Standards for Business

ETSI White Paper No. 7

Testing ePassport Readers using TTCN-3

Authors:

Jean-Marc Chareau (Joint Research Centre of the European Commission)
Laurent Velez (ETSI)
Zdenek Riha (Masaryk University)

November 2011

European Telecommunications Standards Institute
F-06921 Sophia Antipolis Cedex, France
Tel +33 4 92 94 42 00 Fax +33 4 93 65 47 16
info@etsi.org www.etsi.org

About the authors

Jean-Marc Chareau

Joint Research Centre of the European Commission

Jean-Marc Chareau is a technical expert at the TEMPEST (Thermal, Electro-Magnetic, Physical Equipment Stress Testing) laboratory of the European Commission – Joint Research Centre (JRC).

He joined the JRC's Institute for the Protection and Security of the Citizen at Ispra in Italy in 2006 to take charge of test and measurement activities on contactless smart cards and to promote conformity and interoperability of ePassports.

He contributes to ISO/IEC subcommittee JTC1/subcommittee17 "Cards and personal identification", Working Group 8 "Integrated circuit cards without contacts".

Laurent Velez

ETSI

Laurent Velez is a technical expert at the Centre for Testing and Interoperability (CTI) at the European Telecommunications Standards Institute (ETSI).

Before joining ETSI he was an engineer at Ericsson, Siemens and Nortel, with experience of testing core networks, and data routers and switches.

He joined ETSI in 2008 and is currently developing and validating test specifications across a range of technologies. In addition to the ePassport reader testing activities, he was also involved in the FP7 WALTER project on UWB testing in cooperation with the JRC.

Zdenek Riha

Masaryk University

Zdenek Riha is a professor at the Masaryk University Faculty of Informatics in Brno, Czech Republic.

Between 2005 and 2008 he has been seconded as Detached National Expert to the European Commission's Joint Research Centre in Italy where he worked on various ePassport projects. In addition Zdenek was involved in the ePassport interoperability group known as Brussels Interoperability Group.

Contents

Testing ePassport Readers using TTCN-3

November 2011

From January 2010 to August 2011 ETSI has conducted a project, co-financed by the European Union (EU) and European Free Trade Association (EFTA), to develop a Test System Prototype for Conformance Testing of ePassport readers.

The objective of this project was to design, build and test a TTCN-3 based Test System Prototype for ePassport Reader Conformance Testing. The project team decided to use a well standardized methodology following ISO/IEC 9646 [9], providing also support to ISO/IEC 17025 [12] requirements for test laboratories.

This project was a joint effort between the EC Joint Research Centre (JRC) and ETSI.

The ETSI-standardized test language TTCN-3 has already been widely used in many testing projects across different technologies. However, to date it has not been applied in the area of contactless smart card testing. This is particularly true for e-ID and e-MRTDs (Machine Readable Travel Documents) such as ePassports.

This White Paper provides an overview of the approach taken in the project, demonstrating the expertise which ETSI can bring to such a task, and presents a summary of the experience gained from this novel application of TTCN-3.

Introduction to ePassport

Biometric identification is the automated means of recognising a living person through the measurement of distinguishing physiological and behavioural traits. Fingerprint systems are the most widely used biometric identification systems. Face, iris, hand geometry, voice and handwriting recognition are among the other most common biometric techniques.

An Electronic Passport is similar to a regular passport with the addition of a small embedded contactless chip which stores information about the holder and the issuing institution.

The chip securely stores information in 16 data groups, in the form of a facial photograph, fingerprint image and/or template and iris image. Within the European Union it was decided to use the facial image and fingerprint images only. This combination of biometric techniques aims to create an unrivalled level of security and protection against fraudulent identification papers.

Biometrically enhanced, the identification used in an e-MRTD (Electronic Machine Readable Travel Document) like the ePassport, is an efficient way to improve security, both at national and European level.

However, the deployment of biometric identification systems is a real challenge as it involves a collaborative effort by many participants, both regulatory bodies and industry.

The ePassport, its reader and the associated inspection system have been specified and designed to operate correctly across a wide variety of infrastructure worldwide. With such a widespread deployment, interoperability becomes a global challenge. This project demonstrates that testing according to defined standards will enable interoperability and can help ensure successful global deployment of this technology.

Providing application-specific testing and compliance scenarios for biometric security applications is essential to allow the EU to keep its leadership in present and future biometric technology.

