

# E-Passport Testing

## Ensuring Global Acceptance

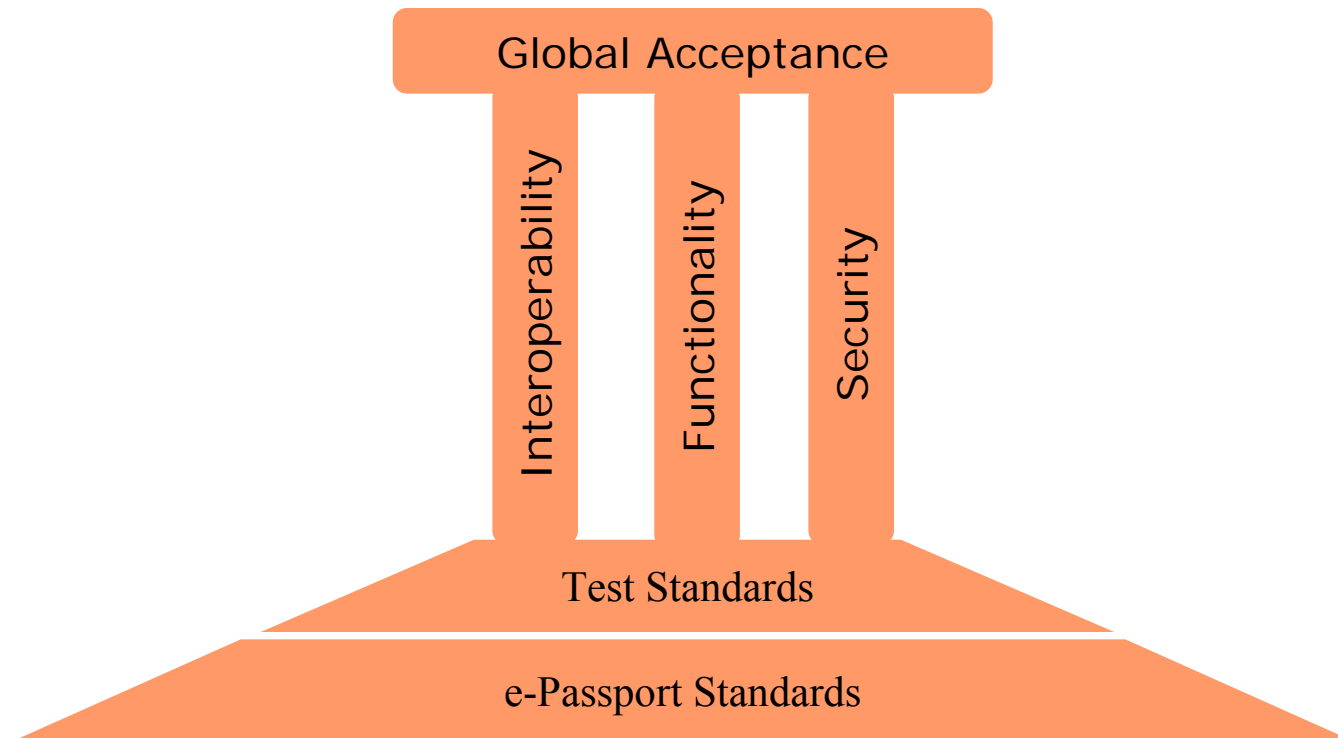
By: Jos Chehin

Date: 17 November 2006

Location: ASML



# Global Acceptance of the e-Passport

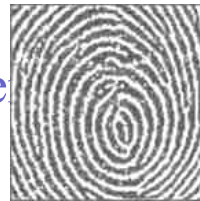


## Agenda

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

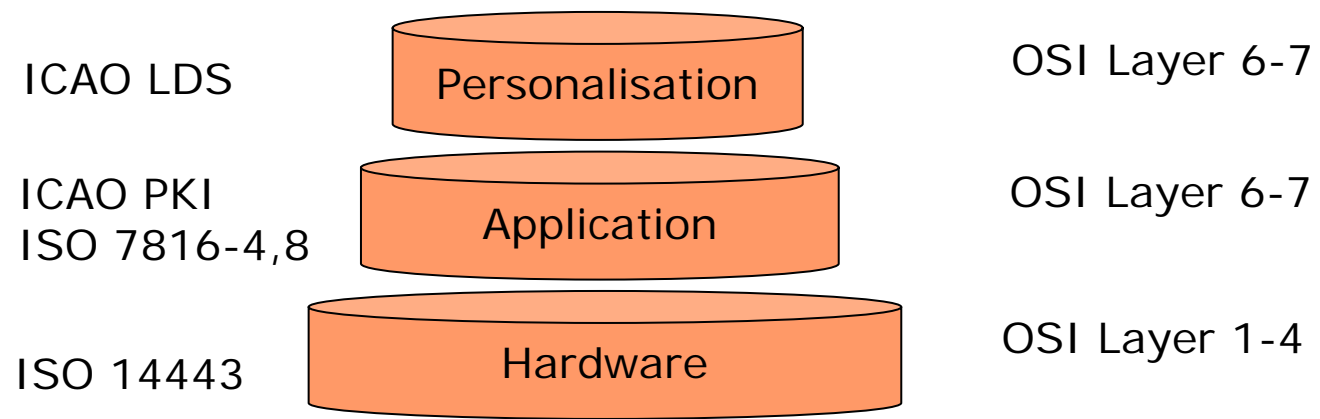
## The e-Passport

- ❖ Contactless chip
  - ❖ Processing capability
  - ❖ Data storage
- ❖ PKI
- ❖ Biometrics (Face, finger, 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  $\neq$  ISO/ICAO conformance



