

INTEGR I Testing and Test Tools <as easy as it looks>

Testing and Test Tools

e-Passports Interoperability



Copyright (c) Integri 2006 Page 1

INTEGR I Testing and Test Tools <as easy as it looks>

Testing and Test Tools

e-Passports Interoperability

- Outline
 - Introduction
 - Cross-Over Testing & Parametric Testing
 - ICAO Tests - e-Passport Conformity Certificate
 - Questions



Copyright (c) Integri 2006 Page 2

■ Introduction (1)

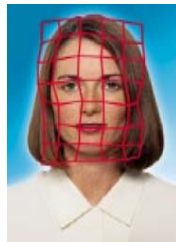
- In the early 80's, first specifications for machine readable travel documents (MTRD) written by International Civil Aviation Organisation (ICAO).
- Over the years, evolution of this technology from documents suitable for optical character recognition (OCR) towards documents with embedded contactless smart card technology offering possibility to store biometric data in a secure way.
- The aim of this migration to contactless chip passports for citizens and visa waiver countries is to strengthen laws and processes around border control and immigration.

■ Introduction (2)

- In today's world, international travel is common. More and more people are free to travel abroad either for business or leisure.
- Increased demand to control and monitor growing flows of people when crossing national borders → Electronic passports linked with international exchange of information
- On global scale, with a large difference in infrastructure, interoperability is vital. All e-Passports issued should be readable on all card readers, worldwide. An error in the application has a widespread impact.

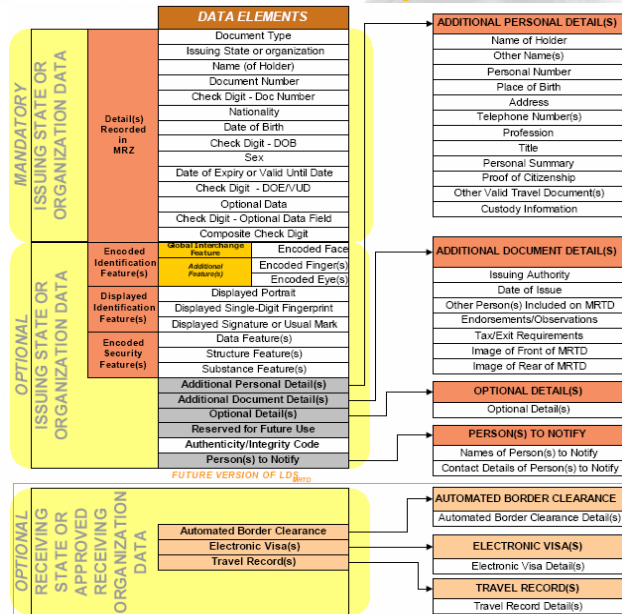
■ Introduction (3)

- ICAO defines basic, mandatory set of protocol, application data and security requirements for e-Passports and readers for their interoperability.
- In addition, more advanced and optional data set (including biometric data of retinal scans, fingerprints, facial information) and an advanced set of security requirements



■ Introduction (4)

- Logical Data Structure (LDS) Mandatory & Optional Data Elements



INTEGRI **Testing and Test Tools**
<as easy as it looks>

- **Introduction (4)**
 - Beyond technology – Focus on Trust and Security
 - Modern e-passports are
 - **Physical document**, with data page, MRZ and well proven security features establishing trust in physical passport book.
 - **Digital document**, with RF chip, personal and biometric features, protected by cryptographic security features, establishing trust in digital data.
 - **Privacy protecting features**, establishing confidence in legal and conscious use of personal data.
 - Beyond the pure functional testing – Physical and digital security measures
 - Focus on mandatory Passive Authentication Scheme standardized in **public key infrastructure (PKI)** – arrangement that binds public keys with respective user identities by means of a certificate authority (**CA**). The user identity must be unique for each CA.
 - Test and report performance with respect to ability of systems to check integrity and authenticity of digitally signed data on e-passports.