Standardization of ePassport

The International Civil Aviation Organization (ICAO) is a United Nations agency responsible for civil aviation and international travel. It also works on standardization in the area of passports and travel documents.

Already in the 1980s the storage of some passport data in two machine processable lines of text has been standardized. These lines, called the Machine Readable Zone (MRZ), contain basic data about the passport and its holder (name, surname, date of birth, date of expiry etc.). This data is printed in a standardized font so that it is machine readable and processable. Because the amount of data which can be stored in the MRZ is only very small (88 characters) and the only security factor are check digits, new ways of storing data for automated processing were investigated.

The 6th version of the ICAO Doc 9303 [8], describing travel documents, introduces the technology of contactless chips, symmetric and asymmetric

cryptography and biometrics. New passports equipped with a contactless chip are called electronic passports or ePassports.

Legislation

The characteristics of the new European Union electronic passport have been initially established with the European Council Regulation (EC) No 2252/2004 [7] of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. These characteristics were then further refined in two subsequent pieces of legislation:

- The Commission Decision C(2005) 409 [3] of 28 February 2005 which defines the integration of the facial image on a secure storage medium in the passport.

- The Commission Decision C(2006) 2909 [4] of 28 June 2006 which establishes security standards to protect biometrics in passports (in particular fingerprints) against misuse.

The Joint Research Centre (JRC) of the European Commission has been charged by the Directorate General of Home Affairs within the European Commission to provide technical support & coordination to achieve ePassport interoperability across the EU.

The Institute for the Protection and Security of the Citizen (IPSC) of the JRC provides this support. The Safety Technology Assessment unit (STA) of the IPSC aims to support EU policies for the security of citizens and society in electronic communications, transactions and interactions.

This unit has been involved in previous interoperability test events for ePassports and runs an ePassport Test Laboratory.

ePassport and Inspection System

ePassport

The difference between a traditional passport and an ePassport is the presence of an embedded chip with a contactless interface (and the electronic passport logo on the front cover). The location of the contactless integrated circuit with its associated antenna in the ePassport is at the discretion of the issuing State. States should be aware of the importance of the need for the contactless IC to be protected against physical tampering and casual damage including flexing and bending. (see Figure 1). The chip is a contactless smart card compliant to the ISO 14443 [11] standard (both variants – A and B – are allowed). Technology based on ISO 14443 is designed to communicate over distance of 0-10 cm and supports also relatively complex cryptographic chips and a permanent memory of kilobytes or megabytes.

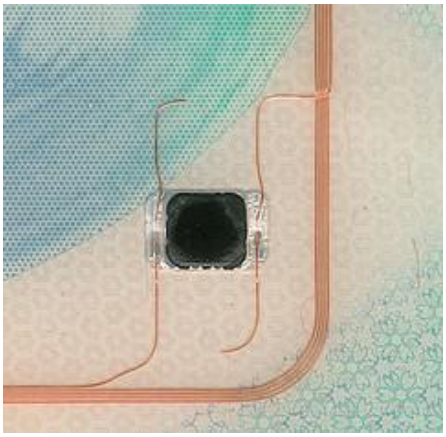


Figure 1: Directly visible contactless chip and antenna in UK passports

The chips are passive, i.e. they carry no source of power, but instead derive power indirectly from the reader signal.

Extended Access Control and Biometrics

So-called second generation electronic passports store fingerprints as images in the WSQ format (lossy compression optimized for images of fingerprints). As fingerprints are considered to be more sensitive data than facial images (their recognition capabilities are much better), access to the DG3 file is protected by an additional mechanism. This mechanism is called the Extended Access Control (EAC). In the EU the Extended Access Control is based on asymmetric cryptography and PKI as defined in the Technical Guideline TR-03110 1.11: "Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC)" [2] published by the German Bundesamt für Sicherheit in der Informationstechnik or Federal Office for Information Security (BSI).

The European EAC consists of two protocols: Chip authentication and terminal authentication. The aim of the chip authentication is to verify authenticity of the passport chip and replace low-entropy session keys for Secure Messaging with new session keys with high entropy to cope with the problem of communication eavesdropping. The role of the terminal authentication is to control access to sensitive biometric data (fingerprints, possibly also iris images).

