

DTC Validation

R Rajeshkumar

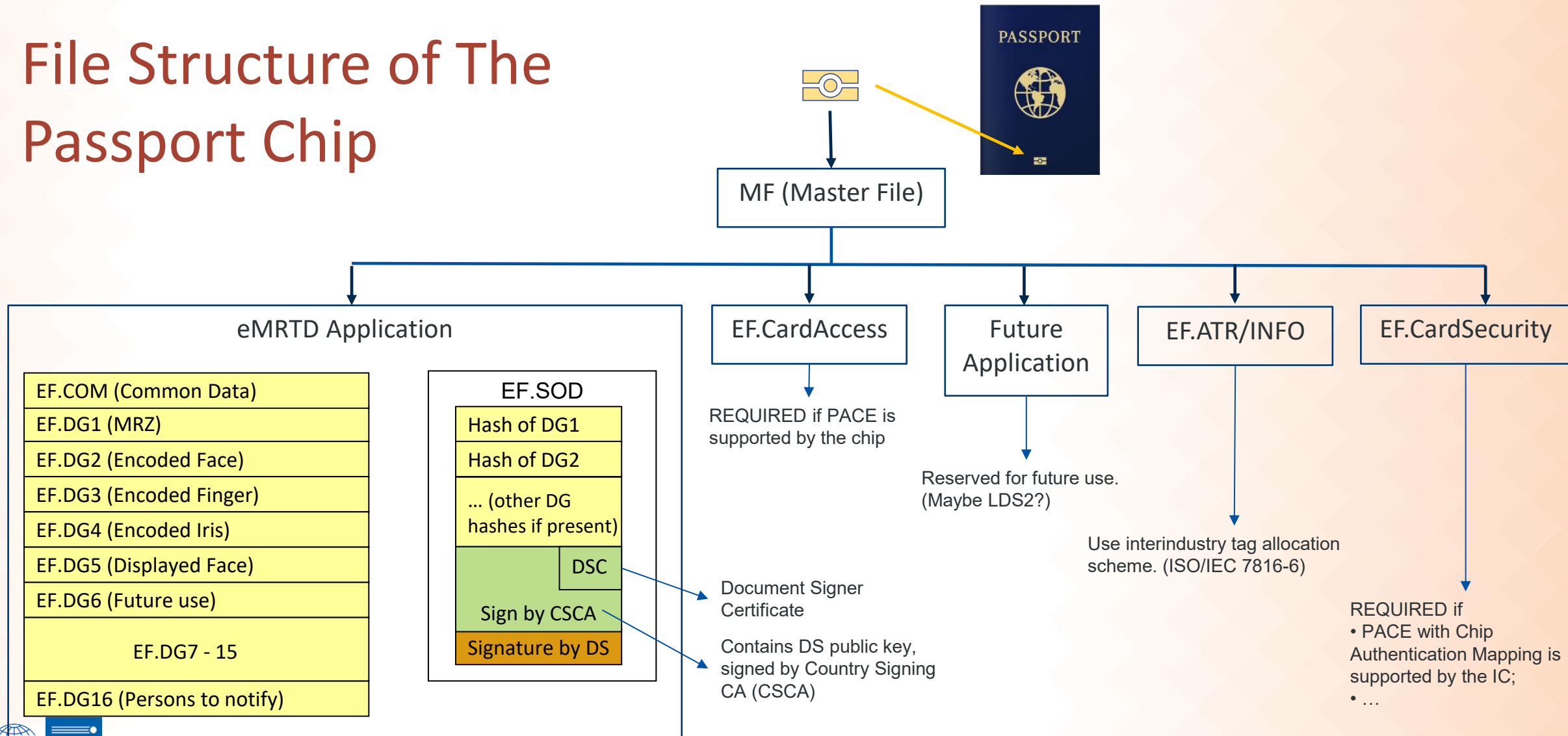
Convener – ISO/IEC JTC1 SC17/WG3



Validation of a DTC
uses the same
mechanism as
validating an eMRTD

1. ePassport Validation

File Structure of The Passport Chip

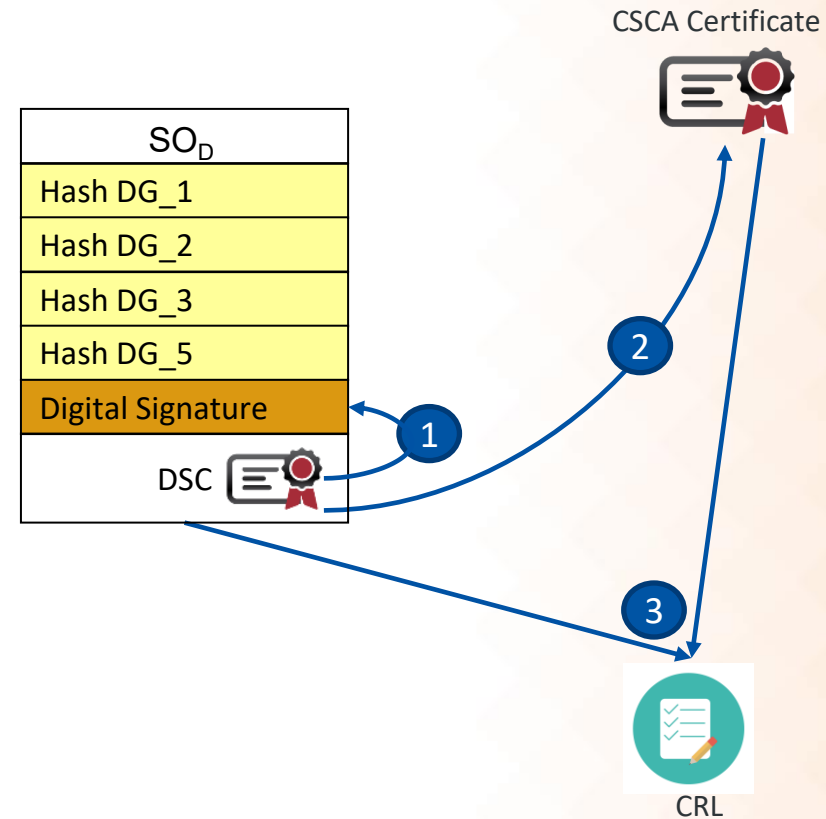


Understanding E-Passport validation

- Trust is established by proper verification of the e-Passport
 - SOD is valid
 - LDS is valid
 - eMRTD is valid
 - Traveller is valid

