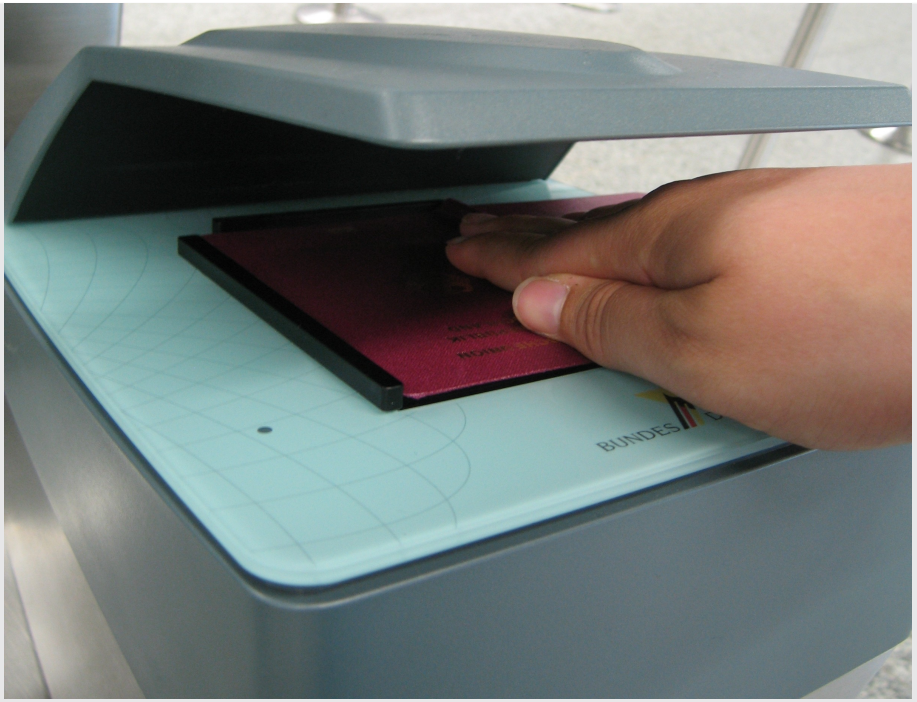
Federal Office
for Information Security

ePassport Based Identity Check



Benjamin Marzahn
Federal Office for Information Security (BSI)
Germany

BSI – activities regarding eMRTDs

- IT security
  - Specification and standardization of security mechanisms (ICAO, ISO, EU, national level)
  - National root CAs (CSCA, CVCA, N-PKD)
- Biometrics
  - Evaluation of biometric technologies
  - Biometric framework BioMiddle
- Certification and approval
- Pilot projects
  - ePassports at the German border (e.g. EasyPASS)

Main steps
ePassport & EasyPASS

- Nov. 2005: Issuance of the 1st generation ePassport (face)
- Nov. 2007: Issuance of the 2nd generation ePassport (face and finger)
- Nov. 2007 – June 2009: Pilot project “Reading and Checking ePassports”
- Aug. 2009: Start of the pilot project **EasyPASS**

Main steps
New German ID Card & EAC IS

- Nov. 2010: Issuance of the new German ID card (face and optional finger)
- Since May 2011: Pilot Extended Access Control Inspection System (EAC IS) for
  - Read access to Extended Access Control (EAC) protected data in ePassports
  - Support for the new German ID Card in EasyPASS and during regular border control
  - Complete support of Masterlists and Defectlists
- Approx. Q3/2012: Regular operation including exchange of DV-certificates within EU

EasyPASS – project overview

- Pilot project of BSI and the German Federal Police
- Semi-automated eGate scenario
  - Monitoring (and if necessary interaction) by border police officer
- 4 Self-service eGates, 1 monitoring station
- Open for citizens of EU/EEA/CH (18+ years old)
- Located at Frankfurt Airport
- Timetable
  - Start of operation was in August 2009
  - Pilot phase until March 2010
  - Since April 2010 regular operation