Inspection system

An Inspection system is a hardware and software system used to inspect electronic MRTDs by any public or private entity having the need to validate the electronic MRTD, and using this document for identity verification, e.g. border control authorities, airlines or other transport operators.

Interoperability

Passports were amended with an electronic part to increase security and to improve the level of identity verification. Passports must be usable at any border crossing point worldwide. Currently not all the border control points are equipped to read electronic passports, but when reading the electronic part, verification should not be impeded by interoperability issues. As the ePassport is seen as a tool to improve security, simple declarations of conformity are not sufficient. Full interoperability is required between European countries regarding ePassports, the Inspection Systems and the test tools used, in order to meet the high expectations of improved traveller identification.

One of the definitions of interoperability is the ability of products, systems, or business processes to work together to accomplish a common task. Global interoperability can be defined in a technical way or in a broad way, taking into account social, political and organizational aspects. It is seen typically and especially in the security domain as an additional element to conformity.

The current level of interoperability in the field of electronic passports is good, even if there is still room for improvement. The initial focus has been on the ePassports themselves. Now the effort should be focused on the Inspection Systems used.

To improve interoperability the following steps were foreseen by the ETSI project:

- Production of sample test cases according to the BSI TR-03105 Part 5.1: Test plan for ICAO compliant Inspection Systems with EAC [1], written in the standardized test specification language TTCN-3;

- Implementation of the complete test system prototype.

The need for Conformance testing of ePassport Readers

European Mandate

In the 2009 European Commission ICT standardization work programme, the European Standardization Organizations (ESOs) were invited to identify standards specifying interoperability tests for biometric identification products like ePassport and ePassport readers, and to initiate any further European activity that might be needed in relation to the testing and validation of biometric identification products.

It is also worth noting that the Council Regulation (EC) No 2252/2004 [7] requires that “passports and travel documents issued by Member States shall comply with the minimum security standards...”.

The JRC has already been very active in interoperability testing of electronic passports, playing a prominent role in the organization and execution of interoperability test events with relevant players in the field (industry, Member States representatives, etc.) and acting as an independent source of technical and scientific expertise in the field.

ETSI has worked closely with JRC’s IPSC at Ispra in charge of ePassport conformance testing to address the issue of conformity of ePassports and readers to support biometric passport implementation.

The European Commission has also prepared the technical specification for electronic residence permits for third country nationals. This specification follows a similar line to electronic passports, and the same reader infrastructure will be used in future for both types of travel documents.

Standardization, conformance and interoperability

A passport must be usable at any border in the world and, in order to benefit from the new security features introduced in the electronic component, ePassports and readers at border inspection system must be able to communicate with each other. In fact, the inspection system must be able to read the data from the ePassport and it must also be able to verify and interpret the data.

Worldwide Interoperability of electronic passports is a process which starts typically with the specification of standards and continues with testing. Testing is divided usually into conformance tests and field interoperability tests.

Conformance testing in the case of ePassport verifies the conformity of the electronic passport and its reader to the ICAO Doc 9303 [8] and other referenced standards. Conformance testing is comprised of hundreds of test cases on almost all OSI layers of communication. Conformance test cases verify that the behaviour of the system under test is according to the standard, and help identify interoperability issues which can potentially lead to security issues.

Strength of conformance testing

Conformance testing concentrates on specific components in a system, often related to a single standard (or set of related standards). It is *unit* testing rather than system testing. Conformance testing is applied over open interfaces and checks for conformance to the requirements of a base specification (standard). Conformance tests are executed under controlled conditions using a dedicated test system.

One of the strong points of conformance testing is that the tester has a very high degree of control and observation. This means, for example, that he can explicitly test error behaviour by provoking abnormal scenarios. In this sense, a good conformance test suite will include aspects of robustness, something which interoperability testing cannot (explicitly) do. Conformance testing gives a high-level of confidence that key components of a device or system are working as they were specified and designed to do.

Using TTCN-3 in Conformance Testing

The objective of the project was to design, build and test a prototype TTCN-3 Test System for ePassport Reader Conformance Testing. The project aimed to use a standardized methodology following ISO/IEC 9646 [9], providing also a full support to ISO/IEC 17025 [12] requirements for test laboratories.

The Test system prototype implemented a selection of 50 testcases from the BSI TR-03105 Part 5 [1] test specification. The project experts have identified them as the most relevant testcases for the most efficient coverage of the full specification.