Copyright (c) Integri 2006 Page 7

INTEGRI **Testing and Test Tools**
<as easy as it looks>

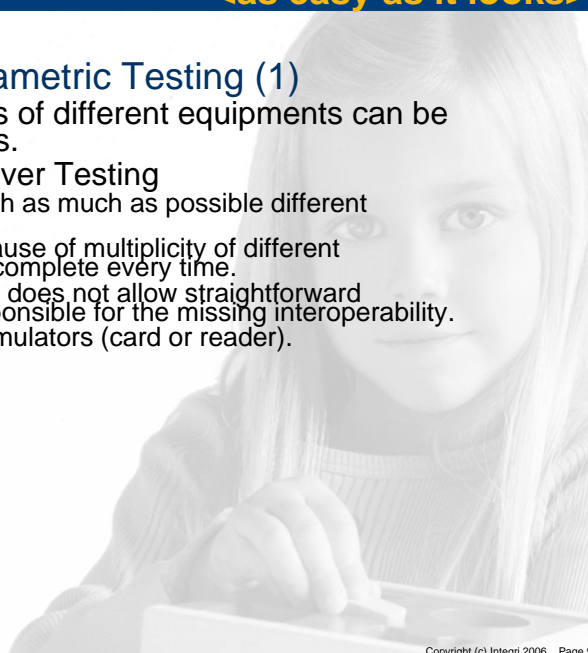
Testing and Test Tools

e-Passports Interoperability

- **Outline**
 - Introduction
 - Cross-Over Testing & Parametric Testing
 - ICAO Tests - e-Passport Conformity Certificate
 - Questions

Copyright (c) Integri 2006 Page 8

- **Cross-Over Testing & Parametric Testing (1)**
 - Communications capabilities of different equipments can be proofed by different methods.
 - Industry first move: Cross-Over Testing
 - Performing functional tests with as much as possible different passports and readers.
 - Principally extensive and because of multiplicity of different implementations it cannot be complete every time.
 - In case of error this procedure does not allow straightforward conclusion of parameters responsible for the missing interoperability.
 - It means implementation of simulators (card or reader).



- **Cross-Over Testing & Parametric Testing (2)**
 - Industry implements common understanding of ICAO recommendations (LDS and PKI) → Golden Reader Tool (e-Passport Reader simulator)
 - Since 2004, industry organizes events like Berlin e-passport interoperability test event
 - 350+ registered participants from 38 countries
 - 400+ e-passports samples from 175 countries and companies
 - 48 readers from 38 different companies and organizations



E-PASSPORT INTEROPERABILITY TEST EVENT
29 MAY – 1 JUNE 2006, BERLIN / GERMANY

■ Cross-Over Testing & Parametric Testing (3)

- A more systematic approach: parametric testing of chips within dedicated certification systems.
- Parameters relevant for Interoperability of the test sample are collected in a test setup and compared with specifications requirements → Test Scenarios
- Challenge is to ensure a lasting global interoperability for e-passports (Valid 5 to 10 years)
 - Different chip generations and types
 - Different readers generations (firmware) and types
- This goal is not reachable via Cross-Over Testing only
- These issues can only be addressed by international accepted test specifications to ensure conformity

■ Cross-Over Testing & Parametric Testing (4)

- Based on functional specifications, ICAO defines test scenarios to validate e-Passport implementation. A set of test scenarios deals with contactless interface level.
- These tests cover physical and electrical parameters, initialization and anticollision as well as transport protocol. Another part covers conformance of ISO7816 chip card commands and conformance of application data (LDS).
- Parametric Conformity Testing Certification Scheme implies:
 - Test Tools implementing Test Scenarios, automating Test Scenarios Executions and Execution Results Validation
 - Accreditation of test labs for each Issuing Country using combinations of those Test Tools
 - Certification of official Test Tools
 - Providing Industry with Test Tools for in-house Testing before going to expensive certification processes

Testing and Test Tools

e-Passports Interoperability

■ Outline

- Introduction
- Cross-Over Testing & Parametric Testing
- ICAO Tests – e-Passport Conformity Certificate
- Questions

■ ICAO Tests – e-Passport Conformity Certificate (1)

- Four parts of test standard
 - Part 1: Framework and Scope
 - Part 2: Signal interface and RF protocol (Layer 1-4)
 - Part 3: Application interface (Layer 6-7)
 - Part 4: PCD: Signal interface and RF protocol (Layer 1-4)
- ISO/IEC 14443 : Communication up to 10cm,
 Data rate from 106 kbits/s up to 848 kbits/s
 - 14443-1 → Physical characteristics
 - 14443-2 → Radio frequency power and signal interface
 - 14443-3 → Initialization and anticollision
 - 14443-4 → Transmission protocol