EasyPASS border control process using facial recognition

Check of entitlement

Optical checks
Electronic checks
Background checks

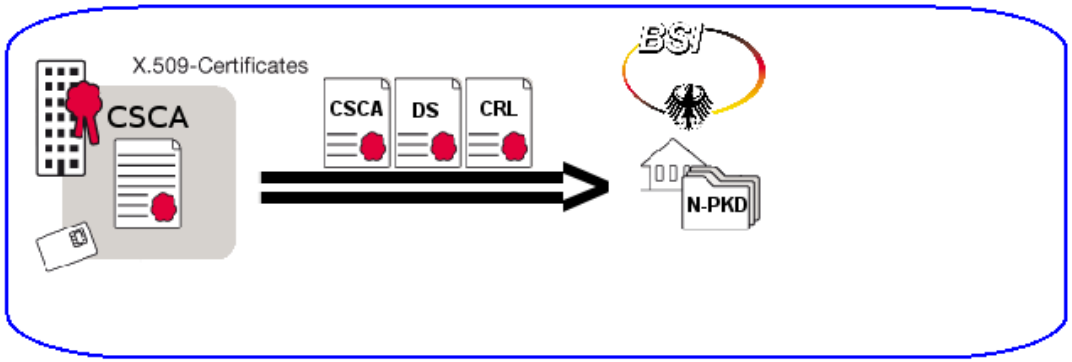
Capture and Comparison
Chip image ←→ Live image

