Technical report

Concept and Test strategy for eIDAS token conformity testing

Version 1.0 draft 1

Date: 2015/08/12

Version history

Version	Date	Editor	Description
1.0	12/08/2015	ANSSI/BSI	Initial Revision (draft)

Foreword

This technical report defines the conformity tests specification for eIDAS token. This document doesn't contain any test cases but describes how the test specification is organized. It refers to the documentation defining conformity tests cases to apply according to eIDAS application and documents profiles.

TABLE OF CONTENTS

TABLE OF FIGURES

Glossary

BAC	Basic Access Control
CA	Chip Authentication
CAN	Card Access Number
ERA	Enhanced Role Authentication
eMRTD	Electronic Machine Readable Travel Document
EAC	Extended Access Control
eID	Electronic Identification application
eSIGN	Electronic signature application
MRZ	Machine Readable Zone
PACE	Password Authenticated Connection Establishment
PIN	Personal identification number
PS	Pseudonymous Signature
RI	Restricted Identification
TA	Terminal Authentication

1. Introduction

As part of the Digital Agenda for Europe 2020, the European Commission has launched a proposal for a Regulation on electronic identification and trust services ("eIDAS").

This regulation constitutes a great opportunity to establish a uniformed European legal framework for building trust in the online environment. It is a key point to economic and social development and to carry out transactions electronically with trust and to adopt new services.

Indeed, this initiative needs to be complemented by offering the appropriated technical interoperability model. The eIDAS token specification is a contribution from the German and French IT security agencies (BSI and ANSSI) developed in collaboration with European industry partners and is aiming to be the pillar of the electronic transactions in the internal market that provides the technical interoperability.

Interoperability is achieved through the application of conformity testing. This document is a guideline to define the conformity tests to apply on eIDAS token devices.

Version v2.20 of TR-03110 series defines eIDAS token specifications. TR-03105 part 3 defines the conformity test cases ensuring the interoperability between the implementation of the protocols and applications defined in TR-03110.

eIDAS token specifications introduces new cryptographic protocols (Pseudonymous Signature, Chip Authentication Version 3), but also introduces General Authentication Procedure and Extended General Authentication Procedure with ERA. TR-03105 document shall be updated to cover these new protocols.

During General Authentication Procedure, the protocols PACE, TA, and CA are applied as preconditions to the application selection. The new version of TR-03105 part 3 designs tests methods applicable as modules unlinked to a specific application. eIDAS token specification makes use of eMRTD, eID and eSign application, but test methods modules could also be referenced by other applications as Driving license for instance.

eSign application is defined in [TR-Sign-1]. The part 2 of this technical report defines the conformity test methods for signature application.

2. Normative references

[TR03110-1] Technical Guideline TR-03110-1 v2.20 – Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDS with BAC/PACEv2 and EACv1

[TR03110-2] Technical Guideline TR-03110 v2.20 – Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2 – Protocols for electronic Identification, Authentication and trust Services (eIDAS)

[TR03110-3] Technical Guideline TR-03110 v2.20 – Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3 – Common Specifications

[TR03110-4] Technical Guideline TR-03110 v2.20 – Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 4 – Applications and document Profiles

[TR_Physical_Authentication], Technical Report Physical Authentication v1.0, 2014/12/18

[TR_Sign-1] Technical Report Signature creation and administration for eIDAS token version 1.0 2015/01/19

[TR_Sign-2] Technical Report Signature creation and administration for eIDAS token v1.0, part 2: Conformity Tests Specification[1]

[ICAO 9303] ICAO 9303, Machine Readable Travel Documents - Part 1: Machine Readable Passport, Specifications for electronically enabled passports with biometric identification capabilities (including supplement), ICAO Doc 9303, 2006

[TR-ICAO part 3] ICAO Technical Report “RF protocol and application test standard for ePassport Part 3”, Version 2.07, October 2014

[TR03105-3.1] TR-03105-3.1 v2.0 – Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3.1 – Conformity tests for eIDAS common protocols [1]

[TR03105-3.2] TR-03105-3.2 v2.0 – Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3.2 – Conformity tests for eMRTD with EACv1[1]

[TR03105-3.3] TR-03105-3.3 v2.0 – Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3.3 – Conformity tests for eID application[1]

[TR03105-3.4] TR-03105-3.3 v2.0 – Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3.4 – Conformity tests for eSign application[1]

[1] These documents are still in working draft stage and will be published in 2015.