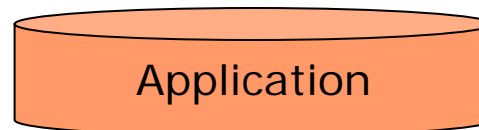
## e-Passport Security Mechanisms

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.”*

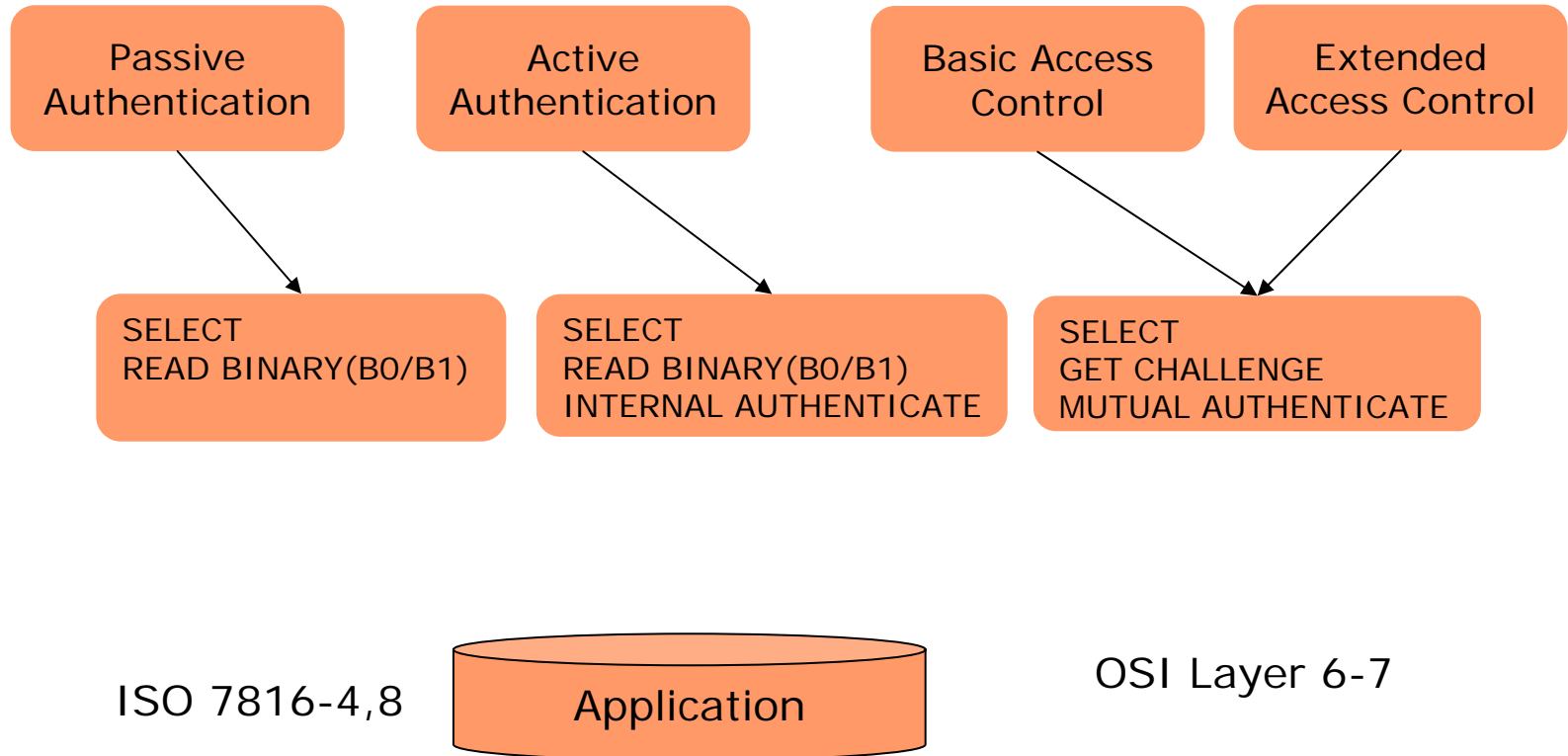
ICAO PKI



OSI Layer 6-7

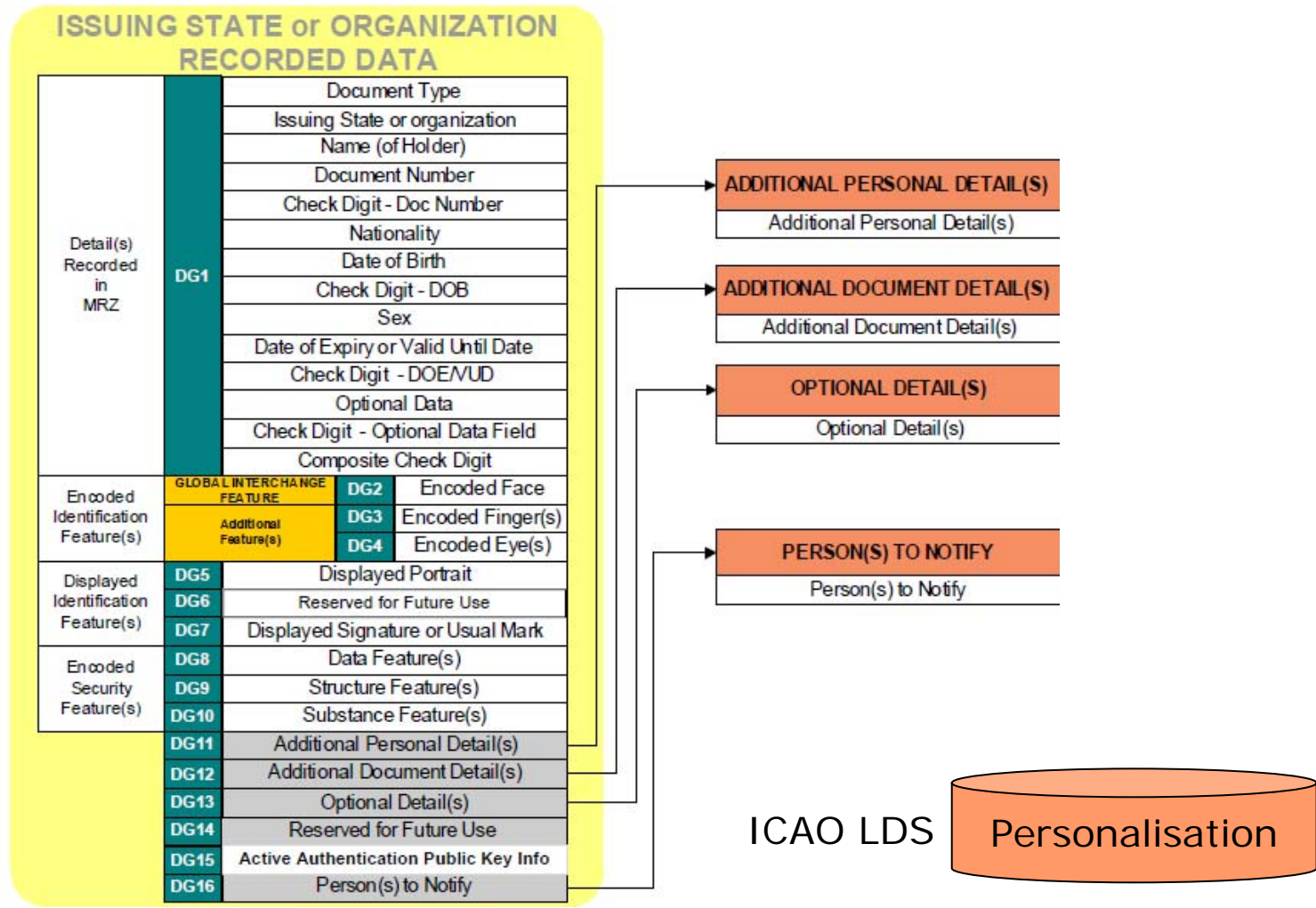
## e-Passport Smartcard Commands

❖ 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
<b>Passive Auth.</b>			
<b>Active Auth.</b>			
<b>Basic Access Control</b>			
<b>Extended Access Control</b>			

