E-Passport Testing

Ensuring Global Acceptance

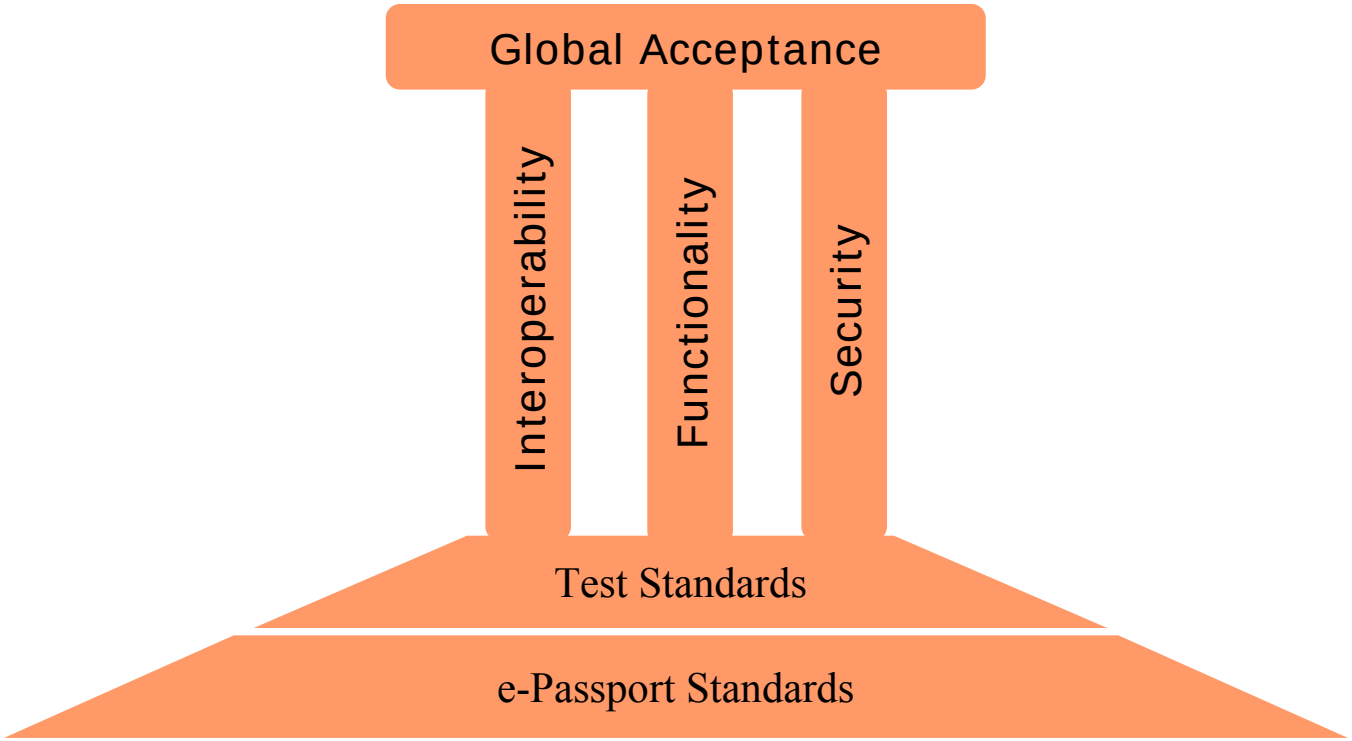
By: Jos Chehin

Date: 17 November 2006

Location: ASML

Collis

Global Acceptance of the e-Passport

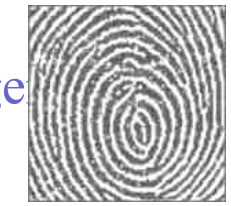


Agenda

- The e-Passport
- The ICAO/ISO e-Passport Standards
- Test coverage of the Application Protocol and Logical Data Structure Test Standard
- Findings and Conclusions

