



ePassport Interoperability Test Event
Berlin, Germany, May 29 – June 1, 2006

Technical Outline

(Version 1.11, Status as of 2006-05-22)

Content

Technical Outline	1
1 Introduction	2
2 Organisational framework.....	2
3 Participating parties.....	2
4 Technical outline	3
4.1 Requirements for participants	3
4.1.1 e-passport samples	3
4.1.2 e-passport reader suppliers	4
4.1.3 System integrators, components.....	4
4.2 Reference Configuration on registration	4
4.3 Cross-Over Test	4
4.4 Focus on security.....	4
4.5 Focus on RF Protocol and Application Test Standard	5
5 Publication of the results	5
6 Workshop and Conference	6
7 References	6

1 Introduction

Following the successful interoperability tests in the past, Germany will host the next interoperability test event for e-passports in Berlin, May 29 –June 1, 2006 (ePassport Interoperability Test Event).

The ePassport Interoperability Test Event will be held by the Federal Ministry of the Interior in close co-operation with the Brussels Interoperability Group (BIG) and is supported by the European Commission and ICAO's New Technology Working Group (NTWG).

Schedule and content of the ePassport Interoperability Test Event is targeted to the European Union's deadline for the introduction of e-passports within all EU Member States by August 2006. It is aimed to assist and provide technical expertise not only to EU Member States, but all nations considering next generation machine readable travel documents (e-MRTDs).

The ePassport Interoperability Test Event will consist of:

- A cross-over test of e-passport samples and readers (see requirements below)
- Testing according to the RF Protocol and Application Test Standard (e-passport conformity testing)
- A workshop session including a poster session
- Limited industry exhibition to give an overview of complete e-passport systems and components

2 Organisational framework

Date	May 29, 2006 – June 1, 2006
Location	Berlin / Germany Hotel Crown Plaza
Organiser	Federal Ministry of the Interior (BMI) Federal Office for Information Security (BSI) Federal Criminal Police Office (BKA) German Standards Body (DIN)
Supporters	European Commission Brussels Interoperability Group (BIG) ICAO New Technologies Working Group (NTWG)

3 Participating parties

The ePassport Interoperability Test Event continues the successful series of interoperability events held in Australia, the USA, Japan and Singapore. Participating parties will be:

- e-passport manufactures
- e-passport reader manufactures
- immigration authorities
- issuing authorities
- system integrators

4 Technical outline

Given the progress made in the previous interoperability events, where participants showed the general ability to comply with ICAO's e-passport standards, the ePassport Interoperability Test Event is aimed to focus on digital security features and compliance with the upcoming RF Protocol Test Technical report and ISO standard. The testing activities therefore shall no longer be based on idealised boundary conditions, but on realistic data that mirror likely conditions in the field.

4.1 Requirements for participants

Technical requirements for participating e-passport samples and readers follow the specifications outlines in [Guide].

4.1.1 e-passport samples

Each e-passport provider is required to deliver *identical* 5 samples each with a non-standard dataset. In order to ensure comparability, it is recommended that the samples within the group of 5 should be *identical* with regard to:

- EF.COM, i.e. same number of data groups on each passport present
- Name, Surname, DOB should be identical
- Data groups DG2 and – if present - DG3 should be identical
- The same security mechanisms (BAC/no BAC; AA/ no AA etc.) should be used.
- The same cryptography should be used (same hash algorithm, same signature algorithm, same key length)
- The same document signing certificate and the same country signing certificate should be used.
- The same chip type and operating system should be used.
- Identical passport serial numbers are not required.

Due to limited resources available to the organisers, two sets of 5 passport samples per participant will be tested. If time permits, more sets could be tested.

The personalisation of the samples should at least correspond to the ICAO and EU minimum requirements: EF.COM, EF.DG1, EF.DG2, EF.SOD, BAC (EU mandatory only)
Standard data sets from previous interoperability tests (Silver data set, Tsukuba data set, Orchid data set etc) are not permitted.

Only passport books (ID-3 size) or ID-3 size cards are allowed to participate.
Each sample is required to have an optically personalised data page, at least having a MRZ.
Samples should be personalised having at least EF.COM, EF.SOD, EF.DG1, EF.DG2.
All data shall be properly signed.

Passport manufacturers are required to submit the Document Signing Certificate (if not on the chip itself) and the Country Signing Certificate C_{CSCA} together with their samples to the organisers in order to allow the validation of the full certificate chain. These certificates will be provided through the Test Event website (www.interoptest-berlin.de) in due time or via LAN/WLAN or by data storage media (CD, USB memory stick etc.) during the test event.

4.1.2 e-passport reader suppliers

All readers shall be able to read the MRZ optically (RF readers with attached swipe readers or full page readers with integrated RF and MRZ reader).

It is highly recommended that readers and software should be able to validate the certificate chain up to C_{CSCA} as required by the ICAO Passive Authentication scheme.

