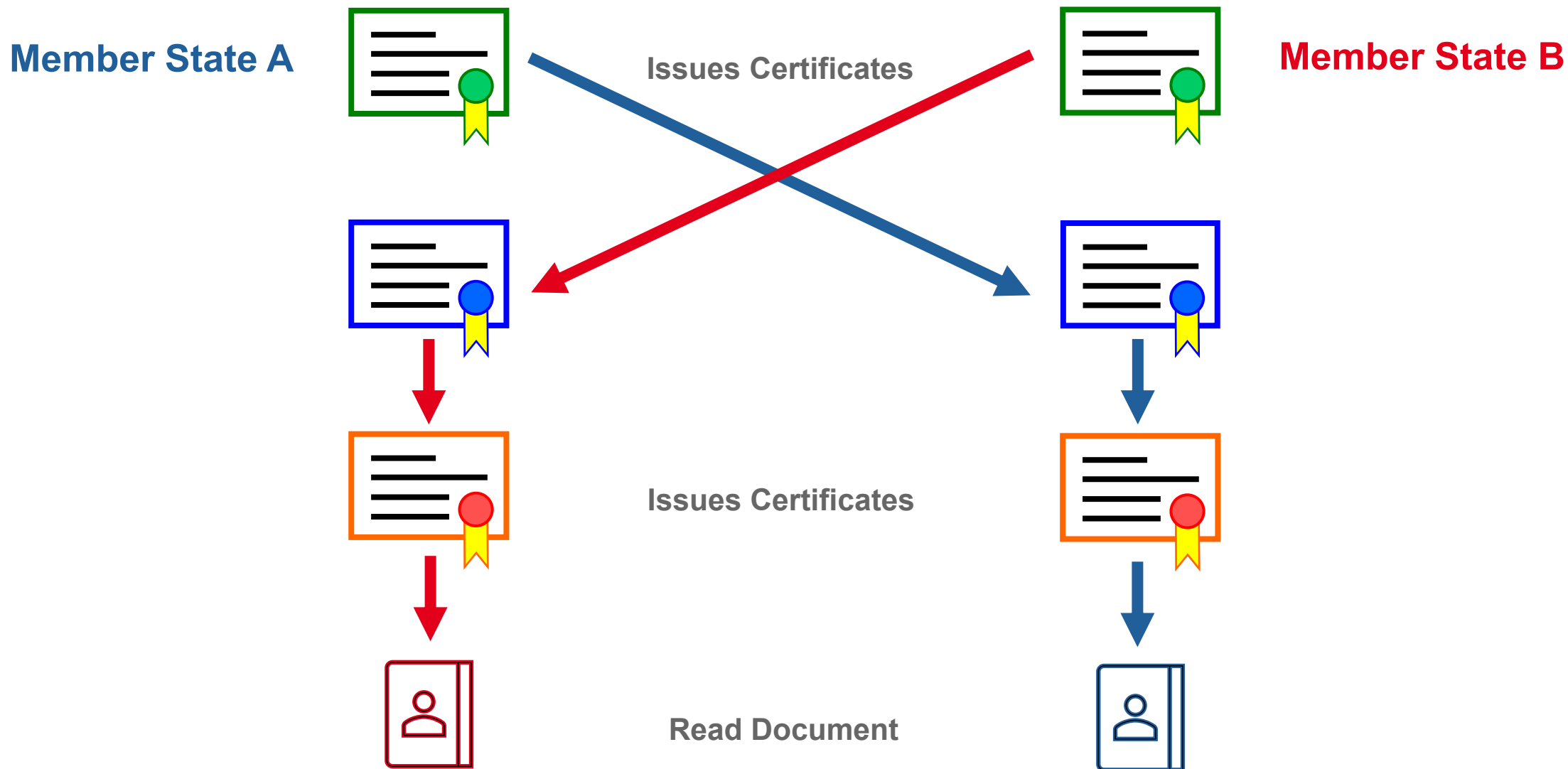
| Swiss Chocolate                                                                     | EAC PKI                                       |
|-------------------------------------------------------------------------------------|-----------------------------------------------|
| The Swiss Chocolate Authority, which decides who may open Swiss sealed compartments | Country <b>Verifying</b> CA (issuing country) |
| A foreign import agency accredited by the Authority                                 | Document Verifier (reading country)           |
| Short-lived tasting passes the agency hands to its shops                            | Inspection System certificates                |
| The box checks the pass chain back to the Authority                                 | Terminal Authentication                       |
| The box proves it's a real box, not a copied wrapper around fake chocolate          | Chip Authentication                           |

## The Swiss Chocolate Analogy, Part 2: The *premium* box (EAC)

**Authenticity is public. Access is privileged.**

- **Passive Authentication:** share the taste with the world (ICAO PKD).
- **Extended Access Control:** passes go only to trusted partners, exchanged bilaterally (SPOC), and they expire quickly.