The e-Passport

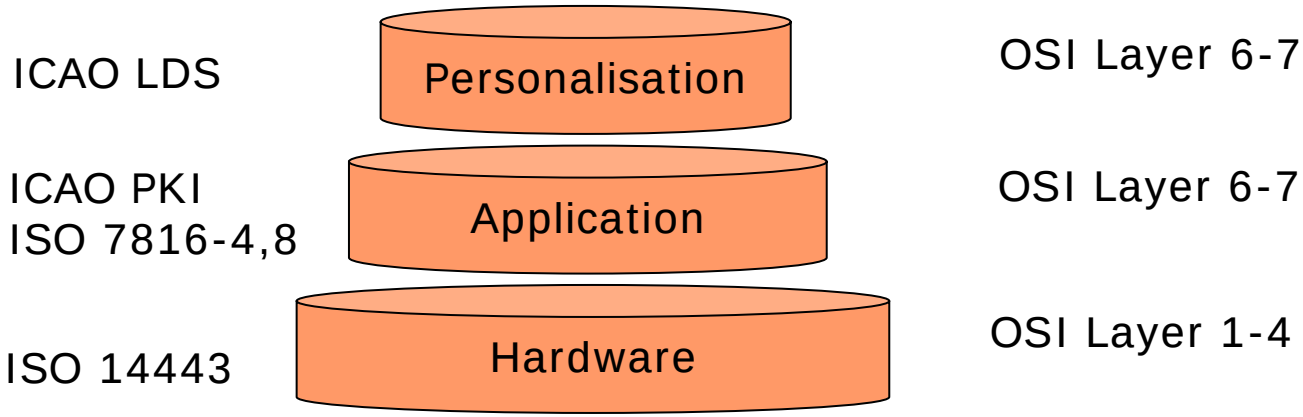
- Contactless chip
  - Processing capability
  - Data storage
- PKI
- Biometrics (Face, finge
  eyes)



- Secure electronic identification

The e-Passport Standards

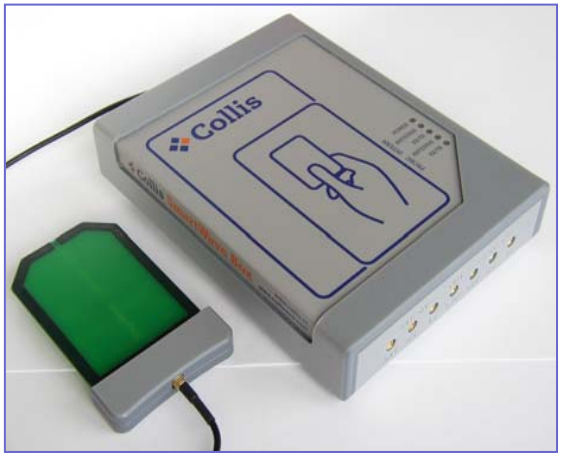
- ISO 14443
- Public Key Cryptography conform to the ICAO PKI standard
- The ISO 7816-4 Standard
- Standard for the e-Passport Logical Data Structure (LDS)



Testing the e-Passport Hardware

- Collis SmartWave box
  - Reads/simulates
- Test Suite's
- Low level interoperability

- Low level interoperability test events (ISO 14443):
  - Cross-over testing
  - 'interoperability' rates
    - 93% in Singapore
    - 87% in Berlin
    - Readable ≠ ISO/ICAO conformance

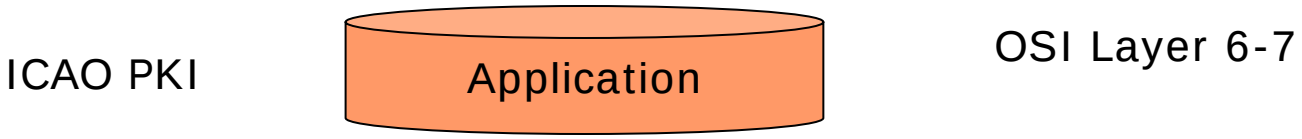


e-Passport Security Mechanisms

Security mechanisms:

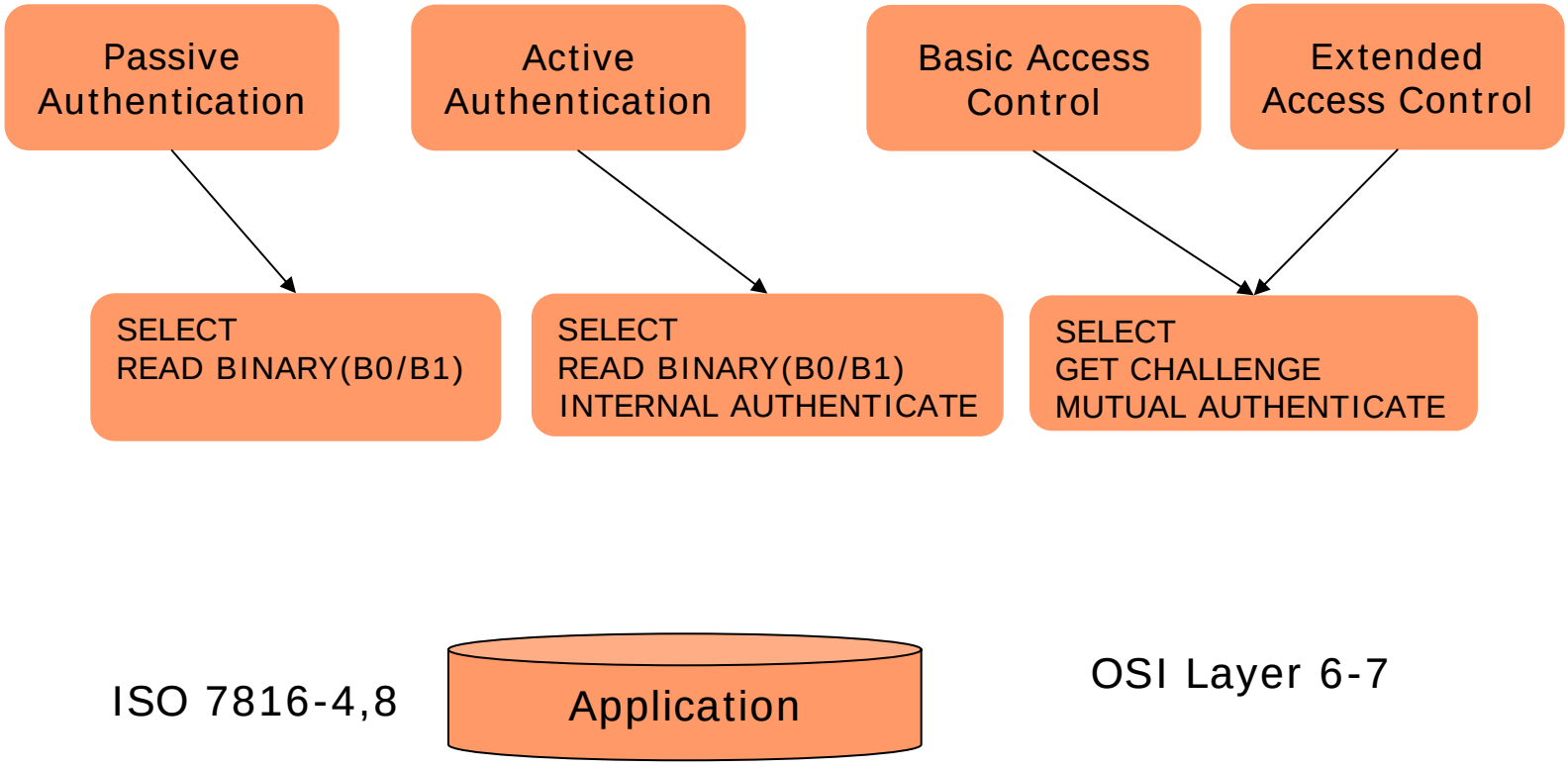
- Passive Authentication (Mandatory)
- Active Authentication (Optional)
- Basic Access Control (Optional)
- Extended Access Control (Optional)

"Issuing States MAY choose additional security, using more complex ways of securing the chip and its data. "