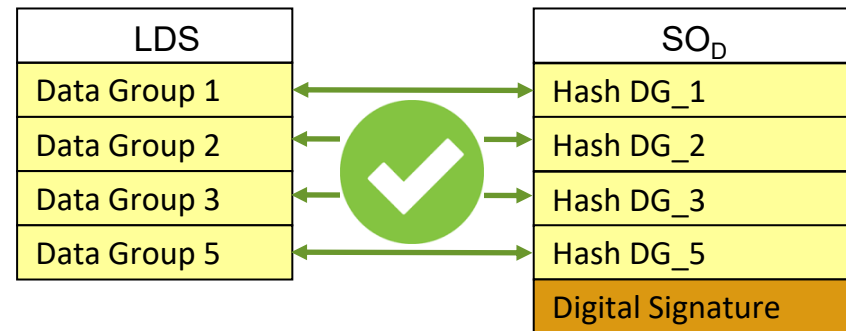
SOD is Valid

1. Verify SOD against DSC
2. Verify DSC against CSCA
3. Verify DSC & CSCA not in CRL

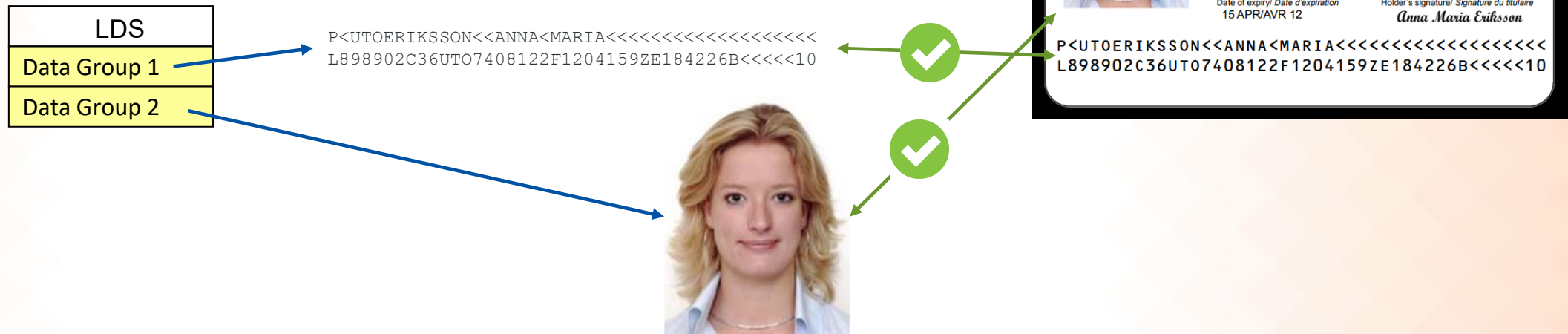


LDS is Valid

- Check that DG hash values matches the hash values stored in SOD



- Compare DG1 with MRZ
- Compare DG2 with printed photo

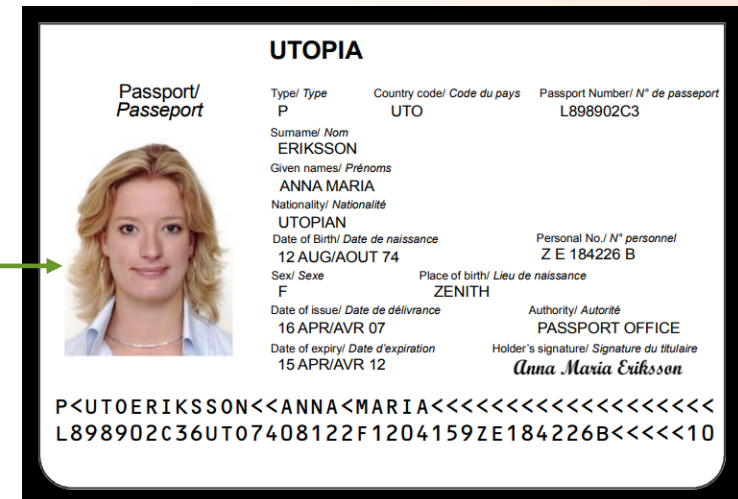


Traveller is Valid

- Compare photo to holder of passport



Passport holder at the border



Understanding E-Passport validation

- Trust is established by proper verification of the e-Passport

- Verify SOD against DSC
- Verify DSC against CSCA
- Verify DSC not in CRL
- Check that DG hash values matches the hash values stored in SOD
- Compare DG1 with MRZ
- Compare DG2 with printed photo
- Compare photo to holder of passport



