Federal Office
for Information Security

Reading Biometric Travel Documents at the Border Properly: State of Play, Challenges and Good Practices / Inspecting Travel Documents and Making Use of the Information

Markus Nuppeney

Section S13 – Inspection Infrastructures

Federal Office for Information Security (BSI)

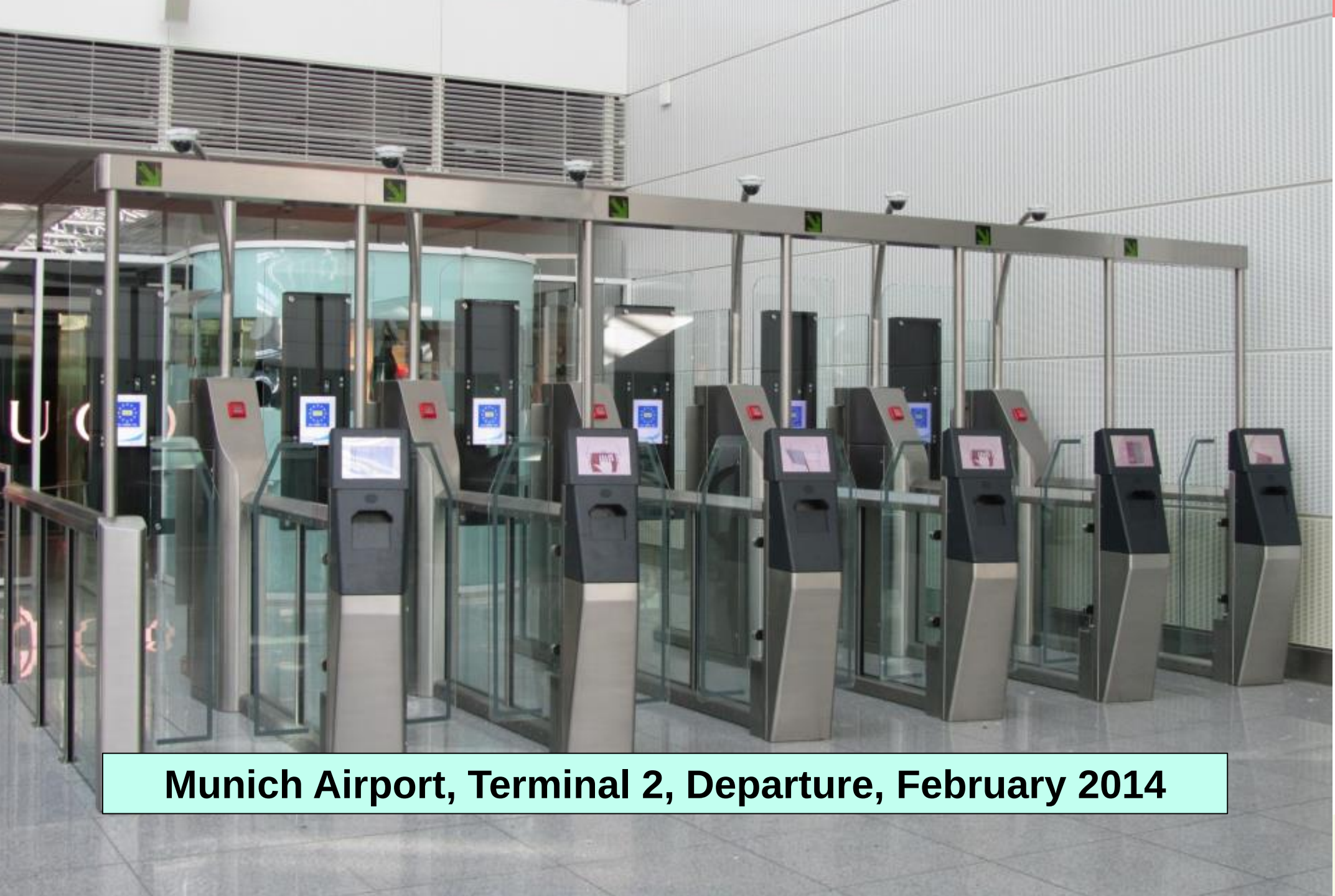
Automated Border Control (ABC) in Europe