3. eIDAS token conformity tests specification

3.1. Overview of eIDAS token conformity tests specification

eIDAS token conformity tests specification is organized around followings documents:

- [TR-ICAO Part 3] – This document provides conformity tests for eMRTD application and Inspection procedure covering PACE mechanism.
- TR-03105-3 part 3.1 – Conformity tests for eIDAS common protocols – This document provides conformity tests for eIDAS common protocols implementation covering PACE, TA1 and TA2, CA1 & CA2 & CA3.
- TR-03105-3 part 3.2 – Conformity tests for eMRTD application with EACv1 – This document provides conformity tests for EACv1 protected eMRTD Application.
- TR-03105-3 part 3.3 – Conformity tests for eID application
- [TR-Sign-2] - Conformity tests for eSign application.

The figure 2 shows the structure of the eIDAS token conformity tests specification.

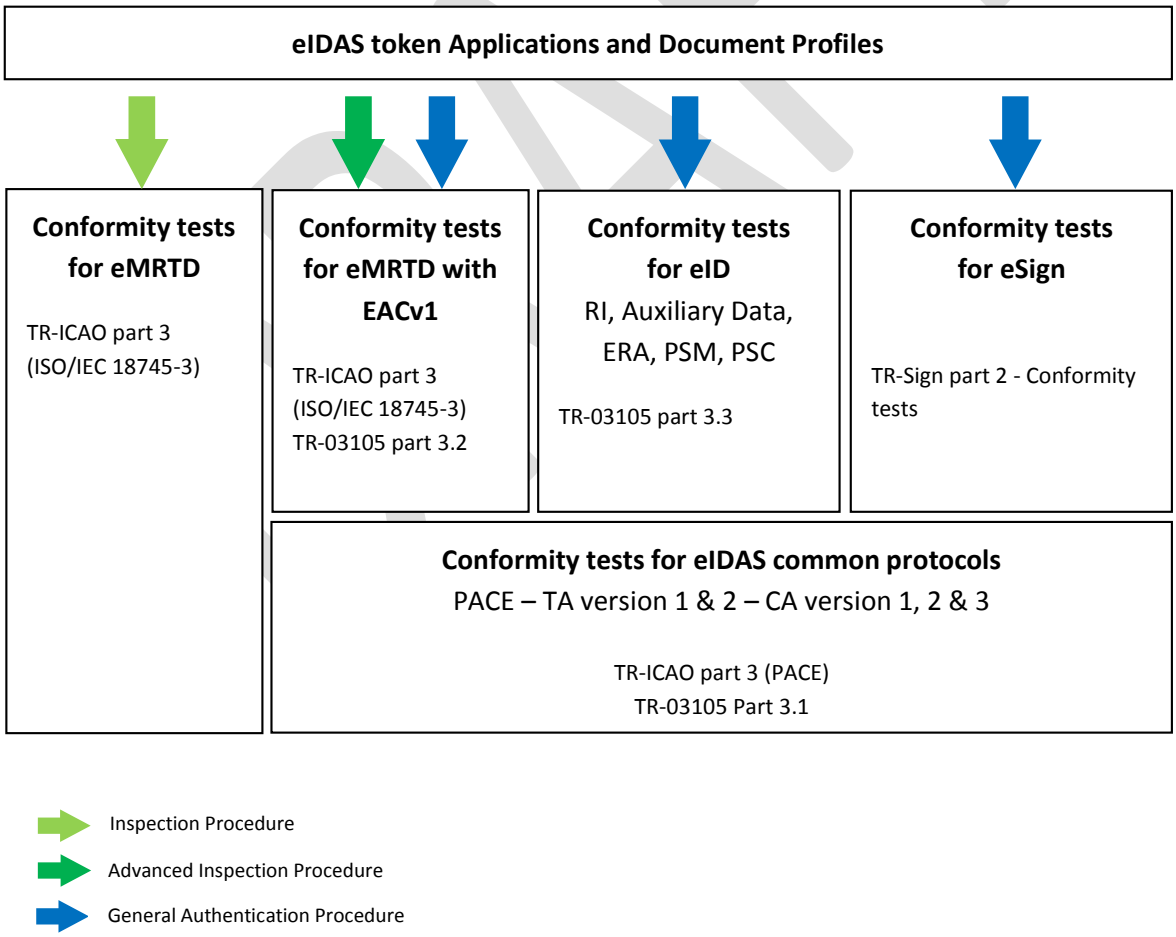

Figure 1 - Structure of the eIDAS token conformity tests specification

3.2. Inspection procedures conformity testing

To protect access to the application services, several inspection procedures are defined in the ICAO and eIDAS token specifications.