Border crossing

EU
EWR
CH

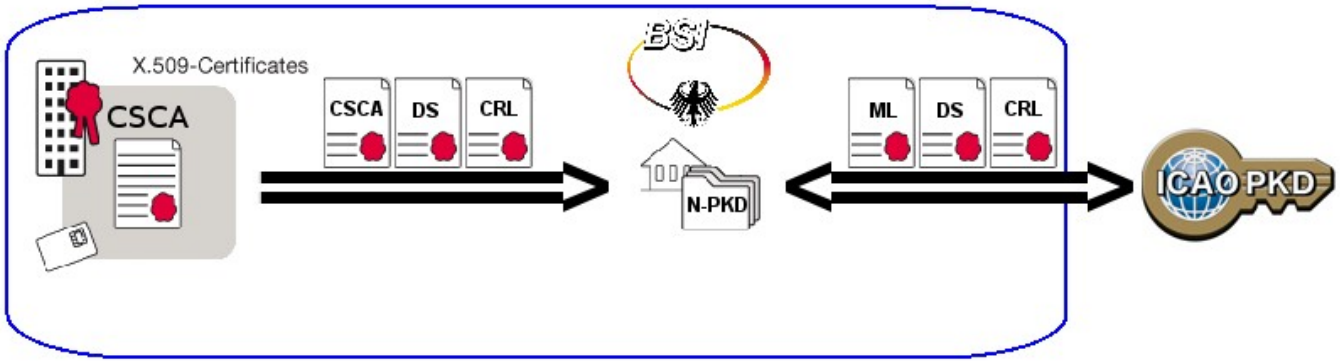
18+

eMRTD PKI landscape



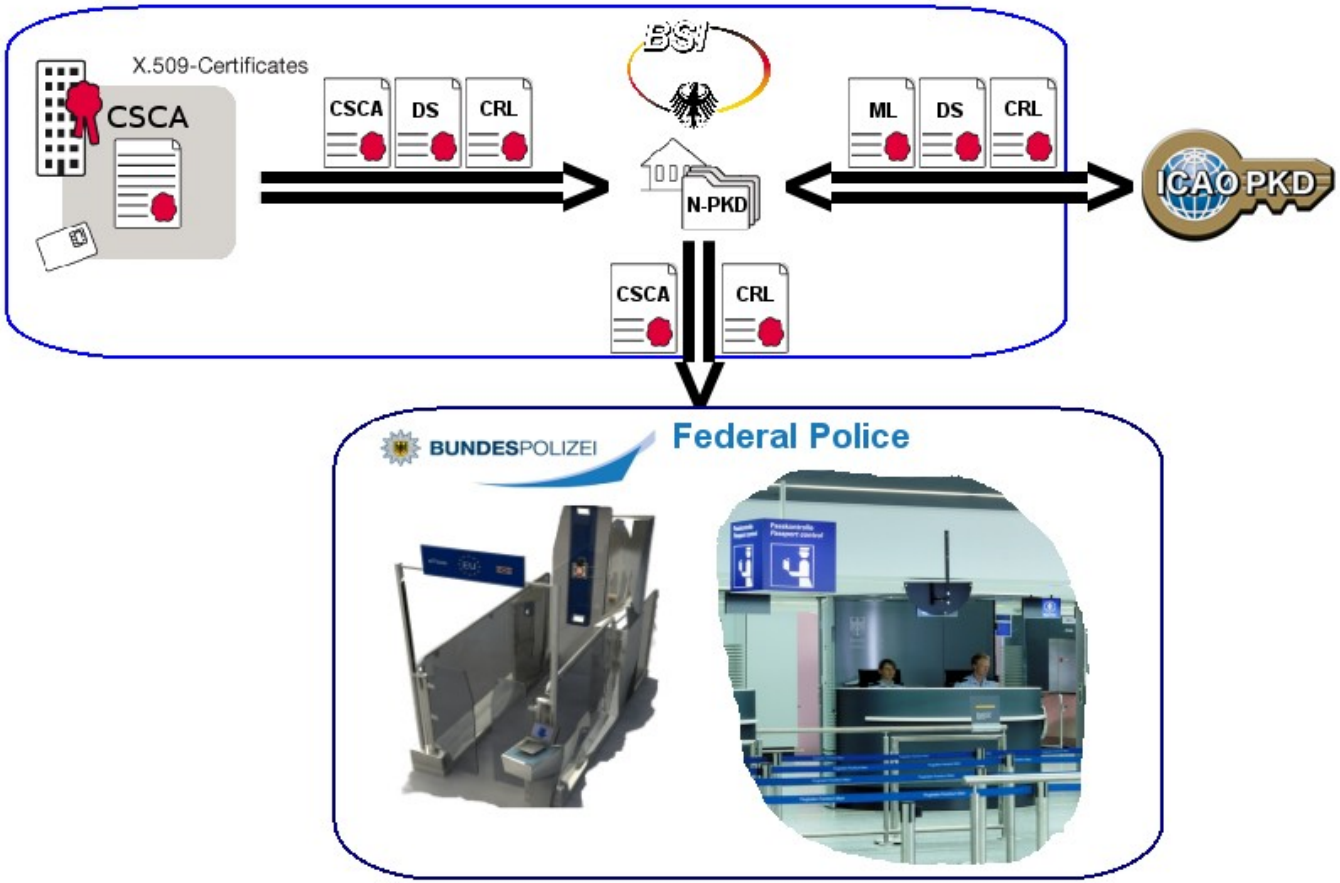
- CSCA generate
  - CSCA certificates
  - Document Signer certificates (DS)
  - Cert. Revocation List (CRL)
- N-PKD
  - Central storage of trusted CSCA certificates
  - Generate Masterlists (ML)

eMRTD PKI landscape



- ICAO-PKD international exchange of
  - CSCA certificates via Masterlist (ML)
  - Document Signer certificates(DS)
  - Cert. Revocation List (CRL)

eMRTD PKI landscape

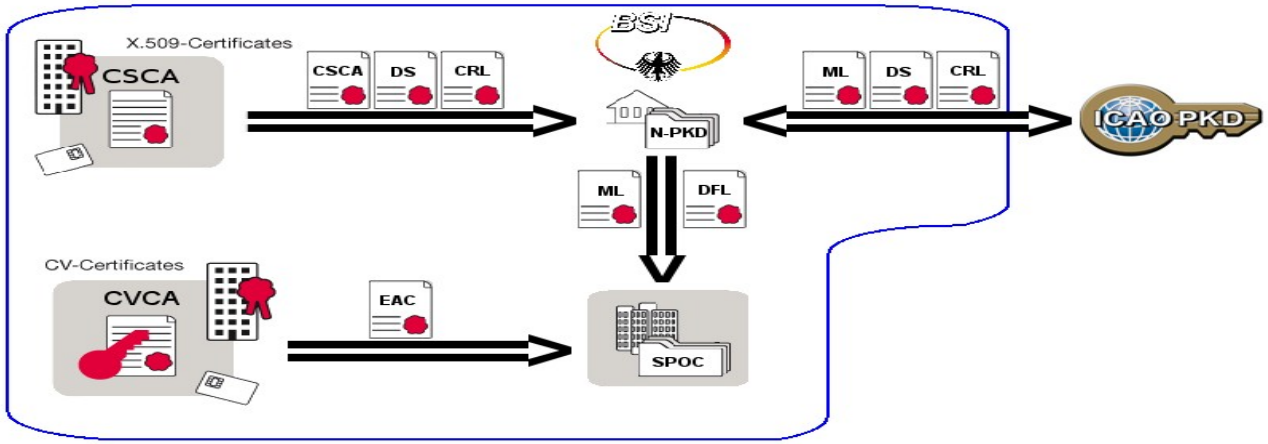


- Federal Police receives from N-PKD for automated and manual border control
  - CSCA certificates
  - Cert. Revocation List (CRL)