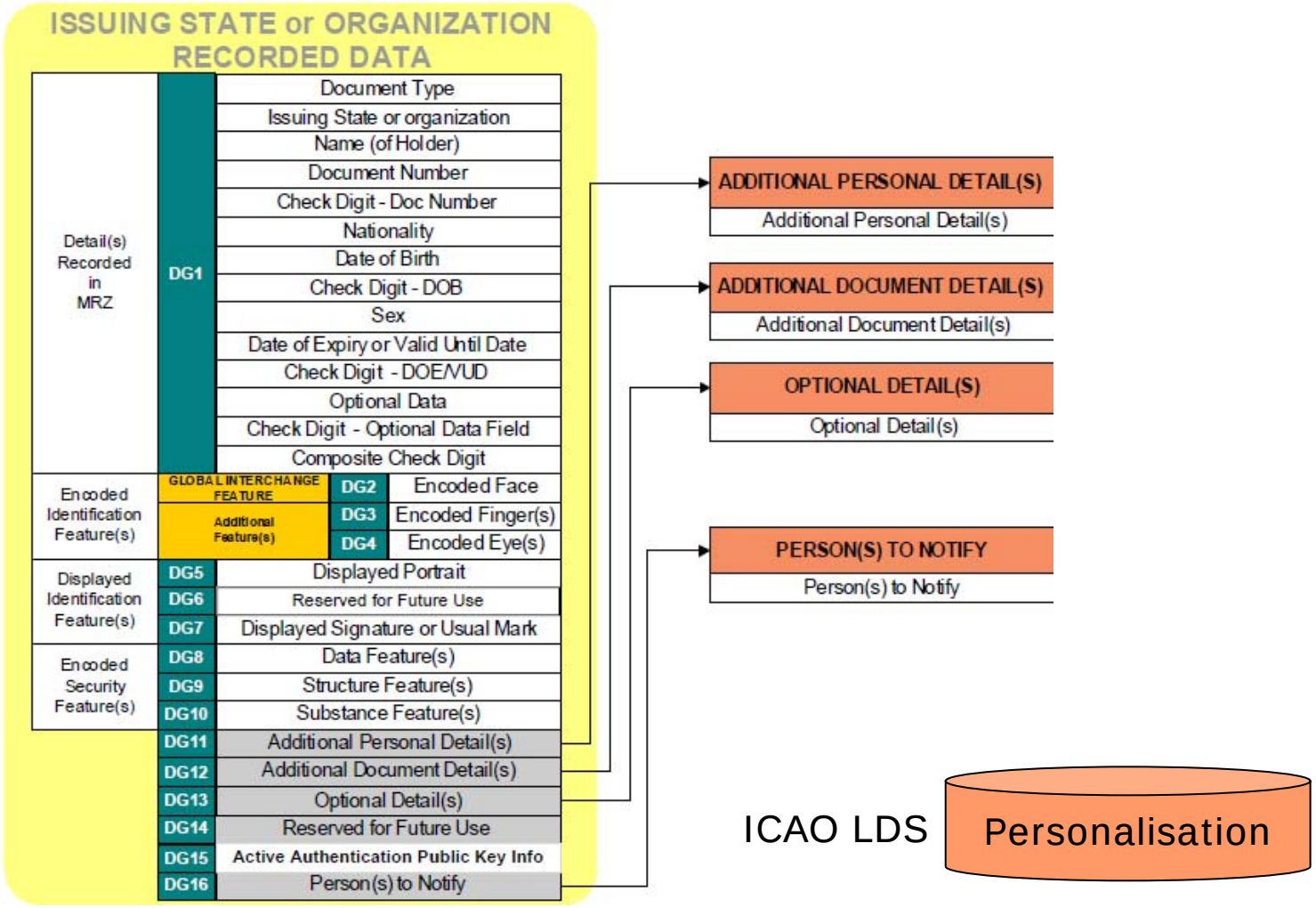


e-Passport Smartcard Commands

- e-Passport to reader communication on APDU level



The e-Passport LDS



Testing the e-Passport Application and LDS