- 15 European countries have ABC in operation (figures from 2014)
  - Total number of eGates: ≈ 450
  - Total pax throughput: ≈ 25 million
- Target group: EU/EEA/CH citizens (32 countries)
  - Extension to selected “Third Country Nationals” in some countries
- Token: ePassport
  - In addition national ID cards in some countries
- Biometric modality: primarily face
  - Multibiometrics (face and fingerprint) applied in some countries
  - “Fingerprint only” is applied in two countries

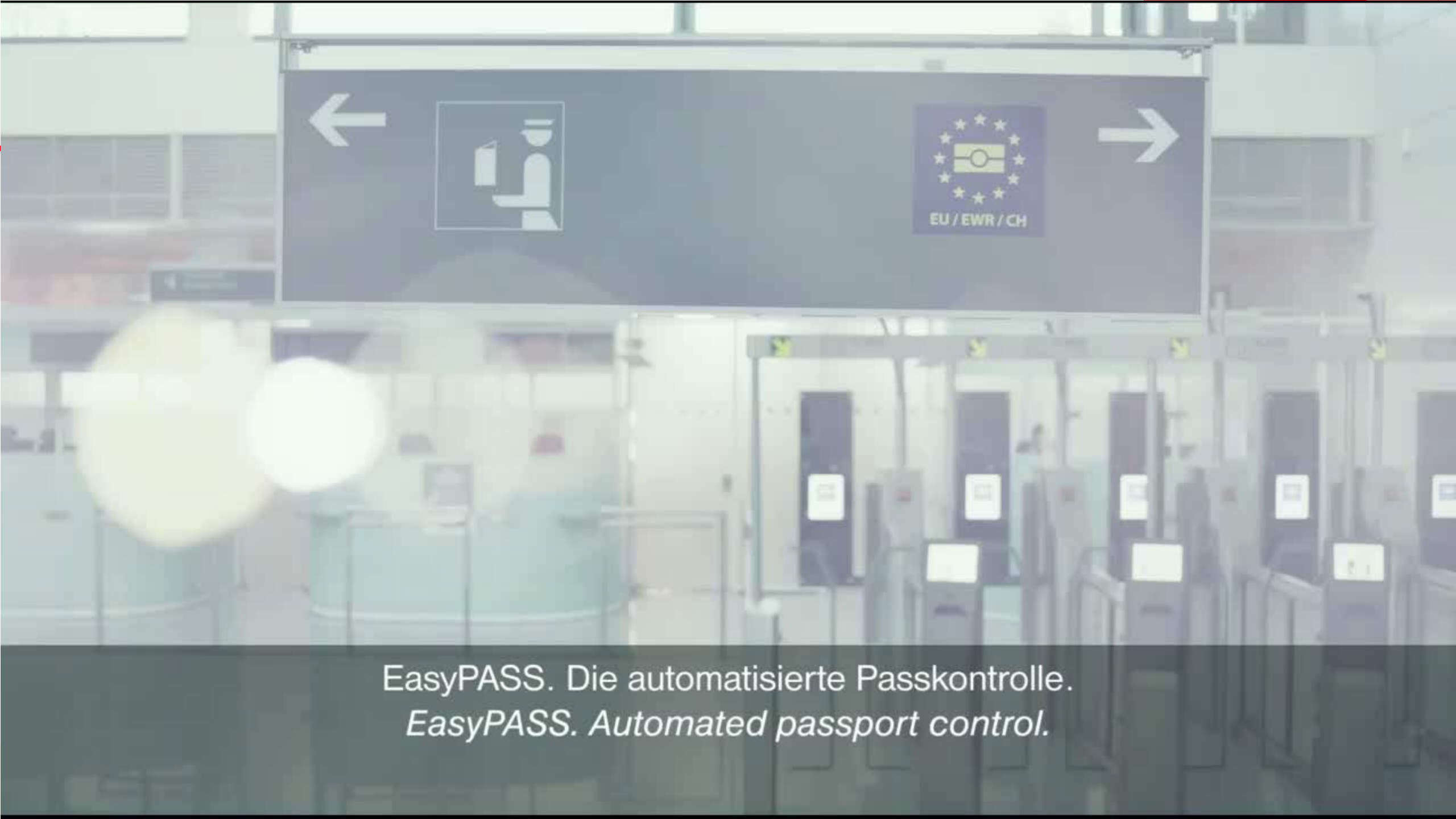
The EasyPASS ABC system

Federal Office for Information Security

