ETSI TS 103 096-2 V1.1.1 (2013-07)

Intelligent Transport Systems (ITS);
Testing;
Conformance test specification for TS 102 867 and TS 102 941;
Part 2: Test Suite Structure and Test Purposes (TSS&TP)

Reference
DTS/ITS-0050019

Keywords
ITS, testing, TSS&TP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

The present document is part 2 of a multi-part deliverable covering Conformance test specification for ITS Security as identified below:

TS 103 096-1: "Protocol Implementation Conformance Statement (PICS)";

TS 103 096-2: "Test Suite Structure and Test Purposes (TSS&TP)";

TS 103 096-3: "Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)";

TR 103 096-4: "Validation report".

1 Scope

The present document provides the Test Suite Structure and Test Purposes (TSS&TP) for Security as defined in IEEE P 1609.2 [1], TS 102 941 [2] and TS 102 867 [3] in compliance with the relevant requirements and in accordance with the relevant guidance given in ISO/IEC 9646-7 [9].

The ISO standard for the methodology of conformance testing (ISO/IEC 9646-1 [6] and ISO/IEC 9646-2 [7]) as well as the ETSI rules for conformance testing (ETS 300 406 [10]) are used as a basis for the test methodology.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] IEEE P1609.2/D12 (January 2012): "IEEE Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages.

[2] ETSI TS 102 941: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".

[3] ETSI TS 102 867: "Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2".

[4] ETSI TS 103 096-1 (V1.1.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specification for TS 102 867 and TS 102 941; Part 1: Protocol Implementation Conformance Statement (PICS)".

[5] ETSI TS 103 096-3 (V1.1.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specification for TS 102 867 and TS 102 941; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".

[6] ISO/IEC 9646-1 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 1: General concepts".

[7] ISO/IEC 9646-2 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 2: Abstract Test Suite specification".

[8] ISO/IEC 9646-6 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 6: Protocol profile test specification".

[9] ISO/IEC 9646-7 (1995): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".

[10] ETSI ETS 300 406 (1995): "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI EG 202 798: "Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

- terms given in IEEE 1609.2 [1], TS 102 941 [2] and in TS 102 867 [3];
- terms given in ISO/IEC 9646-6 [8] and in ISO/IEC 9646-7 [9].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AA	Authorization Authority
BV	Normal behaviour
CA	Certification Authority
CAM	Cooperative Awareness Message
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
EB	Exceptional Behavior
ITS	Intelligent Transport System
ITS-AID	ITS Application ID
ITS-S	ITS Station
IUT	Implementation Under Test
MSEC	Multicast Security
PKI	Public Key Infrastructure
PSID	Provider Service Identifier
SA	Security Association
SSP	Service Specific Permissions
TLS	Transport Layer Security
TP	Test Purposes
TSS	Test Suite Structure

4 Prerequisites and Test Configurations

4.1 Test Configurations

The test configuration 1 as shown in figure 1 is applied for the test group of CA and EA tests.

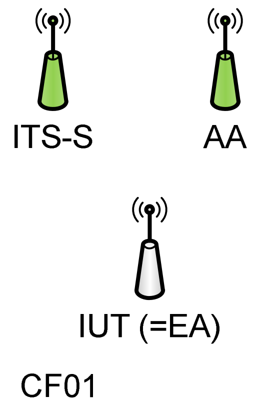

Figure 1: Test Configuration 1

The test configuration 2 as shown in figure 2 is applied for the test group of CA and AA tests.

Figure 2: Test Configuration 2

The test configuration 3 as shown in figure 3 is applied for the test group of ITS-S Enrolment and Authorization tests.

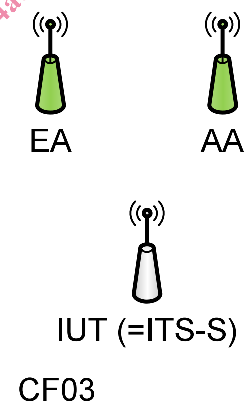

Figure 3: Test Configuration 3

The test configuration 4 as shown in figure 4 is applied for the test group of ITS-S Send and Receive Data tests.