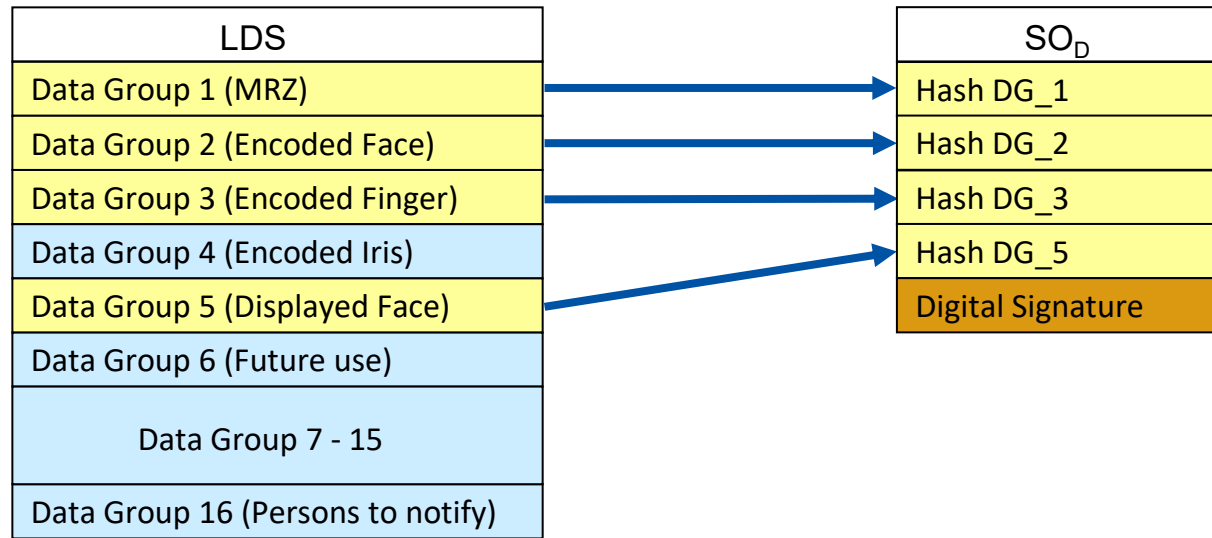
SOD is valid

LDS is valid

eMRTD is valid

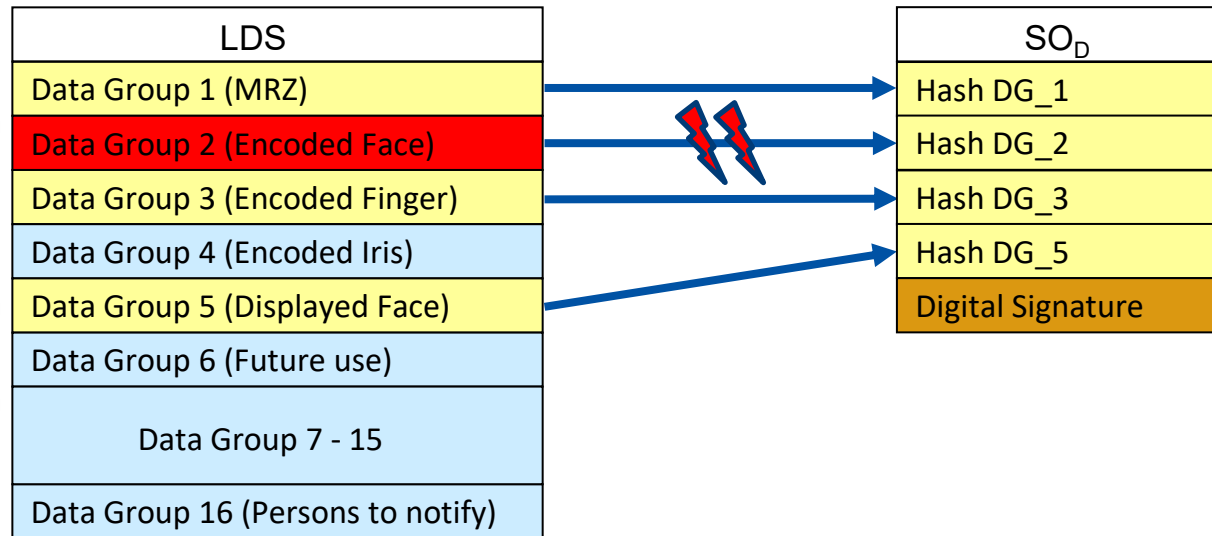
Traveller is valid

Passive Authentication