- EasyPASS := German Automated Border Control (ABC) system
- eGate setting := Integrated 2-Step
  - Step 1: document authentication
  - Step 2: biometric face comparison
- Supported documents
  - ePassports
  - German electronic ID cards
- Delivered by to the consortium Bundesdruckerei / secunet
- 125 eGates installed at 6 German airports by Q3/2015
  - In total 140 eGate installations expected by end of 2015
- About 800.000 transactions per month (Sept. 2015)



Munich Airport, Terminal 2, Departure, February 2014



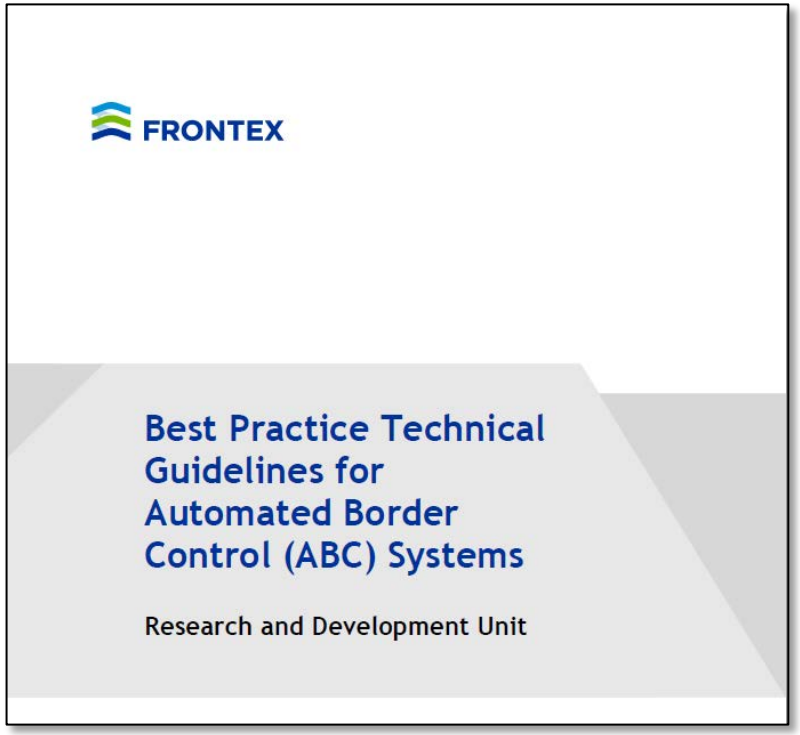
EasyPASS. Die automatisierte Passkontrolle.

EasyPASS. Automated passport control.

