Bundesamt
für Sicherheit in der
Informationstechnik

BSI TR-03105 Part 1.1

A framework for Official Electronic ID Document conformity tests

Version 1.04.1
14.11.2008

CONTENTS

1 Introduction

The process of issuing ePassports and Official Electronic ID Documents according to the ICAO standard and the BSI TRs involves several industrial companies as well as governmental organizations. Since the used RFID technology is evolving rapidly; it is important to establish a standard mechanism to ensure the conformity of the involved components.

This document defines a framework which describes standard procedures for conformity tests of Official Electronic ID Document components. Standard test configuration and protocol formats are specified, so that test scenarios for different modules can be integrated to a consistent assessment procedure. Existing test specifications can be integrated easily and scenarios for new components can be added as needed.

The exchangeable protocol format provides comparable results of different test facilities. The test procedures are arranged in the hierarchical and layered structure so that the performed tests can be composed as needed.

2 Definitions and References

2.1 Definitions

For the purpose of this document, the following definitions shall apply.

- **SCIC**
  Secure Contactless Integrated Circuit

- **PCD**
  Proximity Coupling Device

2.2 References

[1] **LDS,** ICAO Technical Report - Development of a Logical Data Structure - LDS 1.7

[2] **PKI**, PKI for Machine Readable Travel Documents offering ICC Read-Only Access 1.1

[3] **ICAO Doc 9303**, Part 1 – Machine Readable Passports

[4] **ISO/IEC 7816-4:2005**, Ed. 2 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange

[5] **ISO/IEC 10373-6:2001**, Ed. 1 Identification cards -- Test methods -- Part 6: Proximity cards

[6] **ISO/IEC 14443-1:2000**, Ed. 1 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 1: Physical characteristics

[7] **ISO/IEC 14443-2:2001,** Ed. 1 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 2: Radio frequency power and signal interface

[8] **ISO/IEC 14443-3:2001**, Ed. 1 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 3: Initialization and anticollision

[9] **ISO/IEC 14443-4:2001**, Ed. 1 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 4: Transmission protocol

[10]**ISO/IEC 7498-1:1994**, Ed. 2 Information technology –Open Systems Interconnection – Basic Reference Model: The Basic Model

3 Overview

The Conformity Assessment Framework defines several basic elements used by the specialized component test specification. These elements should provide the author of such component specifications with a flexible set of rules and guidelines, so that different specification documents written by different organizations have a common base. This makes the integration of additional specifications into an established conformity assessment process possible.