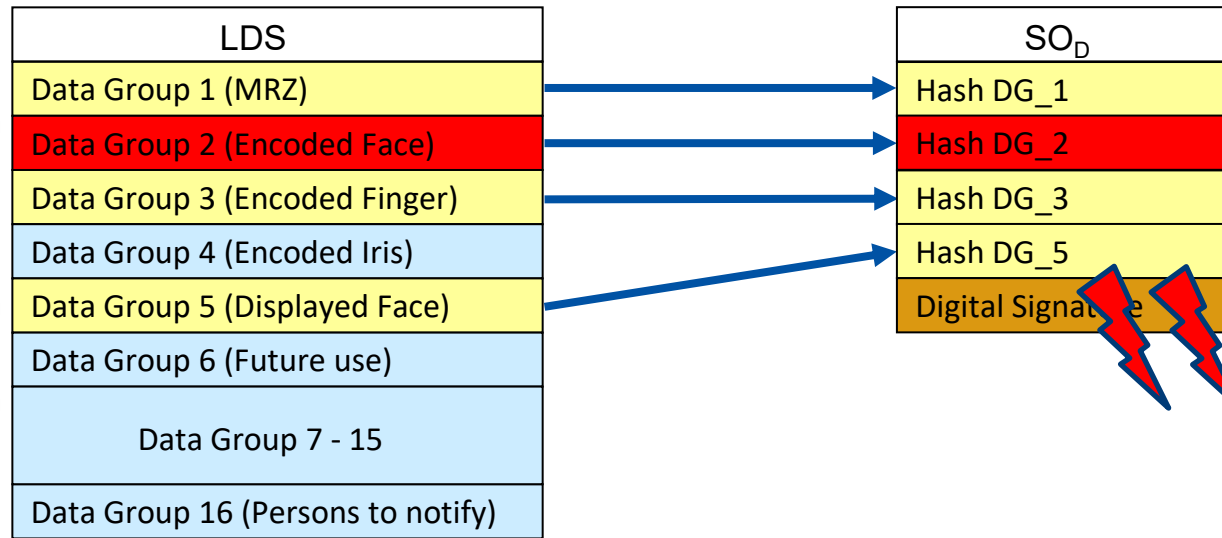
- Hash of each data group is stored in SOD
- Hash of the hashes is then signed and also stored in the SOD