- ICAO compliant eMRTD application is accessible using **Inspection Procedure**. Since 31st of December 2014, new ePassports shall be PACE and BAC compliant. Active Authentication is optional.
  If sensitive data are present in Data Group 3 and/or Data Group 4, **Advanced Inspection Procedure** is required. This is the case for European ePassport or other EU-compliant eMRTD products. PACE, CA version 1 and TA version 1 shall be supported. BAC is also supported to be interoperable with legacy.
- Protected eMRTD application, eID and eSign are accessible using **General Authentication Procedure**. PACE, TA version 2, CA version 2 or 3 are required.

The figure 2 shows how the Inspection procedures are covered by eIDAS conformity tests specification.

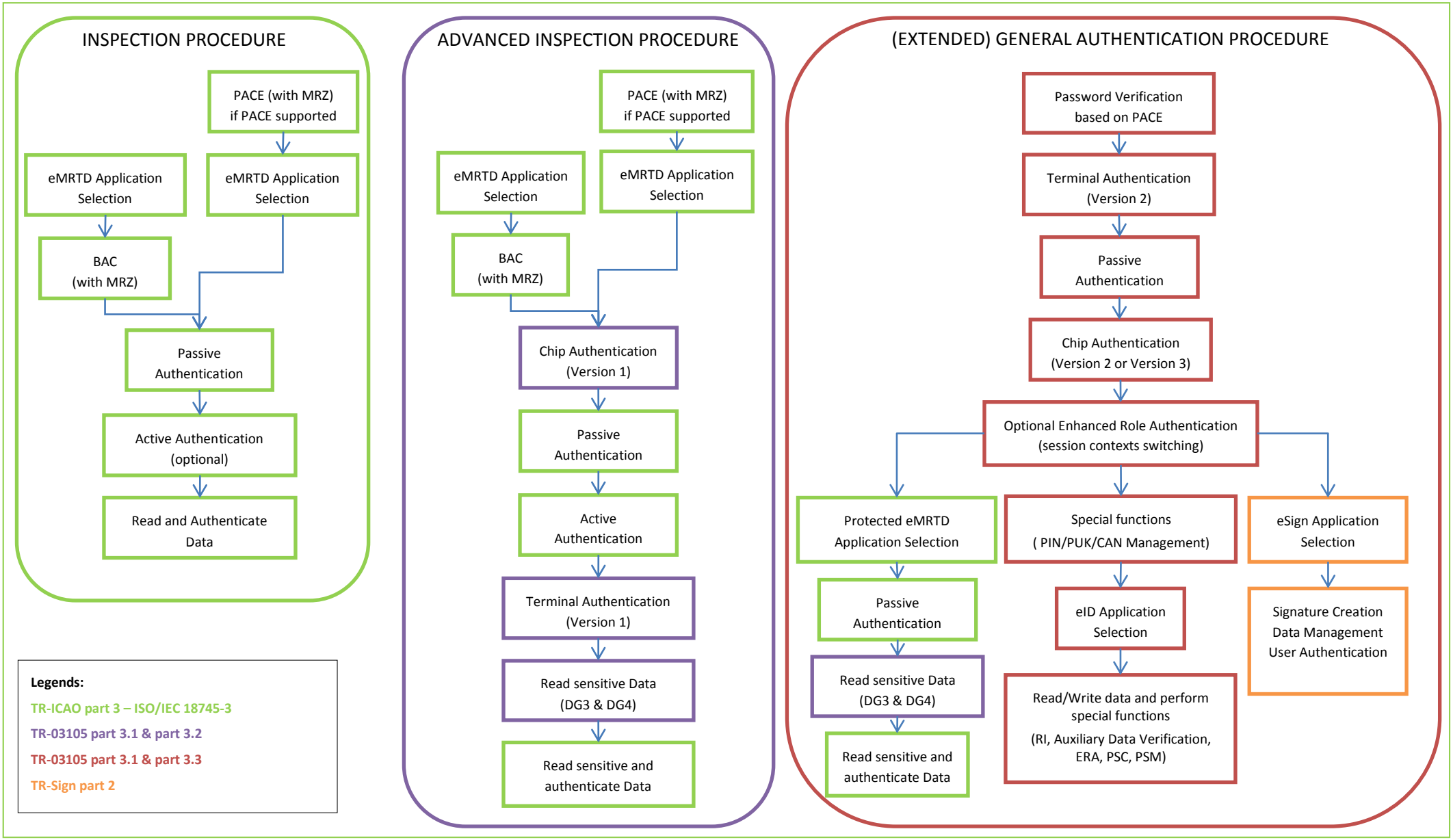
INSPECTION PROCEDURE
PACE (with MRZ) if PACE supported
eMRTD Application Selection
eMRTD Application Selection
BAC (with MRZ)
Passive Authentication
Active Authentication (optional)
Read and Authenticate Data
ADVANCED INSPECTION PROCEDURE
PACE (with MRZ) if PACE supported
eMRTD Application Selection
eMRTD Application Selection
BAC (with MRZ)
Chip Authentication (Version 1)
Passive Authentication
Active Authentication
Terminal Authentication (Version 1)
Read sensitive Data (DG3 & DG4)
Read sensitive and authenticate Data
(EXTENDED) GENERAL AUTHENTICATION PROCEDURE
Password Verification based on PACE
Terminal Authentication (Version 2)
Passive Authentication
Chip Authentication (Version 2 or Version 3)
Optional Enhanced Role Authentication (session contexts switching)
Protected eMRTD Application Selection
Passive Authentication
Read sensitive Data (DG3 & DG4)
Read sensitive and authenticate Data
Special functions (PIN/PUK/CAN Management)
eID Application Selection
Read/Write data and perform special functions (RI, Auxiliary Data Verification, ERA, PSC, PSM)
eSign Application Selection
Signature Creation Data Management User Authentication
Legends:
TR-ICAO part 3 – ISO/IEC 18745-3
TR-03105 part 3.1 & part 3.2
TR-03105 part 3.1 & part 3.3
TR-Sign part 2