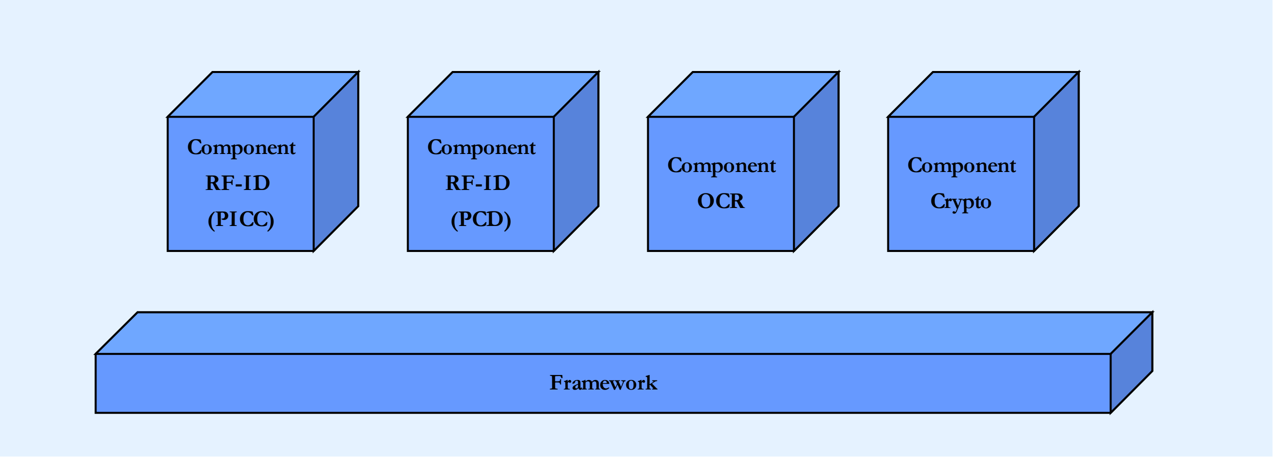

Figure 1 General structure

On top of this framework there are several component specifications each defining the conformity criteria for one element of the Official Electronic ID Document environment (Figure 1).

The framework specifies guidelines on the following topics:

- Component Structure Definition
- Documentation Scheme
- Result Rating Scheme

Within these guidelines it is referred to the layer structure of the ISO OSI-Model 2.2. Therefore in particular the lower layers 1-4 and the higher layers 6-7 are of major interest.

4 Component Structure Definition

All conformity test components should have the same structure as defined in this paragraph. This provides a common layout for all test scenarios and simplifies the integration of new tests.

The general structure of a component is shown in the following Figure 2:

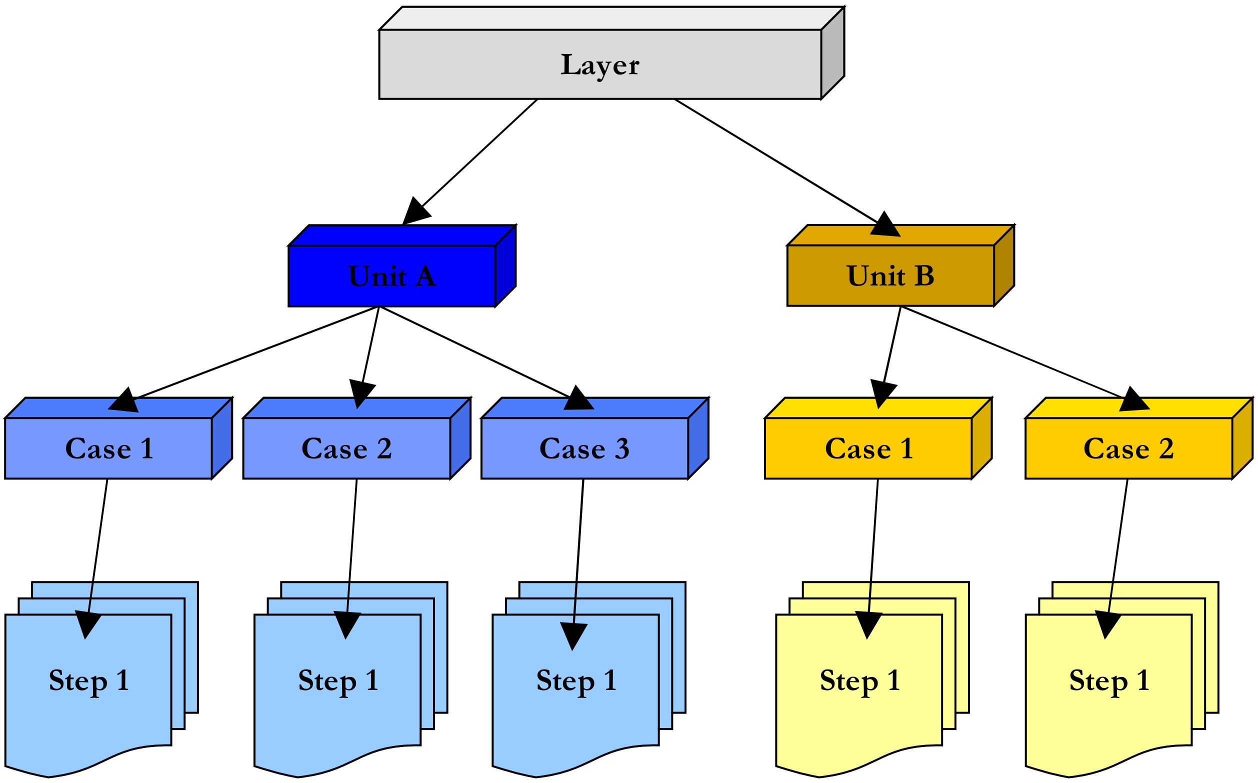

Figure 2 Component structure

This common structure is also reflected in the standard result protocol scheme as defined in paragraph 5.