Introduction

ETSI test specifications are usually developed for a single base protocol standard or for a coherent set of standards. As such, it is possible to follow the methodology specified for conformance test development in ISO/IEC 9646-1 [10] without much difficulty. However, the requirements of ePassport and its reader are described across a wide range of documents and an adaptation of the ISO/IEC 9646 [9] approach was necessary. Also, for readability, consistency and to ease reusability of TTCN-3 code it was necessary to apply some guidelines on the use of TTCN-3.

About TTCN-3

TTCN-3 (Testing and Test Control Notation Version 3) is an internationally standardized programming language that has been specifically designed for use in specifying and controlling testing scenarios. TTCN-3 has been developed and is maintained by the Methods for Testing and Specification Technical Committee (TC-MTS) at ETSI. This group is composed of leading testing experts from industry and academia as well as members of ETSI's own Centre for Testing & Interoperability (CTI). TTCN-3 testing technology has been applied widely and successfully in industry for more than a decade.

The TTCN-3 Framework

The TTCN-3 Framework comprises:

- A documentation structure:
  - Test Suite Structure (TSS);
  - Test Purposes (TP);
- Abstract Test Suite (ATS):
  - Test Cases (TC) in TTCN-3 for conformance tests;
- A library of TTCN-3 building blocks:
  - data types and values;
  - templates;

  - general computational functions;
  - TP functions;
- A methodology linking the individual documentation, library and ATS elements together:
  - style guidelines and examples;
  - naming conventions;
  - guidelines on the use and extension of the TTCN-3 library;
  - a structured notation for TPs.

The TTCN-3 Framework used in this case, particularly the methodology, draws heavily on the tried and tested ISO/IEC 9646-1 [10] but modifies it to suit the particular case of ePassport Reader.

Conformance testing methodology

Conformance test specifications are produced following the methodology described in ISO/IEC 9646-1.The methodology begins with the collection and categorization of the requirements to be tested.

A Test Purpose (TP) should then be written for each identified test and this should make it clear what is to be tested but not how this should be done. Finally, a detailed Test Case (TC) is written for each TP. In the interests of test automation, TCs are usually combined into an Abstract Test Suite (ATS) using a specific testing language such as TTCN-3.

Developing ePassport test specifications

Test Suite Structure

The Test Suite should be structured according to natural divisions in the base specification(s) and should follow the functionalities specified. The architecture of the testing configuration should also be taken into account.

In the case of ePassport, the test suite is structured as a tree. The first level, the root, identifies the ePassport Inspection System. The second level separates the root into two groups, each one representing a protocol layer, application protocol (Layer 6), and logical data structure (Layer 7). The third levels are the sub-functional areas defined in sub-groups.

Test Purposes

A Test Purpose (TP) is written for each potential test of an ePassport Reader requirement, remembering that a requirement may need more than one TP to ensure that it is fully tested. As well as describing what is to be tested, the TP should identify the initial conditions to be established before testing can take place, the required status of the Implementation Under Test (IUT) from which testing can proceed and the criteria upon which test case verdicts can be assigned.

The contents of a TP should be limited to a description of what is to be tested rather than how that testing is to be carried out.

Using the Test Purpose Language

There is considerable benefit to be gained by having all Test Purposes written in a similar and consistent way. With this in mind, a simple, structured notation named TPLan, has been developed for the expression of TPs. For details, see ETSI ES 202 553 [6].

The benefits of using TPLan are:

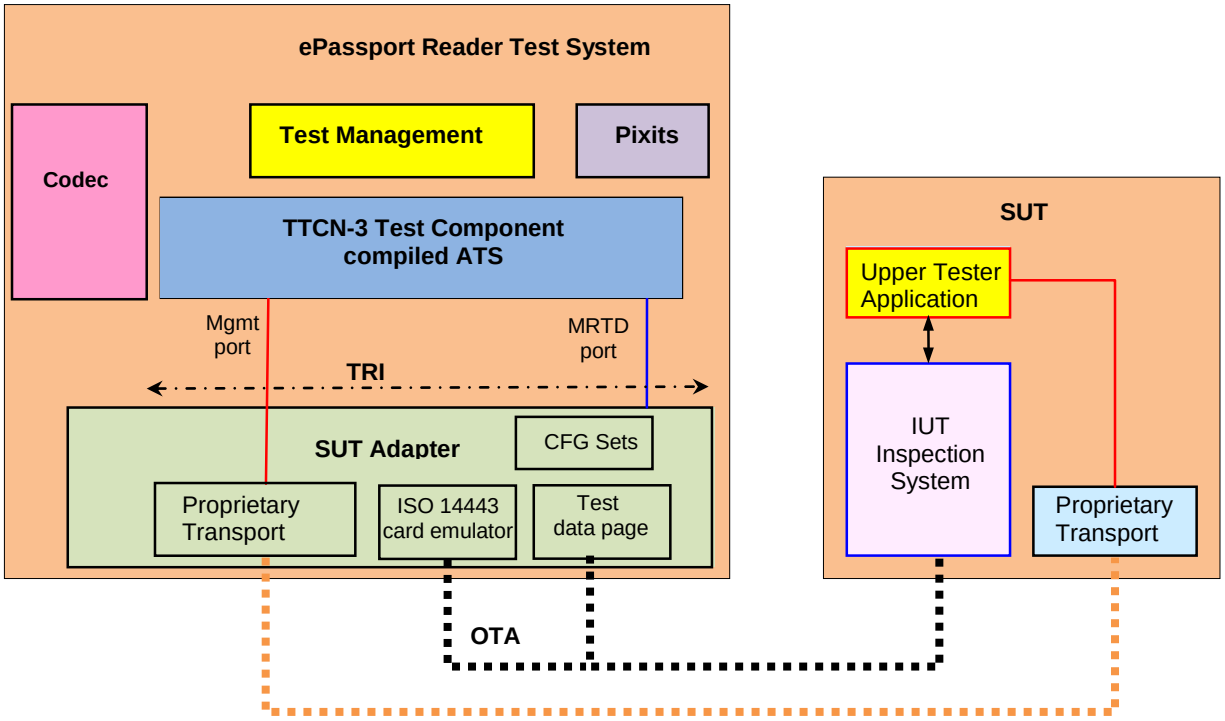
- consistency in test purpose descriptions - less room for misinterpretation;
- simpler identification of preamble, test description and postamble;
- automatic test purpose syntax checking;
- a basis for a TP transfer format;
- possible TTCN-3 code stub generation;
- possibility to graphically or textually render TP descriptions for different users.

Source code Documentation

As part of the TTCN-3 framework, the source code documentation is produced automatically from the TTCN-3 Core Language, e.g. in the form of

hypertext web pages. The tool such as T3DOC can be used, according to the methodology defined in ETSI ES 201 873-10 V4.3.1 [5].

Architecture



PIXIT: Provides means to change values of variables during run time. It is used to configure the ATS.

Test Management: Test execution, Result Analysis and Logging. The ePassport Test Management software is used to control the SUT, to drive tests and to get test verdict/result/report

TTCN-3 Test Component: Simulates ePassport behaviour; sends and receives APDU and analyses the received APDUs for conformance.

Implements in TTCN-3 control of the Upper Tester Application. The Upper Tester Application is used to

- Trigger the test procedure. In case of unavailability of such an interface, the human tester is prompted with screen messages;
- Read the Failure Interface. This information is used to determine the Test Verdict.

Codec: TTCN-3 defines protocol messages in terms of an abstract syntax. In a real test system when sending messages this abstract format needs to be converted to the actual messages (ultimately bit strings). Conversely, when receiving incoming messages as bit strings these need to be converted to the format (data types) understood by TTCN-3. The software package that does this processing is called the Codec.

In the specific case of the ePassport Reader Test system, the Codec handles the encryption/decryption module of the messages.

TRI: Communication between TTCN-3 and the Lower Tester. Communication goes via the Codec**.** Different Codecs can be activated at the same time.

ePassport adaptation layers software. In order to execute the case study, adaptation layers interfacing the TTCN-3 test drivers (system) to the underlying System Under Test (SUT) needs to be implemented.

Proprietary Transport: Communication between the Upper Tester Control of the TTCN-3 Test System and the Upper Tester Application in the SUT.

ISO14443 [11] Card Emulator and Test Data Page: Hardware for Over the Air communication controlled by Test Adapter.

Config Sets: Data Files (configuration) containing MRTD settings

Specific challenges in the implementation of the prototype

The implementation of TTCN-3 and the development of the Test System has been challenging on many aspects.

For ETSI, it was the first use of TTCN-3 to test e-MRTD/e-ID systems and more generally in the smartcard domain.