# Extended Access Control (EAC) – PKI

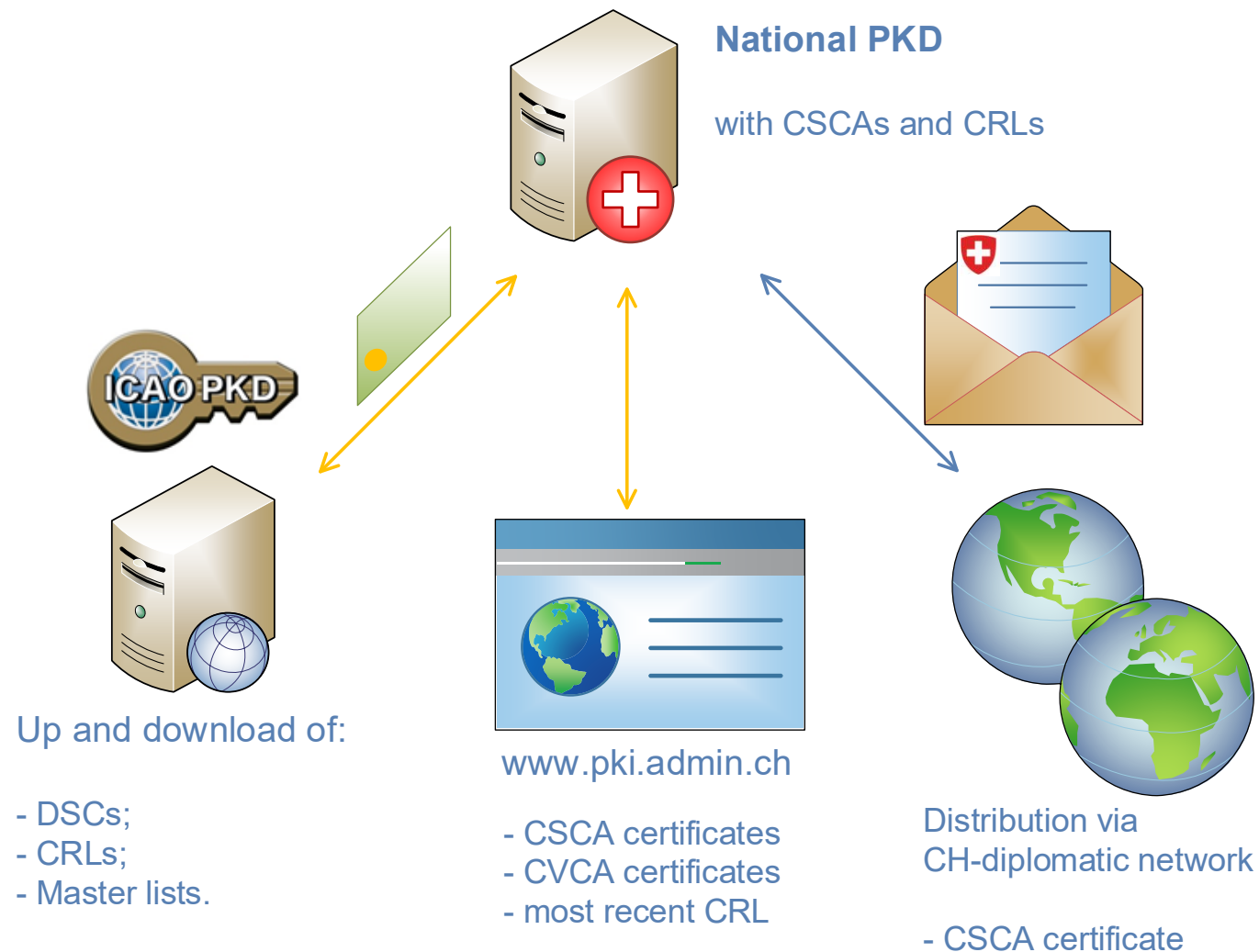




# Conclusion

- **eMRTD PKI (Passive Authentication):** public keys prove a passport is genuine and unaltered. Publishing them reveals nothing secret and is the only way others can verify your documents.  
→ *Share openly via the ICAO PKD.*
- **EAC PKI:** certificates decide who may read sensitive biometrics.  
→ *Share selectively, bilaterally, with short validity.*

# Where can I find these certificates ? PKD



# Follow us



@fedpolCH



Bundespolizei fedpol



Swiss Federal Police fedpol



# Sources

|                |                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Document       | Machine Readable Travel Documents                                                                                                      |
| Version / Date | Eighth Edition / 2021                                                                                                                  |
| Issuer         | International Civil Aviation Organization (ICAO)                                                                                       |
| Identification | Doc 9303                                                                                                                               |
| Document       | Common Certificate Policy for the Extended Access Control Infrastructure for Travel and Residence Documents issued by EU Member States |
| Version/Date   | 2.2 / 31. July 2018                                                                                                                    |
| Issuer         | Bundesamt für Sicherheit in der Informationstechnik (BSI)                                                                              |
| Identification | BSI TR-03139                                                                                                                           |

# Extra Slide – Asymmetric Cryptography