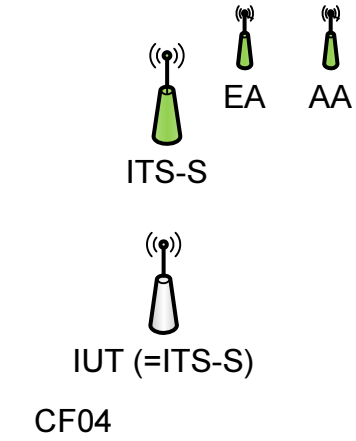

Figure 4: Test Configuration 4

4.2 PKI Hierarchy

The PKI Hierarchy is depicted below. Four different types of certificates are defined. They are listed hereafter.

- CERT_ROOT
- CERT_EA_x
- CERT_AA_x
- CERT_ENR_x
- CERT_AUTH_x

These names are used in the TP definitions, where _x is a placeholder for numbering different certificates.

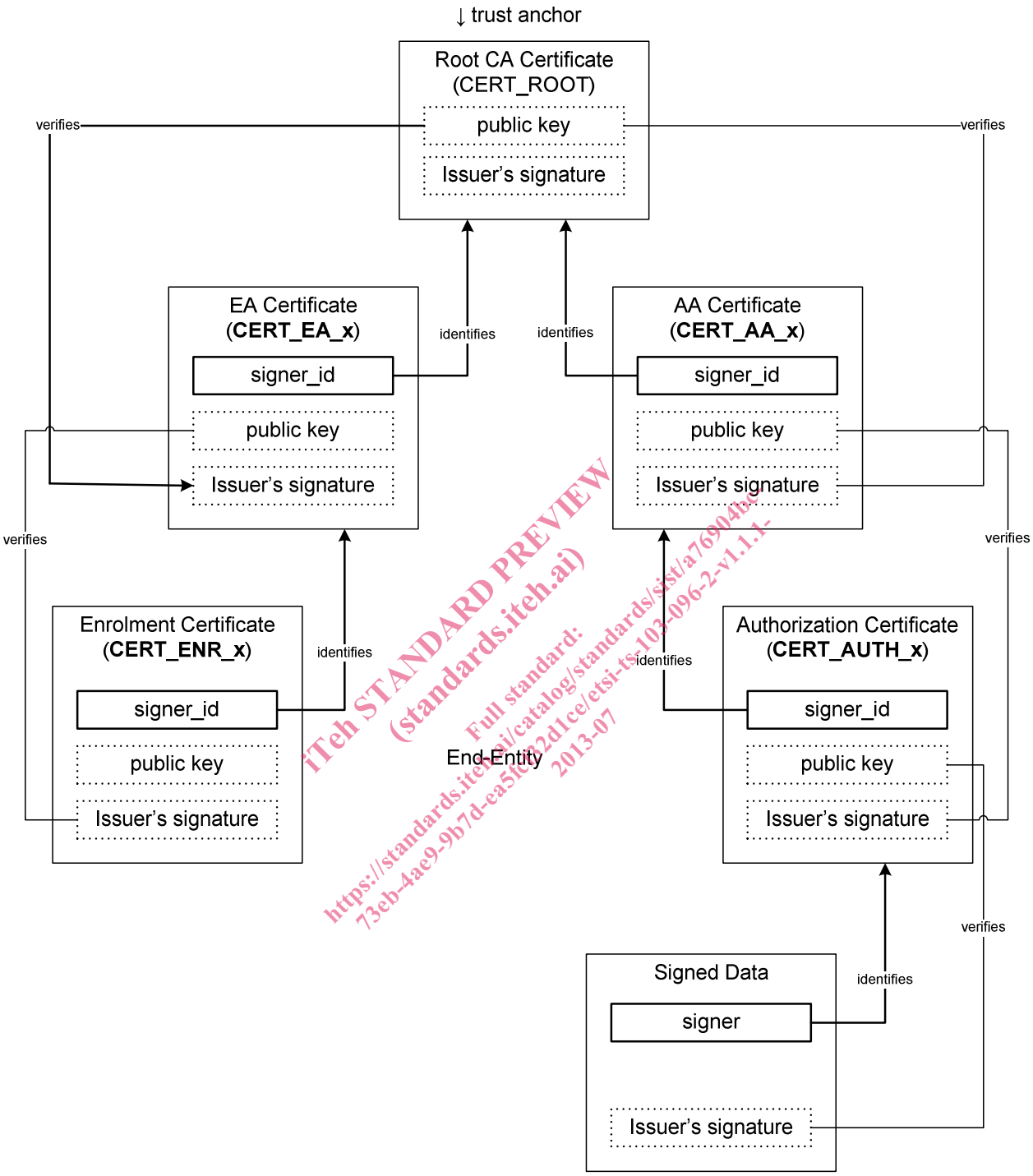

Figure 5: PKI Hierarchy

4.3 Feature Restriction and Pre-Enrolment

4.3.1 Feature Restriction

In this clause all feature restrictions are listed:

- Certificate chains where subordinate certificates make use of inherited permissions are not supported
- Only circular regions

- Only explicit certificates
- Revocation is not tested, i.e. certificate responses contain only empty revocation list
- Update Enrolment Credentials is not tested
- Remove Enrolment Credentials is not tested
- Update Authorization Tickets is not tested
- The name which identifies the CA shall be no longer that 32 bytes

4.3.2 Pre-Enrolment

Enrolment is the process by which an ITS-S obtains an enrolment certificate, which can later be used to authenticate requests for authorization certificates. An ITS-S undergoes initial enrolment by executing the Enrolment Request information flow from TS 102 941 [2].

When devices enrol with an Enrolment Authority, they should be authenticated as devices that are entitled to receive enrolment credentials of the type requested. There are two three different authentication approaches:

- Public key: Enrolment requests are authenticated by using a private key of the ITS-S. The corresponding public key is previously registered with a unique ITS-S module ID at the EA in a secure process. Every ITS-S has to be registered separately.
- Certificate: Enrolment requests are authenticated by a certificate or certificate chain.
- Self-signed: Enrolment requests are signed by the public key contained in the enrolment request. In this case the signature provides proof of possession of the corresponding private key, but does not authenticate that the private key holder is in fact authorized to receive an enrolment credential of the type requested. This authorization is provided by other mechanisms.