	Mandatory	EU	US
<b>Passive Auth.</b>			
<b>Active Auth.</b>			
<b>Basic Access Control</b>			
<b>Extended Access Control</b>			

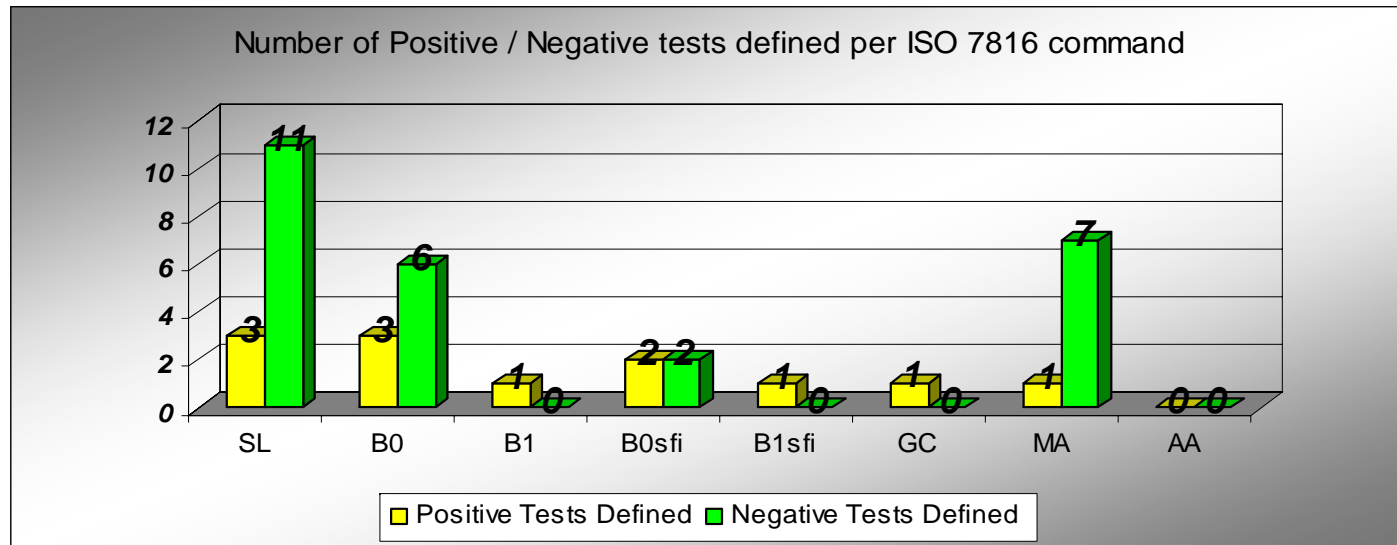
## Test Coverage of the ICAO LDS Test Standard

	Mandatory	EU	US
EF.COM	Yes	Yes	Yes
DG1 Machine Readable Zone (MRZ)	Yes	Yes	Yes
DG2 Encoded Face	Yes	Yes	Yes
DG3 Encoded Finger (s)	No	Yes	No
DG4 Encoded Eye (s)	No	No	No
DG5 Displayed Identification features : DG7	No	No	No
DG8 Encoded Security Features : DG10	No	No	No
DG11 Additional personal details	No	No	Yes
DG12 Additional Document Details	No	No	Yes
DG13 Optional Details	No	No	No
Dg14 Reserved for future use	No	No	No
DG15 Active Authentication Pk	No	Yes	No
DG16 Persons to notify	No	No	No
EF.SOD	Yes	Yes	Yes