INTEGRi **Testing and Test Tools**
 <as easy as it looks>

■ ICAO Tests – e-Passport Conformity Certificate (2)
 – Presentation focuses on e-Passport Testing Card Side (Part 2 & 3)

Copyright (c) Integri 2006 Page 15

INTEGRi **Testing and Test Tools**
 <as easy as it looks>

■ ICAO Tests – e-Passport Conformity Certificate (3)
 – Highlights of ICAO & ISO Conformity Testing Layers 1 - 4


- Parametric testing
 - all characteristics which are important for interoperability are tested separately
- Controllable testing
 - no influence from other instances than THE device under test
- Repeatable
 - test are to be performed in lab environment monitoring all parameters that can have influence
- Single-ended testing
 - only The Device under Test is tested and not a combination of devices that are more or less known
- Application-independent
 - The tests can be performed for all systems using ISO 14443 which is broadening the acceptance
- After successful testing Conformity Certificate is available

Copyright (c) Integri 2006 Page 16

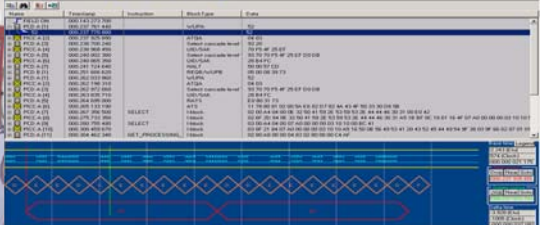
INTEGRI **Testing and Test Tools**
 <as easy as it looks>

■ ICAO Tests – e-Passport Conformity Certificate (4) – L1 to L4


L1: Physical characteristics



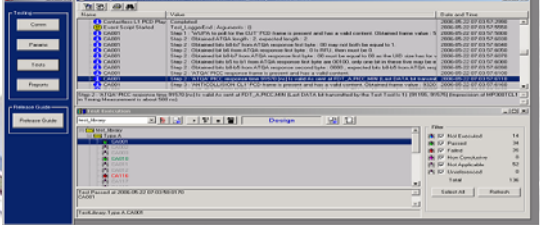
L3: RF protocol activation



L2: RF power and signal interface



L4: RF transmission protocol

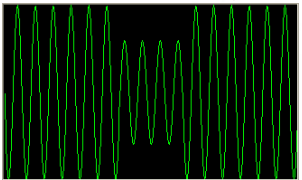



Copyright (c) Integri 2006 Page 17

INTEGRI **Testing and Test Tools**
 <as easy as it looks>

■ ICAO Tests – e-Passport Conformity Certificate (5) – L1 to L4

- The Proximity Coupling Device (PCD) generates a RF field via an antenna. Frequency is equal to 13.56 MHz
- The field strength is expressed in Amperes per meter (A/m)
- The proximity card (PICC) capture the RF field via its antenna
- The induced current allows to power-up the PICC
- The PCD communicates with the PICC coding using the Amplitude Shift Keying (ASK)

- To communicate with the PCD, the PICC modulates the RF field by switching a load

Copyright (c) Integri 2006 Page 18

INTEGRI **Testing and Test Tools**
 <as easy as it looks>

■ ICAO Tests – e-Passport Conformity Certificate (6) – L1 to L4

– 2 Communication Protocols:

- Type A
 - Data rate from 106 up to 848 kbits/s.
 - ASK 100%
 - 1 ETU : 128 periods at 106 kbits/s
64 periods at 212 kbits/s
32 periods at 424 kbits/s
16 periods at 848 kbits/s
- Type B
 - Data rate from 106 up to 848 kbits/s
 - ASK 10%

Copyright (c) Integri 2006 Page 19

INTEGRI **Testing and Test Tools**
 <as easy as it looks>

■ ICAO Tests – e-Passport Conformity Certificate (8) – L1 To L4

– Main L1 & L2 PCD/PICC Problems

- Insufficient Operating Volume
 - Bandwidth of the antenna
 - Field strength
 - Load modulation reception (Loading effect: Electromagnetism reaction, Distance, antenna layout, Field and rise time of the modulation)
- Modulation index not respected (ASK)