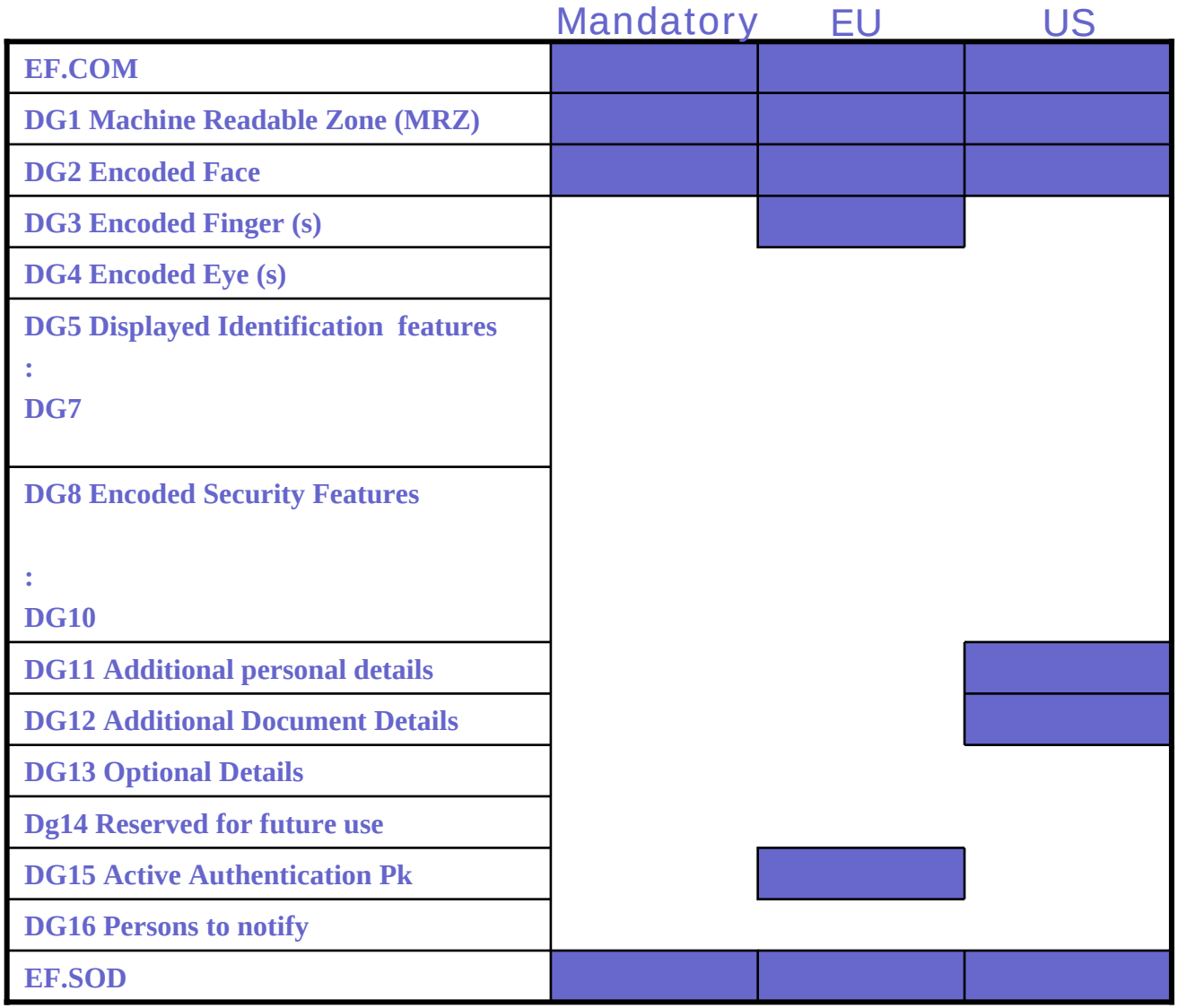
- ICAO/ISO Test Standard
- Security
  - Security Mechanisms
- Smartcard commands
  - Positive
  - Negative
- The LDS
  - Encoding of the LDS data objects