In some cases it can be advantageous to apply an alternative structure that is based on already established standards and guidelines. For example in the scope of layers 1-4 it is often related to the representation in ISO/IEC 10373 2.2 and ISO/IEC 14443 2.2, 2.2, 2.2, and 2.2. Therefore the following structure is applied:

- **Test description**

  Gives a short overview about the following test scenario and describes the goals of the test.

- **Conditions**

  States which conditions have to be accomplished in order to be able to start the test.

- **Parameters**

  Specifies the different kind of parameters that are needed to start the test case.

- **Report**

  To be able to compose a report that encloses the final results of the executed test it is necessary to specify which items have to be listed.

In some cases the structure may be shorter due to the fact that not every element is mandatory (e.g. no condition is needed for a specific test).

Note: If a component can not make reference to already established documents the component structure of figure 2 should be favored.

4.1 Component

A component is the top level element of the test architecture. A component encapsulates a well-defined area of the Official Electronic ID Document environment. For every component a closer examination is needed. This is done by the respective conformity testing which is combined in an extra document. Within the conformity testing the concrete test plan is presented.

The component definition is given in a clearly arranged table that should contain the following information:

Purpose	Which elements of the Official Electronic ID Document environment are covered by this component and which are not?
Precondition	Specifies the general requirements the test facility must meet to be able to perform the tests. One facility may not be able to perform all tests of a component, in this case the test are performed on a layer base.
Importance	The importance of a component signals whether this component must be supported by the corresponding Official Electronic ID Document element. There are may be components which are optional, so that one is free to not apply to the tests defined in this component.
Layer specification	A component consists of one or more layers. Each layer covers a different level of test procedures. Even if there's only one layer, the layer definition should be kept separate from the component definition, to the able to add additional layers afterwards. Each layer may be specified in a separate document.

4.2 Layer

A layer contains tests with a similar abstraction level for a given Official Electronic ID Document element. For example a component can consist of a layer for low level tests which are closer to the actual hardware or software architecture; while other higher level tests are performed in a more logical layer.

All tests in a layer should be performed together and should result in a single protocol document.

This framework defines a template for the layer specification document. This template is based on a spreadsheet.

The layer definition contains the following information:

Layer-Id	The Layer-Id must uniquely identify the Layer inside the component.
Purpose	Specifies the abstraction level addressed by this layer.
Version	The version number of this layer specification.
References	Defines on which reference documents the specified tests are based on (ISO standards, ICAO TR, BSI TR, ...).
Profile	In the scope of ICAO specification some elements are defined as optional for the application of the ePassport. For layer 6-7 this can e.g. be EAC or BAC, for a lower level like layer 1-4 the separation of Type A and Type B is accomplished.
Preconditions	All tests in one layer should require the same set of test items. For example some low level tests require only parts of the Official Electronic ID Document element covered by this test layer.
Importance	The importance of a layer signals if this layer must be supported by the corresponding Official Electronic ID Document element to be compliant. There are may be layers which are optional, so that one is free to not apply to the tests defined in this layer.
Human Resources	Specifies the required skill level of the test operating staff.

Hardware Resources	Contains the specification of the needed hardware, tools etc. May refer to external specification documents.
Software Resources	Contains the specification of the needed software tools. May refer to external specification documents.
Response Status Bytes Categories	In some cases it is necessary to specify the status bytes that are returned by the SCIC in more detail than it is done by ICAO specification. This can be done within the response status bytes categories.
Unit Specification	A layer consists of one or more units. A unit covers an individual topic inside the layer. Even if there's only one unit, the unit definition should be kept separate from the layer definition, to the able to add additional units afterwards.