– Tested via parameters variation

- PICC Resonance Frequency (resonance frequency influences strongly « loading effect »), Sweep PCD frequency from 11MHz to 24MHz with a weak field strength stimulation
- Modulation Index
- Variation of Environmental Conditions
- Variation of Field Strength
- Variation of PCD Signal Characteristics Including verification of Response Times & Framings

Copyright (c) Integri 2006 Page 20

INTEGRi **Testing and Test Tools**
 <as easy as it looks>

- ICAO Tests – e-Passport Conformity Certificate (9) – L1 To L4
 - Protocol (L3 & L4) Test Execution Automation via Software
 - Terminal is simulated by hardware device able to exchange information with contactless cards (card reader and terminal simulator).
 - Software Platform manages Tests Execution and synchronizes communication with hardware.
 - Each time a test is launched within platform, a scenario is loaded in the hardware
 - Protocol (L3 & L4) Automated Validation of execution results
 - Navigator allows to browse within traces produced by executions and sent back by hardware, giving access to:
 - Frames and bytes content,
 - Card response timings (at frame/byte/electrical transition level)
 - Electrical Events
 - Navigator accessible from scripts allowing automation of validation,
 - Navigator manually accessible within Viewer for traces, allowing manual validation (and check tool results)

→ e-Passport Level 1 Test Suite

Copyright (c) Integri 2006 Page 21

INTEGRi **Testing and Test Tools**
 <as easy as it looks>

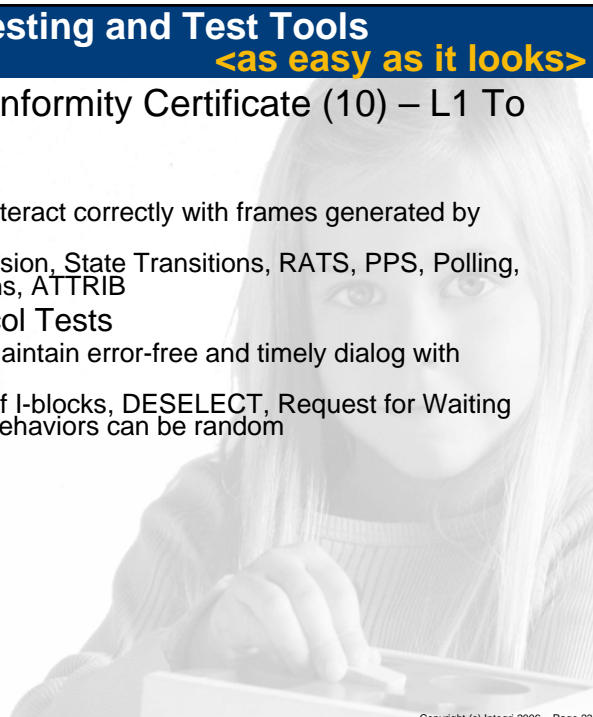
- ICAO Tests – e-Passport Conformity Certificate (9) – L1 To L4
 - Digital RF Framing Tests
 - Verify that ePassport is able to interact correctly with RF fields generated by compliant readers to enable exchange of information at bit, byte and frame levels.
 - Timings checked: Startup Time, Frame Delay, Time Start-Of-Frame- & End-Of-Frame-Timing, Extra Guard Time (EGT), Timing before PICC SOF