Electronic security features / electronic document checks

Federal Office for Information Security

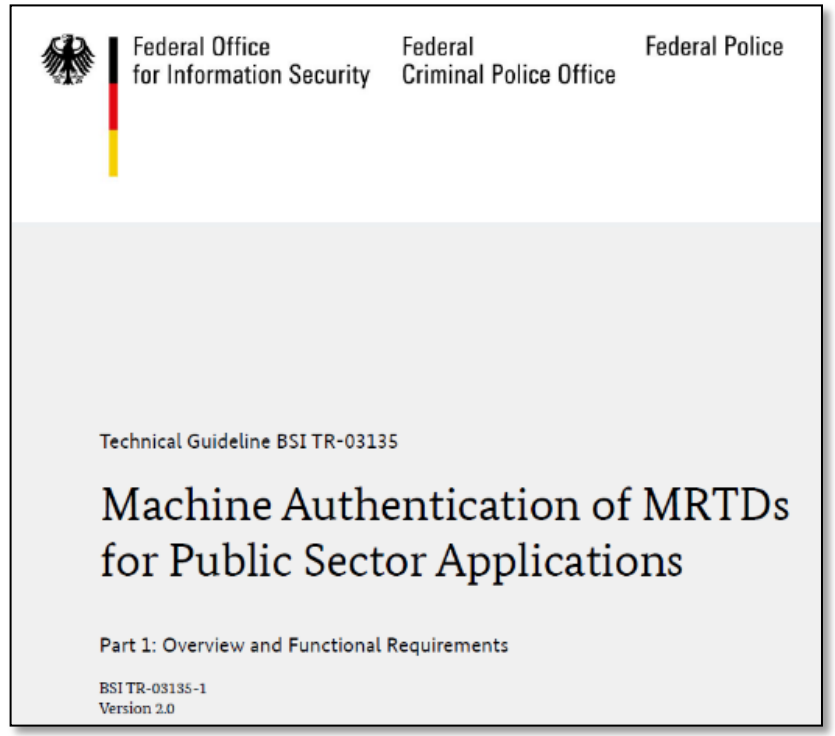
- Background Public Key Infrastructures (PKI, PKD)
- Checking chip access protocols (BAC, PACE, TA)
- Checking the chip's content
  - **Passive Authentication (PA)**
  - Chip authenticity (AA, CA)
- Main focus of Doc9303 is on the travel document itself
- Public available guidelines (complementing Doc9303) focusing on document inspection
  - By Frontex: Best Practice Technical Guidelines for ABC Systems
    - http://frontex.europa.eu/publications



Electronic security features / electronic document checks

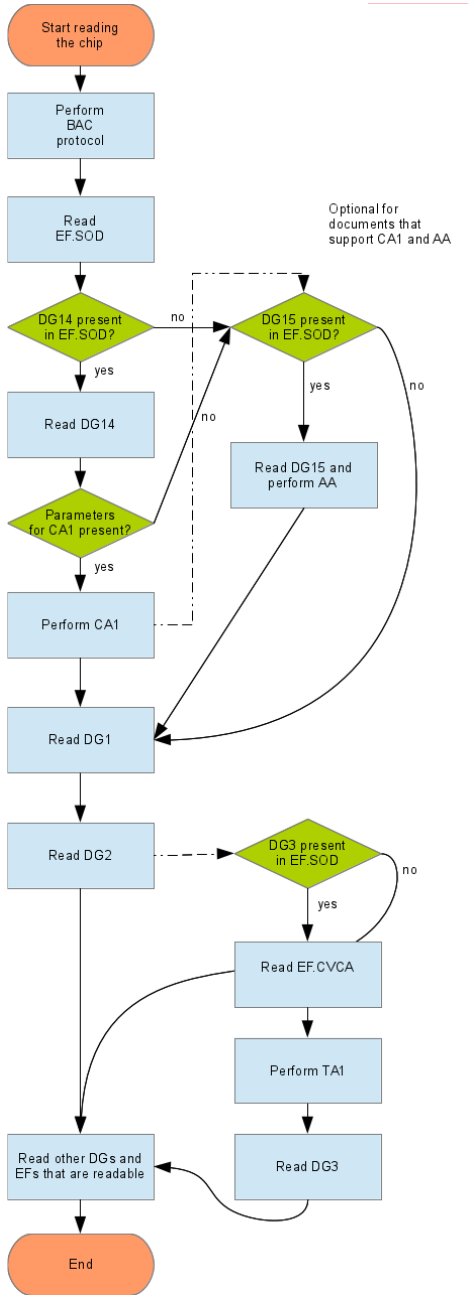
Federal Office for Information Security

- Background Public Key Infrastructures (PKI, PKD)
- Checking chip access protocols (BAC, PACE, TA)
- Checking the chip's content
  - **Passive Authentication (PA)**
  - Chip authenticity (AA, CA)
- Main focus of Doc9303 is on the travel document itself
- Public available guidelines (complementing Doc9303) focusing on document inspection
  - By Frontex: Best Practice Technical Guidelines for ABC Systems
    - http://frontex.europa.eu/publications
  - By BSI: Technical Guideline TR-03135 "Machine Authentication of MRTDs for Public Sector Applications"
    - https://www.bsi.de/tr03135