eMRTD PKI landscape

- Specifications:
  - PKD Test Bench Procedures – ICAO PKD (Netrust Pte Ltd)
  - PKD Interface Specifications – ICAO PKD Tender (Netrust Pte Ltd)
  - TR CSCA countersigning and Master List issuance (ICAO)
  - Doc 9303 (ICAO)
- Additional Information, Technical Reports and Doc9303 : http://www2.icao.int/en/MRTD/Downloads/Forms/AllItems.aspx

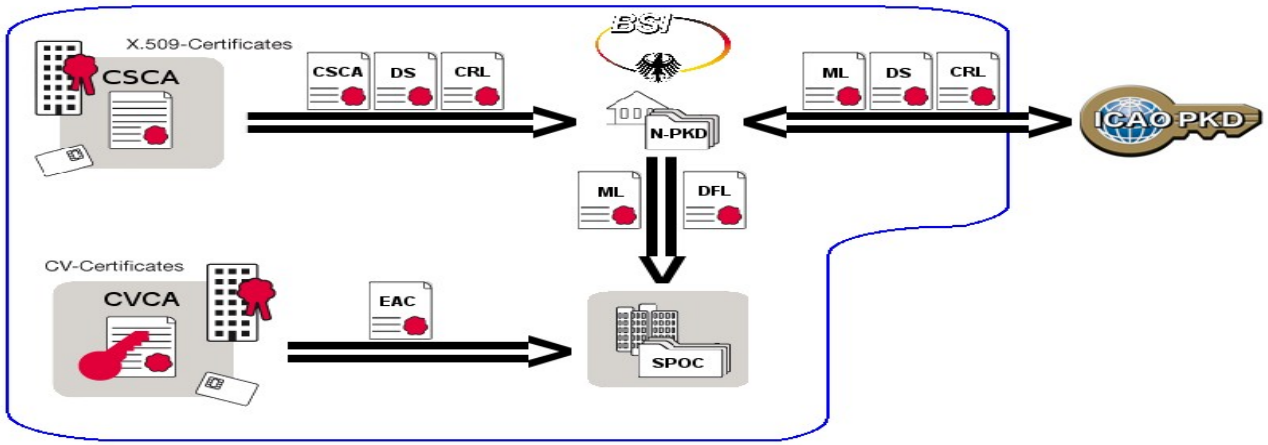
eMRTD PKI landscape
Additional EAC-PKI



- CVCA generates
  - Certificates for Extended Access Control (EAC)
- NPKD generates
  - Defectlists (DFL)