Readers and software should be able incorporate other countries C_{CSCA}'s in order to validate the certificate chain up to C_{CSCA}. These certificates will be provided through the Test Events website via LAN/WLAN.

All readers must support both ISO 14443 type A and type B chips.

4.1.3 System integrators, components

The focus of the ePassport Interoperability Test Event is on passport books and ID3-sized cards.

For the Cross-Over test and the official RF Standard Test, only officially registered samples are permitted.

If time and space permit, components such as inlays, ID1-sized cards etc. can be tested during the event in the cross-over setup on a bilateral basis. These results will not be included in the official reporting.

Within the exhibition, participants are free to set up and run test equipment for both passport books and components.

4.2 Reference Configuration on registration

Following the specifications outlines in [Guide], on registration, each e-passport will be checked and registered using the reference configuration:

Rochford Thompson RTE 6701 Swipe MRZ reader

Golden Reader Tool version 2.7.x

4.3 Cross-Over Test

All registered e-passport samples will be tested vs. all registered e-passport readers. Results will be captured manually by testers and subsequently evaluated:

Read times will be recorded at 0 cm reading distance only.

Along with the read times, the data groups read will be recorded and subsequently compared with data groups present on the chip.

Read times will be most likely reported as rates, i.e. transmitted data per time.

Reported read times (or rates) will be separated by BAC, AA, Chip Authentication (CA), swipe/full page reader etc. in order to compare similar groups of equipment.

In order to obtain highly comparable results, each e-passport will additionally be checked by the Essen Group reference configuration using:

Various RF readers (e.g. Pegoda for Type A and NMDA for Type B)

Rochford Thompson RTE 6701 Swipe MRZ reader

Golden Reader Tool version 2.7.x

4.4 Focus on security

Beyond functional testing, the ePassport Interoperability Test Event will focus on ICAO's mandatory Passive Authentication mechanism as it is outlined in [PKI].

It is strongly recommended that reader manufacturers authenticate the data on the e-passport by validating the complete certificate chain up to C_{CSCA} and to display the result of this operation.

Participants are required to provide their Document Signing Certificates (if not stored on the chip itself) and Country Signing Certificates (C_{CSCA}) to the Organizers.

Alternatively, they can use a test document signing certificate and the corresponding test Country Signing Certificate to sign the data on their samples. The certificates might be generated for the sole purpose of the ePassport Interoperability Test Event.

For the test, these certificates will be provided via the Test Event website (www.interoptest-berlin.de) in due time or via LAN/WLAN or by data storage media (CD, USB memory stick etc.) during the test event.

4.5 Focus on RF Protocol and Application Test Standard

Just in time for the EU's deadline on the issuance of e-passports, the ePassport Interoperability Test Event will provide the unique opportunity of in-depth testing against the upcoming ISO RF Protocol Testing Standard [TR_RF2, TR_RF3] and will go beyond Cross-Over testing of readers vs. passport samples.

Issuing nations will be given the possibility to thoroughly test their samples by using the Draft RF Protocol and Application Test Standard. By doing so, they can identify possible weaknesses and deviations from the ICAO recommendations and ISO standards. This part of the test will run independently and parallel to the regular cross-over test.

Participants will receive a detailed test report of their samples performance. These results are not to be published.

The results of the ePassport Interoperability Test Event are fed back to the Draft International Standard and will provide real-world input for the ongoing finalisation. Selected test cases will cover layers 1-4 [ISO 14443, TR_RF2] as well as 6-7 [ISO7816, LDS, PKI, TR_RF3].

5 Publication of the results

Following a request from ICAO/NTWG, all participants (passport suppliers and reader manufacturers) are asked to agree to a full publication of results achieved in the Cross-Over-Test. This will include:

- company name,
- product name if available
- High level product details (swipe/full page reader, chip type, BAC/no BAC, AA / no AA, etc.)
- Selected results.

Results published will be divided into comparable subsets.

The results achieved in the e-passport conformity testing will not be made public. A detailed report will be given to the manufacturer/issuer only. Anonymous results might be published to

give a general overview of the State of the art and highlight problematic issues within the standard.

6 Workshop and Conference

Workshop and conference details and programme will follow.

7 References

All references listed below are provided on this website under "[Further technical information](#)".

- [LDS] ICAO NTWG, Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Technical Report, Revision 1.7, 18 May 2004, www.icao.int/mrtd
- [PKI] ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Technical Report, Version 1.1, 1 October 2004, www.icao.int/mrtd
- [Guide] Guide to Interfacing e-MRTDs and Inspection Systems
Version – 1.0, February 14, 2005
- [TR_RF2] RF protocol and application test standard for e-passport - Part 2: Tests for air interface, initialisation, anticollision and transport protocol
- [TR_RF3] RF protocol and application test standard for e-passport - Part 3: Tests for application protocol and logical data structure