Step	Timestamp	Description	Block Type	Data
1	000.142.037.588	RF Field 1	Logic	00
2	000.227.754.440	RF Field 2	Logic	00
3	000.227.754.440	RF Field 2	Logic	00
4	000.227.754.440	RF Field 2	Logic	00
5	000.227.754.440	RF Field 2	Logic	00
6	000.227.754.440	RF Field 2	Logic	00
7	000.227.754.440	RF Field 2	Logic	00
8	000.227.754.440	RF Field 2	Logic	00
9	000.227.754.440	RF Field 2	Logic	00
10	000.227.754.440	RF Field 2	Logic	00
11	000.227.754.440	RF Field 2	Logic	00
12	000.227.754.440	RF Field 2	Logic	00
13	000.227.754.440	RF Field 2	Logic	00
14	000.227.754.440	RF Field 2	Logic	00
15	000.227.754.440	RF Field 2	Logic	00
16	000.227.754.440	RF Field 2	Logic	00
17	000.227.754.440	RF Field 2	Logic	00
18	000.227.754.440	RF Field 2	Logic	00
19	000.227.754.440	RF Field 2	Logic	00
20	000.227.754.440	RF Field 2	Logic	00
21	000.227.754.440	RF Field 2	Logic	00
22	000.227.754.440	RF Field 2	Logic	00
23	000.227.754.440	RF Field 2	Logic	00
24	000.227.754.440	RF Field 2	Logic	00
25	000.227.754.440	RF Field 2	Logic	00
26	000.227.754.440	RF Field 2	Logic	00
27	000.227.754.440	RF Field 2	Logic	00
28	000.227.754.440	RF Field 2	Logic	00
29	000.227.754.440	RF Field 2	Logic	00
30	000.227.754.440	RF Field 2	Logic	00
31	000.227.754.440	RF Field 2	Logic	00
32	000.227.754.440	RF Field 2	Logic	00
33	000.227.754.440	RF Field 2	Logic	00
34	000.227.754.440	RF Field 2	Logic	00
35	000.227.754.440	RF Field 2	Logic	00
36	000.227.754.440	RF Field 2	Logic	00
37	000.227.754.440	RF Field 2	Logic	00
38	000.227.754.440	RF Field 2	Logic	00
39	000.227.754.440	RF Field 2	Logic	00
40	000.227.754.440	RF Field 2	Logic	00
41	000.227.754.440	RF Field 2	Logic	00
42	000.227.754.440	RF Field 2	Logic	00
43	000.227.754.440	RF Field 2	Logic	00
44	000.227.754.440	RF Field 2	Logic	00
45	000.227.754.440	RF Field 2	Logic	00
46	000.227.754.440	RF Field 2	Logic	00
47	000.227.754.440	RF Field 2	Logic	00
48	000.227.754.440	RF Field 2	Logic	00
49	000.227.754.440	RF Field 2	Logic	00
50	000.227.754.440	RF Field 2	Logic	00
51	000.227.754.440	RF Field 2	Logic	00
52	000.227.754.440	RF Field 2	Logic	00
53	000.227.754.440	RF Field 2	Logic	00
54	000.227.754.440	RF Field 2	Logic	00
55	000.227.754.440	RF Field 2	Logic	00
56	000.227.754.440	RF Field 2	Logic	00
57	000.227.754.440	RF Field 2	Logic	00
58	000.227.754.440	RF Field 2	Logic	00
59	000.227.754.440	RF Field 2	Logic	00
60	000.227.754.440	RF Field 2	Logic	00
61	000.227.754.440	RF Field 2	Logic	00
62	000.227.754.440	RF Field 2	Logic	00
63	000.227.754.440	RF Field 2	Logic	00
64	000.227.754.440	RF Field 2	Logic	00
65	000.227.754.440	RF Field 2	Logic	00
66	000.227.754.440	RF Field 2	Logic	00
67	000.227.754.440	RF Field 2	Logic	00
68	000.227.754.440	RF Field 2	Logic	00
69	000.227.754.440	RF Field 2	Logic	00
70	000.227.754.440	RF Field 2	Logic	00
71	000.227.754.440	RF Field 2	Logic	00
72	000.227.754.440	RF Field 2	Logic	00
73	000.227.754.440	RF Field 2	Logic	00
74	000.227.754.440	RF Field 2	Logic	00
75	000.227.754.440	RF Field 2	Logic	00
76	000.227.754.440	RF Field 2	Logic	00
77	000.227.754.440	RF Field 2	Logic	00
78	000.227.754.440	RF Field 2	Logic	00
79	000.227.754.440	RF Field 2	Logic	00
80	000.227.754.440	RF Field 2	Logic	00
81	000.227.754.440	RF Field 2	Logic	00
82	000.227.754.440	RF Field 2	Logic	00
83	000.227.754.440	RF Field 2	Logic	00
84	000.227.754.440	RF Field 2	Logic	00
85	000.227.754.440	RF Field 2	Logic	00
86	000.227.754.440	RF Field 2	Logic	00
87	000.227.754.440	RF Field 2	Logic	00
88	000.227.754.440	RF Field 2	Logic	00
89	000.227.754.440	RF Field 2	Logic	00
90	000.227.754.440	RF Field 2	Logic	00
91	000.227.754.440	RF Field 2	Logic	00
92	000.227.754.440	RF Field 2	Logic	00
93	000.227.754.440	RF Field 2	Logic	00
94	000.227.754.440	RF Field 2	Logic	00
95	000.227.754.440	RF Field 2	Logic	00
96	000.227.754.440	RF Field 2	Logic	00
97	000.227.754.440	RF Field 2	Logic	00
98	000.227.754.440	RF Field 2	Logic	00
99	000.227.754.440	RF Field 2	Logic	00
100	000.227.754.440	RF Field 2	Logic	00