Test Coverage of the ICAO PKI Test Standard

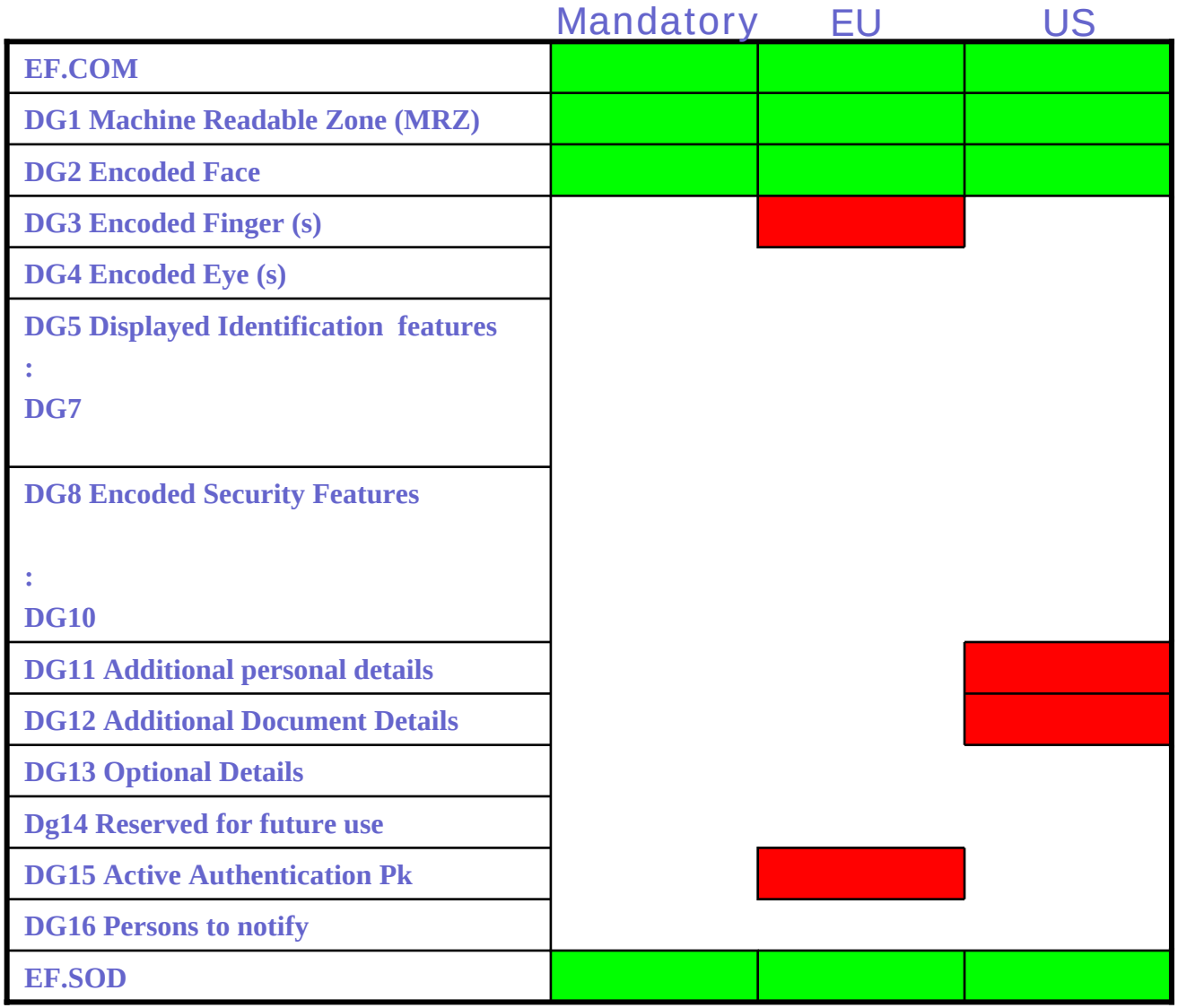
	Mandatory	EU	US
Passive Auth.			
Active Auth.			
Basic Access Control			
Extended Access Control			

	Mandatory	EU	US
Passive Auth.			
Active Auth.			
Basic Access Control			
Extended Access Control			