None of the three authentication approaches start at the device lifecycle: in all cases, there is the question of how the device is originally shown to be authenticated. The test system supports both the certificate and the self-signed forms of enrolment request.

For enrolment request:

- The test system enrolment authority shall accept the following forms of authorization, certificate and self-signed.
- The test system enrolment authority shall check that the signature on the enrolment request is cryptographically valid.
- In the case of an enrolment request signed by a certificate:
  - The test system enrolment authority shall check that the request is consistent with the permissions in the certificate.
  - The test system enrolment authority shall not carry out any other validation on the signing certificate. For example, it shall not check the signature on the signing certificate, check that the certificate chains back to a known CA, or check whether the signing certificate is revoked.

The test system enrolment authority shall issue the enrolment certificate if these validity tests pass.

From the perspective of the IUT, this has the following consequences:

- Certificate: The IUT shall be provisioned with a certificate to authenticate enrolment before testing begins (a pre-enrolment certificate).
  - The supplier shall provide instructions as to how to reset the IUT to a state where it has the pre-enrolment certificate but not the enrolment certificate, to allow the enrolment flow to be run multiple times.

- The supplier shall chose between two options:
  - The test system generates private key and public certificate for the device.
  - The supplier generates a private key and sends a certificate signing request to the test system.

- Self-signed: The IUT supplier shall provide instructions as to how to set the IUT into a state where it will request enrolment with a self-signed request.

4.4 States in Initial Conditions

Each TP contains an initial condition. The initial condition defines in which initial state the IUT has to be to apply the actual TP. In the corresponding Test Case, when the execution of the initial condition does not succeed, it leads to the assignment of an Inconclusive verdict. This clause defines the different initial states of the IUT.