The Codec design was more complex than with previous implementations, because it handled the encryption and decryption of the messages.

Master/Slave mode: The TTCN-3 test system is not leading the test execution as is often the case in other implementations. The message flow is always driven by the Inspection System under test. The test system, which emulates a passport, needs to deal with any possible situation and must be able to answer any request message from the Inspection System. That has considerably increased the complexity of the test suite.

Validation campaigns

In total, 4 validation campaigns were needed to completely validate the prototype and to reach the targeted level of confidence required by the project.

The validation was performed at ETSI and in the JRC lab Biometric lab (TEMPEST) where the project team had the possibility to validate the prototype against a large set of ePassport Inspection systems.

The main outcome that the prototype demonstrated is that there are still improvements needed for Inspection system vendors to reach the required global interoperability of ePassport readers.

Conclusion

The main conclusion drawn from this implementation of a TTCN-3 based framework to test ePassport readers, is that the use of TTCN-3 matches the needs and requirements of conformance testing of e-MRTD or other e-ID systems.

This project has adapted solid and proven tools developed over 20 years at ETSI to address the challenges of ePassport reader interoperability requirements.

The purpose was to demonstrate the feasibility of using such formal techniques which would improve the quality and repeatability of tests, reduce room for interpretation and provide a cost-efficient approach to develop test solutions.

The project has been a fruitful collaboration between ETSI and the EC JRC and has strengthened the relationship between these two organizations.

Abbreviations

APDU	Application Protocol Data Unit
ATS	Abstract Test Suite
BAC	Basic Access Control
BSI	Bundesamt für Sicherheit in der Informationsverarbeitung
CTI	Centre for Testing and Interoperability
EAC	Extended Access Control
EC	European Commission
EFTA	European Free Trade Association
ESO	European Standardization Organization
ETSI	European Telecommunications Standards Institute
EU	European Union
FP7	Framework Programme 7
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
ID	Identification
IEC	International Electrotechnical Commission
IPSC	Institute for the Protection and Security of the Citizen
ISO	International Organization for Standardization
IUT	Implementation under test
JRC	Joint Research Centre
JTC	Joint Technical Committee
MRTD	Machine Readable Travel Documents
MRZ	Machine Readable Zone
OSI	Open Systems Interconnection
OTA	Over The Air
PIXIT	Protocol Implementation eXtra Information for Testing
PKI	Public Key Infrastructure
STA	Safety Technology Assessment unit
STF	Specialist Task Force
SUT	System Under Test
TC	Test Case
TC-MTS	Technical Committee for Methods for Testing and Specification

TEMPEST	Thermal, Electro-Magnetic, Physical Equipment Stress Testing
TP	Test Purpose
TRI	TTCN-3 Runtime Interface
TSS	Test Suite Structure
TTCN-3	Testing and Test Control Notation Version 3
UWB	Ultra-Wide Band
WSQ	Wavelet Scalar Quantization

References

[1] **BSI TR-03105 Part 5.1:** Test plan for ICAO compliant Inspection Systems with EAC (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03105/TR-03105_Part5.1_V1.2_pdf.pdf?__blob=publicationFile)

[2] **BSI TR-03110:** Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/TR-03110_v111_pdf.pdf?__blob=publicationFile)

[3] **Commission Decision C(2005) 409:** establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States

[4] **Commission Decision C(2006) 2909:** establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States

[5] **ETSI ES 201 873-10:** Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; Part 10: TTCN-3 Documentation Comment Specification

[6] **ETSI ES 202 553:** Methods for Testing and Specification (MTS); TPLan: A notation for expressing Test Purposes

[7] **European Council Regulation (EC) No 2252/2004:** on standards for security features and biometrics in passports and travel documents issued by Member States (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:EN:PDF)

[8] **ICAO Doc 9303:** Machine Readable Travel Documents (http://www2.icao.int/en/MRTD/Pages/Document9303.aspx)

[9] **ISO/IEC 9646:** Information technology; Open Systems Interconnection; Conformance testing methodology and framework

[10] **ISO/IEC 9646-1:** Information technology; Open Systems Interconnection; Conformance testing methodology and framework, Part 1: General concepts

[11] **ISO/IEC 14443:** Identification cards; Contactless integrated circuit cards; Proximity cards

[12] **ISO/IEC 17025:** General requirements for the competence of testing and calibration laboratories