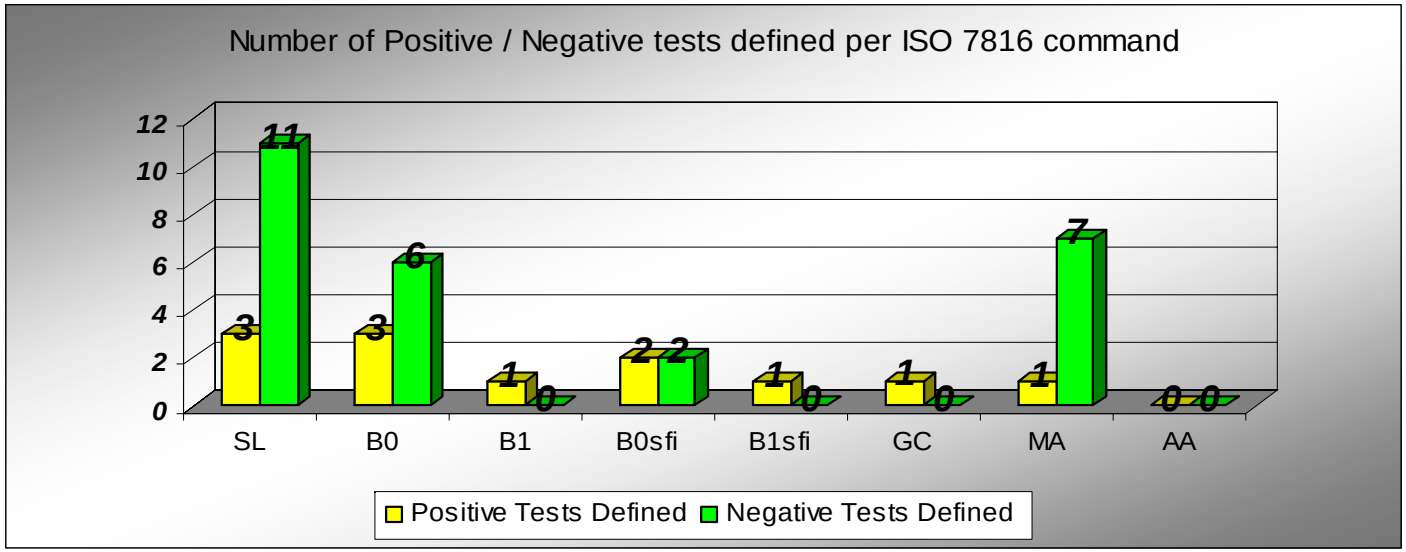
Test Coverage of the ICAO LDS Test Standard



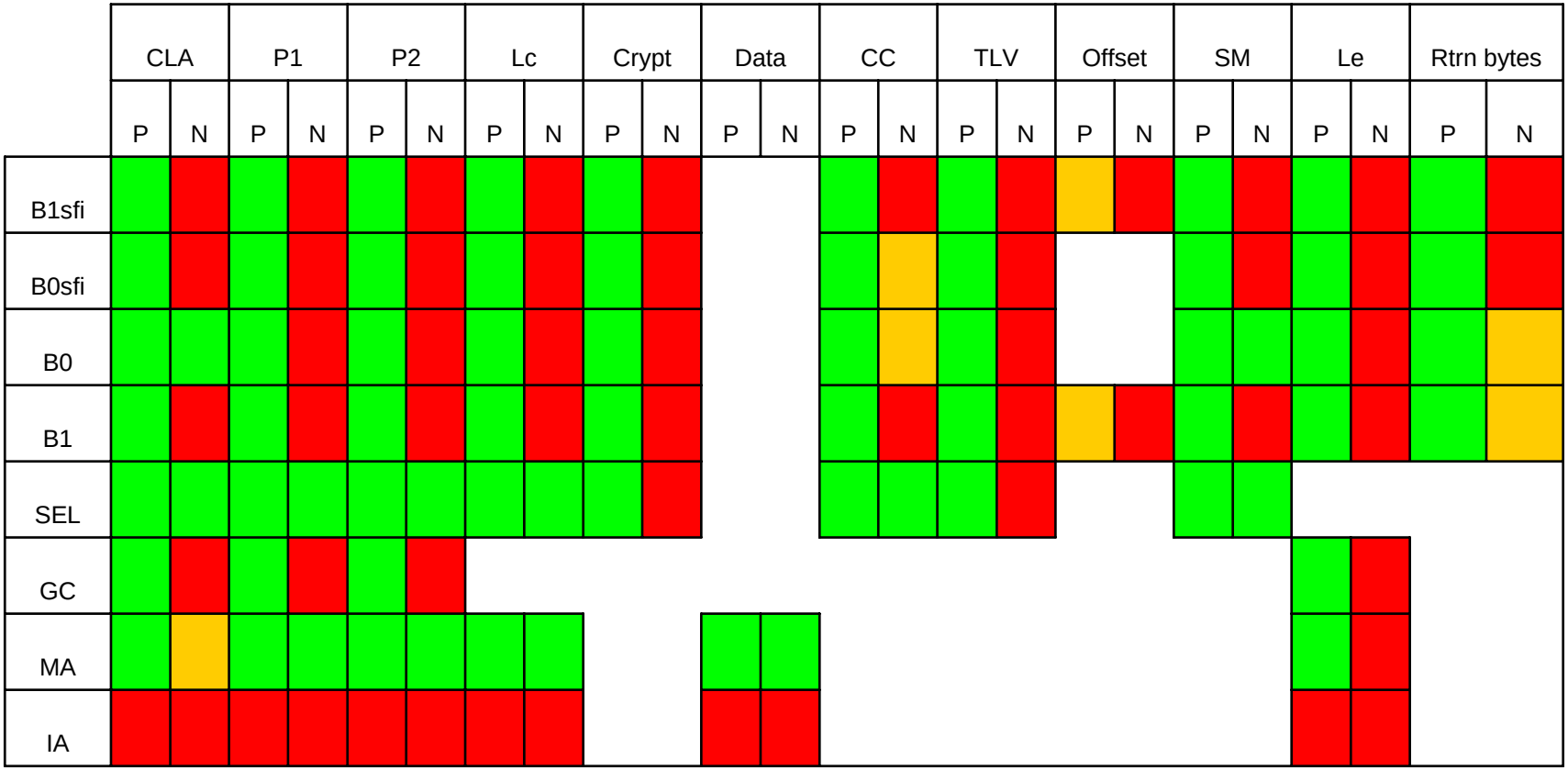
Test Coverage of the ICAO LDS Test Standard