4.4.1 ITS-S send side states

- Not enrolled state: ITS-S has all info necessary to send an EnrolmentRequest but does not have any Enrolment credentials yet
- Awaiting EnrolmentResponse state: ITS-S has sent an EnrolmentRequest and is waiting for an EnrolmentResponse
- Enrolled, but not authorized state: ITS-S has received EnrolmentResponse and is able to send AuthorizationRequest
- Awaiting AuthorizationResponse state: ITS-S has sent an AuthorizationRequest and is waiting for an AuthorizationResponse
- Authorized state: ITS-S has received a successful AuthorizationResponse

4.4.2 ITS-S receive side states

- Operational state: ITS-S has the root certificate and is ready to receive messages

4.4.3 EA states

- Operational state: EA has obtained its certificate and is ready to receive and send Enrolment messages

4.4.4 AA states

- Operational state: AA has obtained its certificate and is ready to receive and send Authorization messages

4.5 Validity of Signed Communication

The check of the validity of signed communication according to clause 5.5 of IEEE P1609.2/D12 [1] (e.g. consistency check of the certificate chain, consistency check between certificate and message etc) forms an integral part of the test suite and is described in TS 103 096-3 [5], clause 6.

4.6 Introduction of Snippets of Data Structures

The data structures in IEEE P1609.2/D12 [1] can become quite complex. In order to allow to write a TP in a concise form, the usage of snippets has been introduced. A snippet is a partial extract of a data structure which is assigned with values. A snippet can be used within a TP. Please refer to clause 6.1.8 for a complete list of all defined snippets.

Within a TP, any element of the snippet can be overwritten or extended. In the example below the TP extends the snippet **MSG_ENRRSP_TS** 'signature.ecdsa_signature' to ' signature.ecdsa_signature.R.type = = uncompressed'.

...
when {
    the IUT receives a valid CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
        containing certificate_chain[last].signature.ecdsa_signature.<u>R.type</u>
            <u>set to uncompressed</u>
    ...

4.7 Variants, Variables and Snippet Naming Convention

The TPs use the concept of variants, variables and snippets. Their definition, how they are used and their naming conventions are defined in this clause.

Variants: In case where for a single field multiple values can be tested (e.g. different public key types), then a table is appended after the TP. This table lists all the different value which need to be tested. The TP identifier is appended with –X (e.g. **TP/SEC/ITS-S/ENR/NB-02-X**). If there are two fields for which multiple values can be tested then X and Y are appended. The field itself is written as X_FIELD_NAME (e.g. **X_PKT_SIGNATURE**).

Variables: Variables are used in TPs in order to highlight the fact that a particular part of request message needs to re-appear in a response message. For example for a TP where the IUT has sent an EnrolementRequest with a permission list, and the test system needs to sent the same permission list back, then the denotation of **V_PERM_LIST (see TP/SEC/ITS-S/ENR/NB-11)**

Snippets: For the definition of snippets refer to the previous clause. The naming convention for snippets is defined to upper case and to have no specific prefix (e.g. **MSG_ENRREQ_IUT**). All snippets in TPs contain hyperlinks which allows to navigate from the TP directly to the snippet definition.

5 Test Suite Structure (TSS)

5.1 Structure for Security tests

Table 1 shows the Test Suite Structure (TSS) including its subgroups defined for conformance testing.

Table 1: TSS for SECURITY

Root	Group	Group	category
SEC	CA	ENR/AUTH	Normal behaviour
			Exceptional behaviour
	EA	ENR	Normal behaviour
			Exceptional behaviour
	AA	AUTH	Normal behaviour
			Exceptional behaviour
	ITS-S	ENR	Normal behaviour
			Exceptional behaviour
		AUTH	Normal behaviour
			Exceptional behaviour
		S-DATA	Normal behaviour
			Exceptional behaviour
		R-DATA	Normal behaviour
			Exceptional behaviour

The test suite is structured as a tree with the root defined as SEC. The tree is of rank 3 with the first rank a Group, the second rank a sub group, and the last rank a category.