4.3 Unit

A unit covers an individual topic inside a layer. All tests in a unit are related to the same Official Electronic ID Document element context.

A unit definition contains the following information:

Unit-Id	The Unit-Id must uniquely identify the unit inside the layer.
Purpose	Defines the topic covered by this unit.
Version	The version number of this unit specification.
Precondition	Unit specific requirements may include the specific configuration or status settings of the test environment which must be met to be able to perform the tests.
Importance	The importance of a unit signals if this unit must be supported by the corresponding Official Electronic ID Document element to be compliant. There are may be units which are optional, so that one is free to not apply to the tests defined in this unit.
Case specification	An unit consists of one or more test cases. A case covers a single test procedure. Even if there’s only one case, the case definition must be kept separate from the unit definition, to be able to add additional test cases afterwards.

4.4 Case

A test case covers a single test procedure. Each case concentrates to a single feature in the Official Electronic ID Document environment. The result of a test case should be clearly limited in respect to the tested feature. The test cases must be executed in the order as specified in the test configuration document. If complex steps are required as preparation for this case; these steps should build their own case, because these preparations may also fail.

A case definition contains the following information:

Case-Id	The Case-Id must uniquely identify the case inside the unit.
Purpose	Defines the procedure covered by this case.
Version	The version number of the case specification.
References	(Optional:) Shows a list of referenced documents.
Profile	The ICAO specification identifies several elements as optional for the ePassport. The profiles for which the case is valid have to be specified.
Preconditions	Some test cases may require former test cases to be performed successfully in order to be executed. If these requirements are not met, the test is skipped and marked in the test protocol.
Importance	The importance of a case signals if this case must be supported by the corresponding Official Electronic ID Document element to be compliant. There are may be cases which are optional, so that one is free to not apply to the test defined in this case.
Test scenario	See paragraph 4.5

<table>
<tr>
<td><b>Expected results</b></td>
<td>For every test step the results are written to the protocol. The result analysis should have the following format: <i>”format:result specification”</i> where format could be one of the following keywords
<table>
<tr><th>Keyword</th><th>Meaning</th></tr>
<tr><td>Hex</td><td>The specified result should be written has hex value to the test protocol. For example an algorithm OID would be written as
<code>06 09 2A 86 48 86 F7 0D 01 01 01</code></td></tr>
<tr><td>Bool</td><td>The test result should be written as a Boolean value which can either be <code>true</code> or <code>false</code>.</td></tr>
<tr><td>ASCII</td><td>The result is written as a simple ASCII String.</td></tr>
</table>
Note that the result must always consist of printable character.

Every test step is connected to respective Pass/Fail criteria. This can be used in the rating step to determine whether the result matches the expected behavior. This field should contain concrete values, so that an automated matching with the result values of the test protocol is possible. For example a test with a bool result analysis specification should contain <code>true</code> or <code>false</code> as Pass/Fail criteria. If there are multiple “pass” conditions possible, this field should contain a comma separated list of all possible values.</td>
</tr>
<tr>
<td><b>Postcondition</b></td>
<td>If necessary a state description of the test object can be given after all steps have been executed.</td>
</tr>
</table>

4.5 Step

A step defines an atomic statement in the test procedure. Each step must cover a simple exactly defined operation with a concrete result that can be included in the test protocol. The steps must be performed in the order of definition in the test configuration. If one step fails the remaining steps may have to be skipped; this must also be marked in the test protocol.

The following table has to be integrated into the test scenario of the case definition. A step definition must include the following information:

Step-ID.	**Description**
	=> Configuration Data

- **Step-Id**
  All steps in the test case are numbered consecutively, so that the Step-Id identifies each step and the execution order in a test case.

- **Description**
  Defines the operation that has to be executed for this step.

- **Configuration data**
  Specifies input data which is required to perform this step.