Smartcard Command APDU Tests

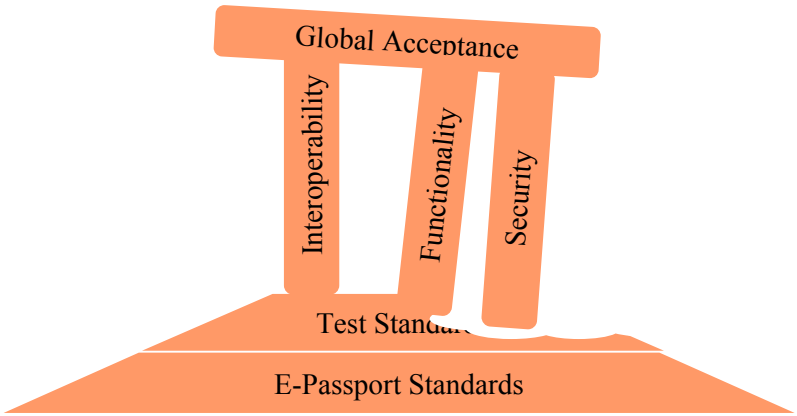


ISO 7816 Command Test Coverage Matrix



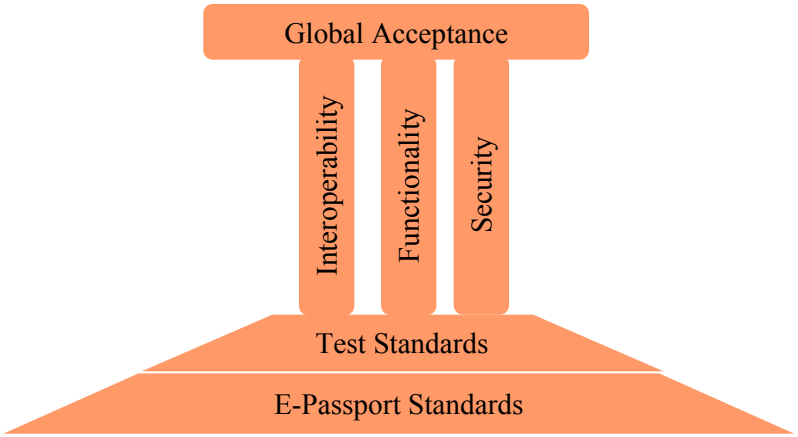
Findings

- Some optional, but important security features not covered by the ICAO test standard (AA, EA)
- e-Passport chip response on incorrect commands not tested thouroughly (negative tests)
- Gaps in the test specification



Recommendation

- Additional tests need to be developed to fill up gaps in the test specification



-End-