Passive Authentication for checking integrity and authenticity of eMRTD chip data

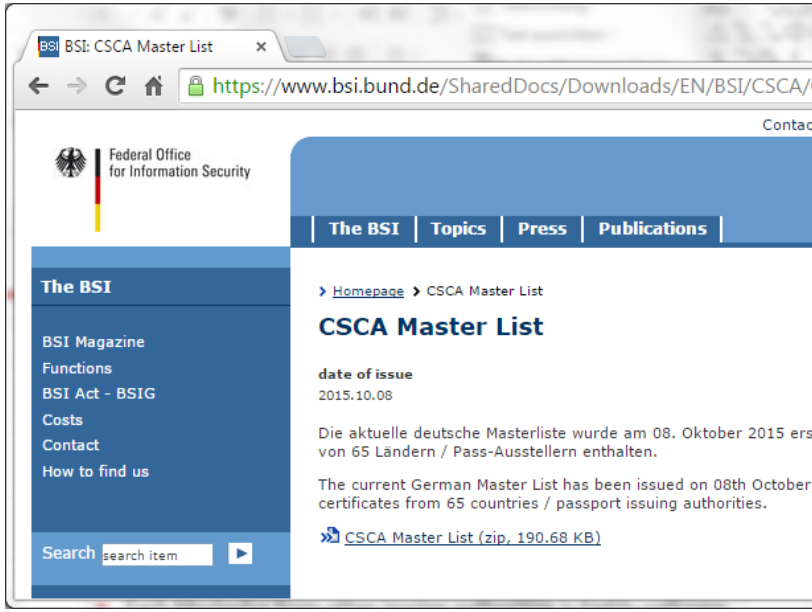
- Passive Authentication (PA)
  - THE FUNDAMENTAL electronic security feature
  - Authenticity and integrity of eMRTD chip data
  - Based on digital signatures and certificates
  - The only mandatory security feature according to Doc9303
- Implementing PA for document inspection requires several sub-processes
  - Verification of the eMRTD Security Object (EF.SOD)
  - **Checking issuer certificates (DS and CSCA certificate)**
  - Checking integrity of chip contents (data group integrity, EF.SOD vs. EF.COM)
  - Issuing state comparison (DG1 vs. DS certificate)



CSCA certificates / MasterLists

Federal Office for Information Security

- Biggest challenge as regards PA is the low availability of CSCA certificates
  - About 120 counties worldwide are issuing ePassports
  - 46 counties are participating in ICAO PKD
  - MasterLists are issued by only 5 countries (CH, DE, ES, FR, HU)
    - German MasterList holds CSCA certificates from 65 counties
    - http://www.bsi.de/csca
- International activities on MasterLists have been started recently
  - ICAO MasterList (lead by ICAO PKD Board)
  - Schengen MasterList (lead by the European Commission)
- Each MasterList from other issuing authorities is highly welcome
  - Allows for each country to check if the right CSCA certificates are included
  - Improvement regarding exchange and circulation of CSCA certificates
  - Essential contribution to the confidence level of CSCA certificates



Conclusion

- Document issuing authorities:
  - CSCA certificates MUST be shared / published in order to allow PA checks of eMRTDs at border control
  - **Certificates (public keys) need to be public !!!**

- Document inspection authorities:
  - Make sure to implement the entire / complete PA process within the document inspection infrastructure
    - Incl. a mandatory verification of the hole certificate chain
  - **There is no added value from eMRTD chip data, if not authenticated !!!**

Thank you!

Federal Office for Information Security

- Federal Office for Information Security (BSI)
- Markus Nuppeney
  - markus.nuppeney@bsi.bund.de
  - https://www.bsi.de