Figure 2 – Inspection procedures test coverage

3.3. Test profiles definition

[TR-03110-4] specifies applications and documents profiles supported by eIDAS tokens. By supporting an application or a specific protocol, some features are mandatory and others optional. Since these elements are optional, it is not possible to define the corresponding tests as mandatory for each eIDAS token. Therefore, the Figure 4 specifies a set of profiles. Each profile covers a specific optional element. A tested eIDAS token shall be assigned to the supported profiles in the implementation conformance statement, and a test shall only be performed if the eIDAS token belongs to this profile.

Information for test setup	**Profile-ID**
eIDAS token common mechanisms:	
- Chip Authentication version 2 is supported	CA2
- Chip Authentication version 3 is supported	CA3
- Session Context switch is supported	SC_Switch
- Change PIN command is supported	CNG_PIN
- Change PIN with PUK is supported	CNG_PIN.PUK
ICAO application The ICAO profile contains the mandatory feature set for ePassport application as defined in [ICAO 9303]. Therefore, this profile and its tests are mandatory for all products which contain the ePassport application.	ICAO
- CAN is supported for PACE	ICAO.PACE_CAN
- Active Authentication is supported	ICAO.AA
- Extended Access Control v1 Chip Authentication and Terminal Authentication version 1 are supported	ICAO.EACv1
Protected eMRTD application The Protected eMRTD profile contains the mandatory feature set for ePassport application restricted to extended inspection systems authenticated by the General Authentication Procedure.	Protected_eMRTD
eID application The eID profile contains the mandatory feature set for [TR-03110-2] compliant electronic Identification application. Therefore, this profile and its tests are mandatory for all products which contain the eID application.	eID
- Restricted Identification	eID.RI

- Explicit Authorization for RI	eID.RI.AuthorizedOnly
- Pseudonymous signature of a Message is supported	eID.PSM
- Pseudonymous Signature of Credentials	eID.PSC
- eID application supports Enhanced Role Authentication	eID.ERA
eSign application The eSign profile contains the mandatory feature set for [TR-Sign-1] compliant application. Therefore, this profile and its tests are mandatory for all products which contain the eSign application.	eSIGN
- Global PIN as eSign PIN	eSIGN.GPIN
- Local PIN	eSIGN.LPIN
- Physical User credential supported	eSIGN.LPIN.PUC

Figure 3 – Test profiles