ıpur

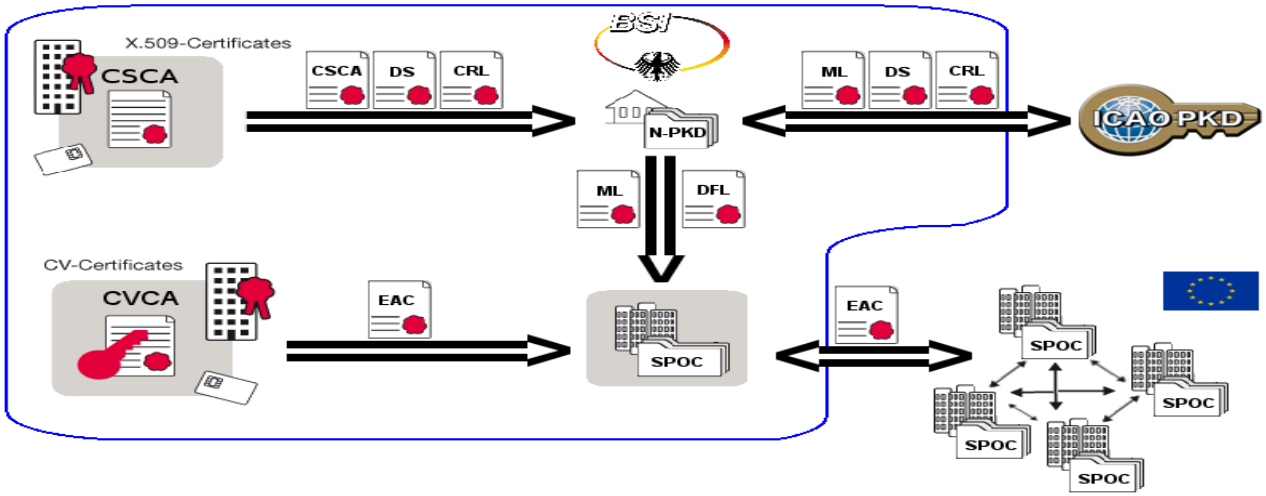
eMRTD PKI landscape
Additional EAC-PKI



- N-PKD provide to Single Point of Contact (SPOC)
  - Masterlists with all trusted CSCA certificates
  - Defectlists with all collected defect information and CRL