5 Documentation Scheme

The Conformity Assessment Framework defines a standard documentation scheme for the information and data exchange. This scheme should be based on a XML document model. The XML structure reflects the component structure as defined in paragraph 3. In general there should be one separate document per component.

This framework defines the following sections in the scope of documentation:

- Definition
- Protocol
- Reference
- Rating
- DTD Definition

Although every section can be described in a separate document it might be reasonable to combine multiple sections in one document.

5.1 Definition

The definition document is geared to the structure in paragraph 4 and specifies the tests to be performed, as well as the corresponding input data. Some of the test cases have variable parameters which can be configured before testing is done. The definition document can be modified to test elements to exclude (optional) elements which are not part of the intended test scope.

Other tests may need certain input parameters to be used. The configuration document provides a standard way to define a test workflow, so that the test is reproducible and can be performed by different test facilities.

5.2 Protocol

This document contains the result of the performed tests. Note that only the plain data is included in this document, it does not contain any rating whether a result matches the ICAO or BSI TR standard or not. The rating is done in a separate step which is described in 6.

5.3 Reference

The reference document contains a set of valid results for each test. In the rating procedure (see 6) this reference result is matched to actual protocol which is gathered from the expected results in paragraph 4.4.

5.4 Rating

The rating document is generated by the final rating procedure (see 6). This document contains the conclusion of the tests and can be used to testify the conformity of the test object.

5.5 DTD Definition

With a XML specification it gets possible to extract and generate concrete test sequences from the test scenarios which can be used later on.

The XML document is defined by the following DTD:

```
<?xml=”1.0”?>
<!ELEMENT conformityDocument (component)>

<!ELEMENT component (purpose, precondition*, importance?, layer
                    specification+)>

<!ELEMENT layer (purpose, references, profile*, precondition*,
                importance?, humanresource*, hwresource*, swresource*,
                respstatebcat*, unit+)>
    <!ATTLIST layer layerId ID
                    version CDATA>

<!ELEMENT unit (purpose, precondition*, importance?, case+)>
    <!ATTLIST unit unitId ID
                   version CDATA>
```

```
<!ELEMENT case (purpose, references*, profile*, precondition*,
               importance?, testscenario, expresults+,
               postcondition*)>
    <!ATTLIST case caseId ID
                   Version CDATA>

<!ELEMENT testscenario  (step+)>


<!ELEMENT step (description, configuration)>
    <!ATTLIST step stepId ID>

<!ELEMENT purpose       (#CDATA)>
<!ELEMENT references    (#CDATA)>
<!ELEMENT precondition  (#CDATA)>
<!ELEMENT importance    (mandatory|optional)>
<!ELEMENT profile       (#CDATA)>
<!ELEMENT references    (#CDATA)>
<!ELEMENT expresults    (#CDATA)>
<!ELEMENT postcondition (#CDATA)>
<!ELEMENT description   (#CDATA)>
<!ELEMENT configuration (#CDATA)>
```

In some cases the creation of a XML document might not be realized e.g. for lower layers 1-4 a different structure related to ISO/IEC 10373 2.2 and ISO/IEC 14443 2.2, 2.2, 2.2, and 2.2 is applied.

6 Rating Method

Due to current changes and enhancements in the ICAO and BSI TR specifications the rating of the test protocol is separated by the results of the test suite. Therefore time consuming tests with real ePassports do not have to be repeated when ICAO or BSI TR specifications are changed. The standardized test protocol can be used again and rated against a changed result reference set.