Copyright (c) Integri 2006 Page 22

INTEGRI **Testing and Test Tools**
<as easy as it looks>

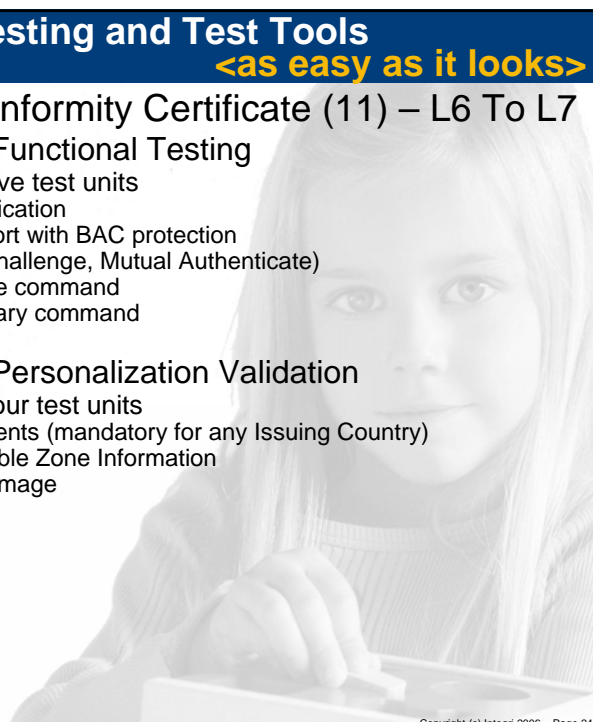
- **ICAO Tests – e-Passport Conformity Certificate (10) – L1 To L4**
 - **Digital RF Activation Tests**
 - Verify that ePassport is able to interact correctly with frames generated by compliant readers
 - Type A & B: Handling of anti-collision, State Transitions, RATS, PPS, Polling, PICC Reception, State Transitions, ATTRIB
 - **Digital RF ISO14443-4 Protocol Tests**
 - Verify that ePassport is able to maintain error-free and timely dialog with compliant readers.
 - Exchange of I-blocks, Chaining of I-blocks, DESELECT, Request for Waiting Time Extension, some of these behaviors can be random



Copyright (c) Integri 2006 Page 23

INTEGRI **Testing and Test Tools**
<as easy as it looks>

- **ICAO Tests – e-Passport Conformity Certificate (11) – L6 To L7**
 - **ICAO Application Data (L6) – Functional Testing**
 - Document structure consists of five test units
 - Selection of the ICAO LDS Application
 - File Access Control for e-passport with BAC protection
 - BAC specific commands (Get Challenge, Mutual Authenticate)
 - Implementation of the Select File command
 - Implementation of the Read Binary command
 - **ICAO Application Data (L7) – Personalization Validation**
 - Document structure consists of four test units
 - EF.COM – Common Data Elements (mandatory for any Issuing Country)
 - Data Group 1 – Machine Readable Zone Information
 - Data Group 2 – Encoded Face Image
 - EF.SOD – LDS Security Data



Copyright (c) Integri 2006 Page 24

■ ICAO Tests – e-Passport Conformity Certificate (3) – L6 To L7

– Typical Test Methods for L6 & L7

- Plain SelectFile command for data group 2 on a BAC (Basic Access Control) protected passport
- Plain ReadBinary command with SFI (Short File Identifier) on a BAC protected passport
- SelectFile command with an invalid parameter P1
- Valid ReadBinary command with SFI for EF.COM
- Version number referred by EF.COM
- Data Group 2 CBEFF Format Owner Element
- Data Group 2 CBEFF Format Type Element
- Coding of the Document Signer Certificate

→ e-Passport Level 2 Test Suite

Testing and Test Tools**e-Passports
Interoperability****■ Outline**

- Introduction
- Cross-Over Testing & Parametric Testing
- ICAO Tests – e-Passport Conformity Certificate
- **Questions**

Thank you for your attention.