## Test Coverage of the ICAO LDS Test Standard

	Mandatory	EU	US
EF.COM	Green	Green	Green
DG1 Machine Readable Zone (MRZ)	Green	Green	Green
DG2 Encoded Face	Green	Green	Green
DG3 Encoded Finger (s)		Red	
DG4 Encoded Eye (s)			
DG5 Displayed Identification features : DG7			
DG8 Encoded Security Features : DG10			
DG11 Additional personal details			Red
DG12 Additional Document Details			Red
DG13 Optional Details			
Dg14 Reserved for future use			
DG15 Active Authentication Pk		Red	
DG16 Persons to notify			
EF.SOD	Green	Green	Green

# Smartcard Command APDU Tests

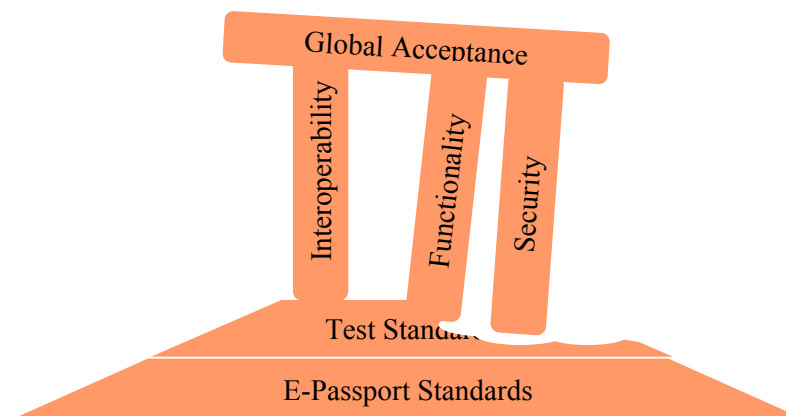


# ISO 7816 Command Test Coverage Matrix

	CLA		P1		P2		Lc		Crypt		Data		CC		TLV		Offset		SM		Le		Rtrn bytes	
	P	N	P	N	P	N	P	N	P	N	P	N	P	N	P	N	P	N	P	N	P	N	P	N
	B1sfi	Green	Red	Green	Red	Green	Red	Green	Red	Green	Red			Green	Red	Green	Red	Yellow	Red	Green	Red	Green	Red	Green
B0sfi	Green	Red	Green	Red	Green	Red	Green	Red	Green	Red			Green	Yellow	Green	Red			Green	Red	Green	Red	Green	Red
B0	Green	Green	Green	Red	Green	Red	Green	Red	Green	Red			Green	Yellow	Green	Red			Green	Green	Green	Red	Green	Yellow
B1	Green	Red	Green	Red	Green	Red	Green	Red	Green	Red			Green	Red	Green	Red	Yellow	Red	Green	Red	Green	Red	Green	Yellow
SEL	Green	Green	Green	Green	Green	Green	Green	Green	Green	Red			Green	Green	Green	Red			Green	Green				
GC	Green	Red	Green	Red	Green	Red															Green	Red		
MA	Green	Yellow	Green	Green	Green	Green	Green	Green			Green	Green									Green	Red		
IA	Red	Red	Red	Red	Red	Red	Red	Red			Red	Red									Red	Red		

## Findings

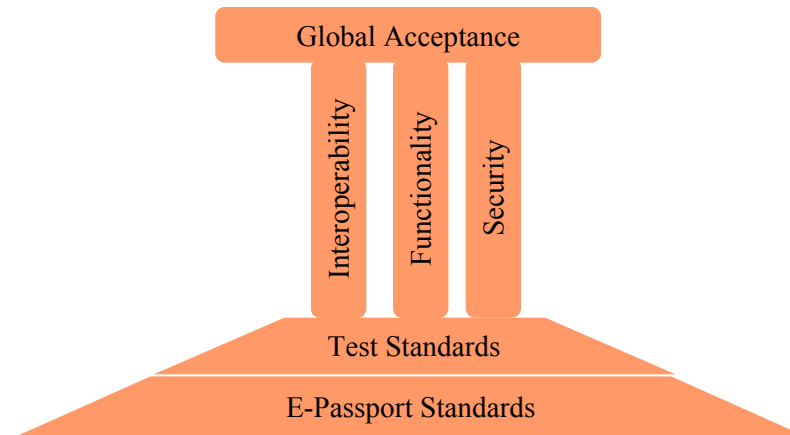
- ❖ Some optional, but important security features not covered by the ICAO test standard (AA, EA)
- ❖ e-Passport chip response on incorrect commands not tested thoroughly (negative tests)
- ❖ Gaps in the test specification





## Recommendation

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



-End-