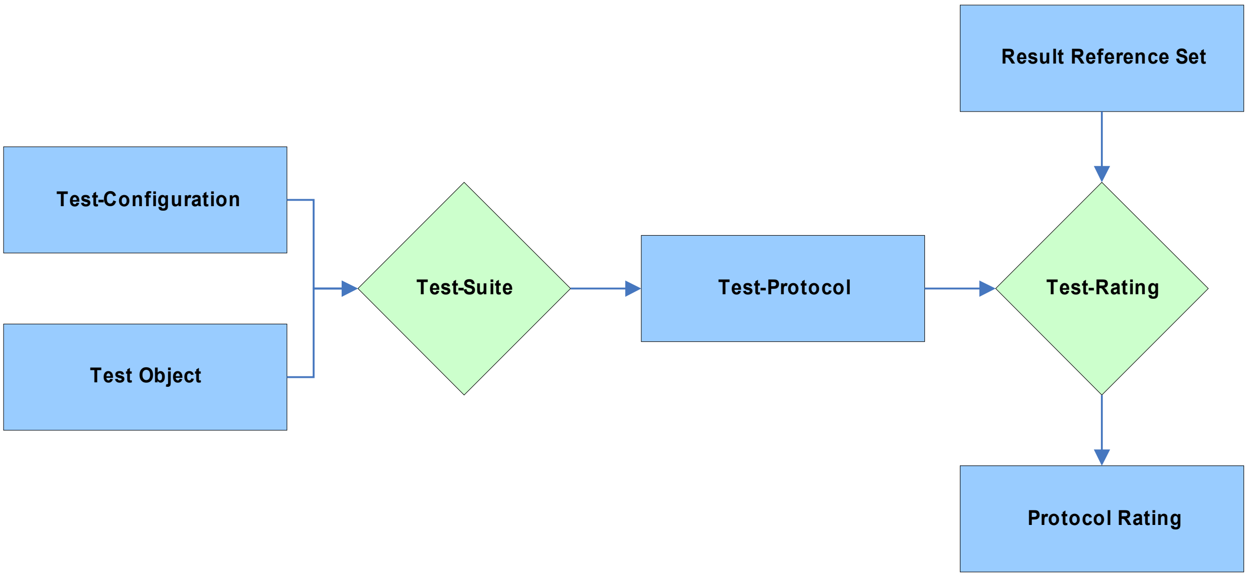

Figure 3: Test Rating

6.1 Rating Categories

Each test result is rated into three categories.

OK	Result exactly as specified.	🟩
FAILURE	Test failed.	🟥

Table 1: Rating Categories

The rating category "OK" is set, if the result of the test case is exactly as specified. There may exist several options leading to an "OK" category not just one fixed value.

The rating category "FAILURE" is set, if the result of the test case is definitely wrong. The vendor of the test object has to revise the test object.

7 Components overview

The initial version of the Conformity Assessment Framework defines four major components. Each component specifies test scenarios for a different aspect of ePassports. Although so far no further conformity testing has been described for the components OCR (paragraph 7.3) and Crypto (paragraph 7.4) it clearly shows that the structure of the framework allows to add more associated modules that are identified at a later date quite simply.

Any conformity testing document can refer to further attachments e.g. EAC. It is necessary to outline these references and relationships.

7.1 RFID (SCIC)

The RFID (SCIC) component defines tests for the transmission and storage of the electronic data stored in the ePassports chip. It covers the chip side (SCIC) with tests of the response on certain ISO command as well as test of the encoding the stored data. This component does not include tests regarding the passport reader (PCD) which are handled in the RFID (PCD) component.

7.2 RFID (PCD)

This component specifies tests regarding the RFID reading device (PCD) including physical tests of the reader’s electro magnetic field and the low level transmission protocol.

7.3 OCR

The OCR component integrates already existing test procedure for the OCR capabilities of passport reading devices. These tests include the device capabilities of detection certain passport security feature and optical recognition of the machine readable data.

7.4 Crypto

The ePassport security mechanisms as defined in the ICAO PKI report require a trustworthy implementation in client applications accessing ePassports. The passive authentication mechanism is based on RSA and elliptic curve signature algorithms as well as on hashing procedures. The secure messaging protocol used for secure transmission of data requires symmetric cryptography and HMAC algorithms.

The strength and stability of the provided implementation is tested by the crypto component based on the crypto interface specified in the ePassport API.