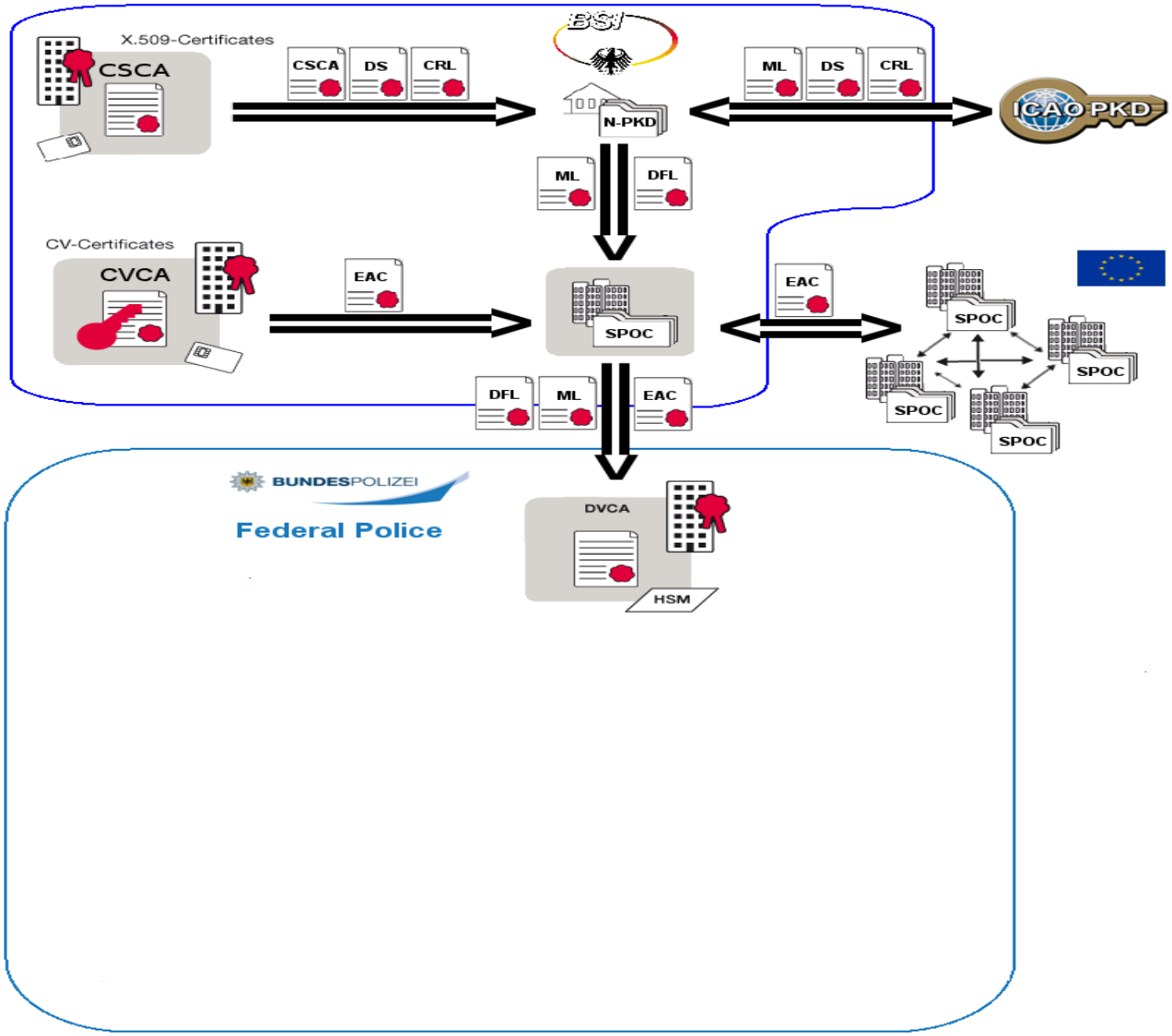
ıpur

eMRTD PKI landscape
Additional EAC-PKI



- Single Point of Contact (SPOC)
  - Provide and receive EAC certificates from other registered SPOCs within EU
  - Manage Registrations
  - Store and provide ML & DFL

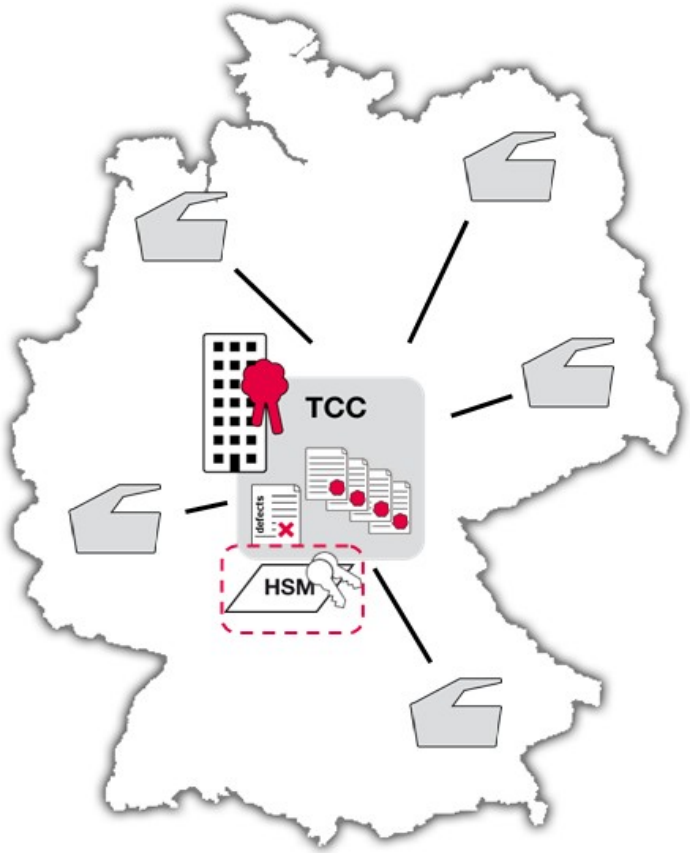
eMRTD PKI landscape
Additional EAC-PKI



- DVCA of Federal Police
  - Receives EAC certificates, Masterlists (ML) and Defectlists (DFL) from national SPOC