Passive Authentication



- DG2 content changed
- Hash in SOD not changed
- Hash Comparison will fail

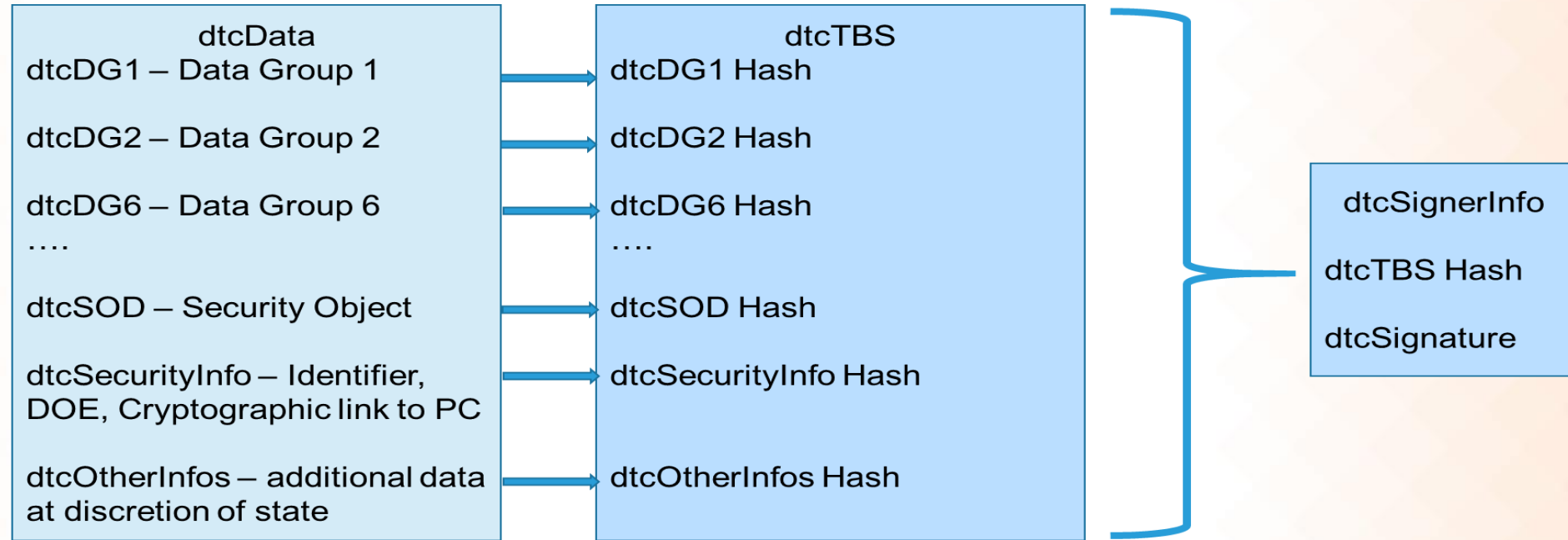
Passive Authentication



- DG2 content changed
- Hash in SOD also changed
- Hash Comparison will succeed but signature verification will fail

2. DTC Validation

DTC Validation



dtcData contains the LDS and SOD. The process of verifying this data (Passive Authentication) is identical to eMRTDs

For Type 2 and 3, additional step of comparing the Hash stored in dtcTBS to the hashed values of dtcData

Then validate the Signature on the whole structure

Validation of DTC

Validating DTC contents is the same as validating the eMRTD

For trusting the Physical Component or the additional information in the DTC, additional validation of the envelope is necessary

Validation of eMRTDs and DTCs

- **Availability of CSCAs** — Country is still root of trust. But, eMRTD may have been issued by an older CSCA and DTC may have been signed by a newer CSCA
- **Availability of CRLs** — A single CRL will cover all Signers
- **Visualization of Validation Result** — Too much information will confuse the verifier. Becomes even more relevant for DTC compare to eMRTD
- **Handling of defective encodings** — The contents of the eMRTD are copied over, so any encoding defects also get copied over. **Defect handling will need to be in place**
- **Checking SLTD** — Currently, check is for eMRTD number only. For DTC, an additional check for DTC Identifier. So two step check

Some basic things to remember in validating eMRTDs

- Refer to my presentation in TRIP 2023 – 9 myths of ePassport Validation
 1. CSCAs are not secret. Please share them with others
 2. Ensure control over possession and usage of your CSCA private key and Signer private key
 3. Passive Authentication and Clone detection are necessary after reading the chip to ensure the authenticity and integrity of the data
 4. Validating an eMRTD is never a binary result, as the validation may fail at different stages. Plan workflow to manage this.
 5. Passports with defects will fail validation – false negatives. This does not render the document invalid. Implement defect management and secondary document checks
 6. Defect Lists cannot differentiate between a defective and a fraudulent document – implement defect management or other means to validate the documents

If your border control system has never detected a fraudulent document based on chip data, there is something wrong in the implementation

No News is not always Good News

Thank You

R.Rajeshkumar@auctorizium.com

RRaj88@gmail.com

www.linkedin.com/in/rraj88