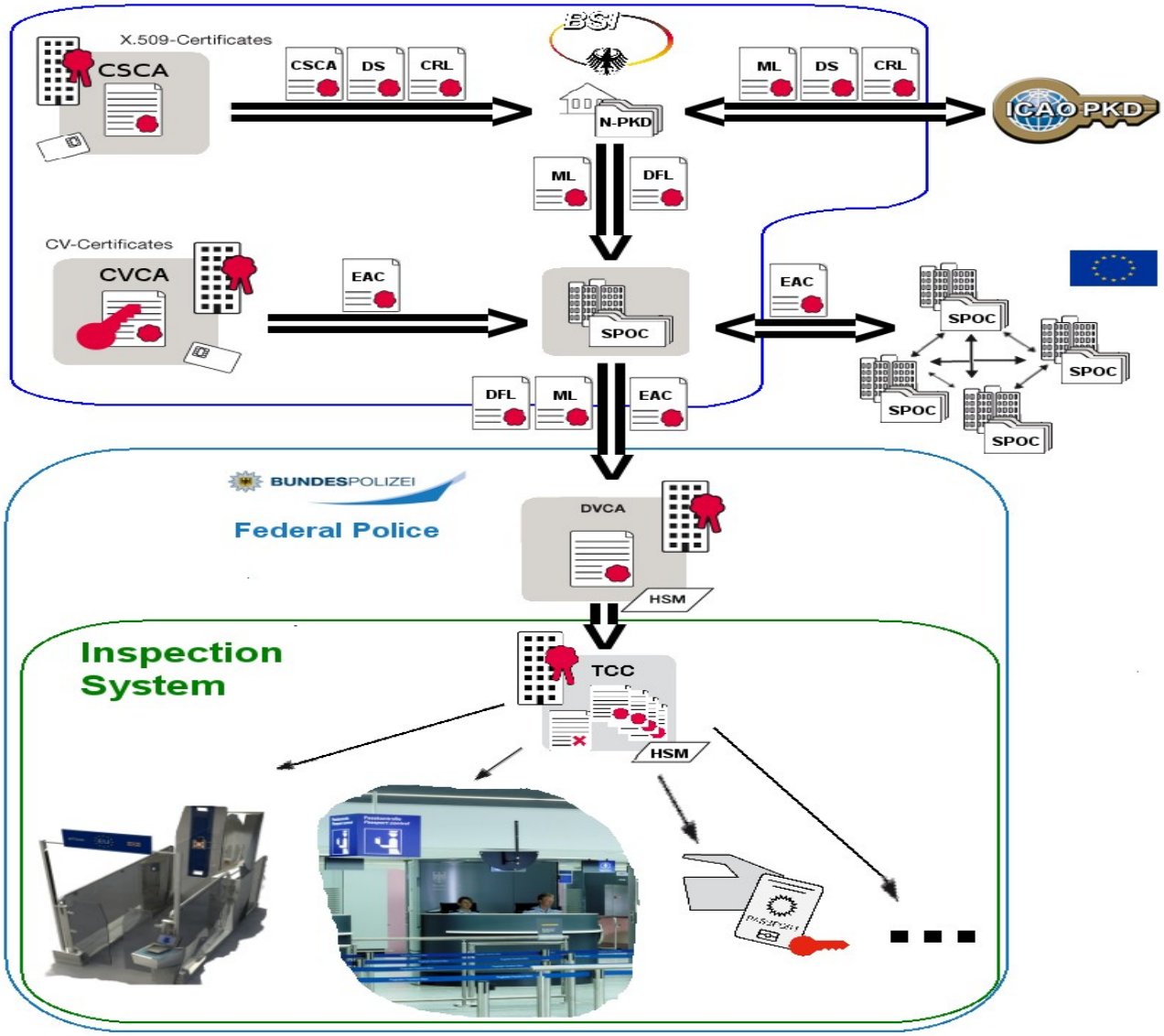
ıpur

TCC –
Terminal Control Center



- TCC as central PKI component
  - Centralized checking of DS certificates
  - Management of certificates and cryptographic keys
  - Authentication of connected terminals
  - Communication to DVCA and terminals via standardized interfaces

eMRTD PKI landscape in Q4/2011



eMRTD PKI landscape

- Specifications:
  - Country Verifying Certification Authority Key Management Protocol for SPOC CSN 36 9791
  - BSI TR-03110 Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents
- Additional for the German PKI:
  - BSI TR-03128 EAC-PKI for the electronic ID card
  - BSI TR-03129 PKIs for Machine Readable Travel Documents-Protocols for the Management of Certificates and CRLs

ePassport Based Identity Check with PKD, SPOC & TCC

- Exchange of CRL, DS and ML via ICAO PKD with 14 active PKD Participants (Nov 2011)
- Exchange of EAC certificates via SPOCs within EU (regular operation estimated Q3/2012)
- TCC to serve Federal Police with all needed certificates for manual and automated border control
- Nov. 2011 this include
  - Read and check ePassports from over 80 countries
  - Check complete chain of trust from 47 countries
  - Support for the new German ID Card

ePassport Based Identity Check for faster & secure border control and happy travelers

Thank you!

Federal Office for Information Security (BSI)

Benjamin Marzahn

benjamin.marzahn@bsi.bund.de
www.bsi.de