ETSI TS 103 600 V1.1.1 (2019-05)

Intelligent Transport Systems (ITS);
Testing;
Interoperability test specifications for security

Reference

DTS/ITS-00548

Keywords

interoperability, ITS, security, testing

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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document contains specification of interoperability test descriptions to validate implementations of ETSI TS 103 097 [1], ETSI TS 102 941 [3] and ETSI TS 102 940 [i.1].

2 References

2.1 Normative 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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://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.

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

[1] ETSI TS 103 097 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

[2] IEEE Std 1609.2™-2016: "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2a™-2017: "Standard for Wireless Access In Vehicular Environments - Security Services for Applications and Management Messages Amendment 1".

[3] ETSI TS 102 941 (V1.2.1): "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".

[4] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) (V1.1).

2.2 Informative 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 referenced document (including any amendments) applies.

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

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 TS 102 940 (V1.3.1): "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

[i.2] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security; Part 2: Security functional components".

[i.3] ETSI TR 103 415 (V1.1.1): "Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management".

[i.4] ETSI TS 102 731 (V1.1.1): "Intelligent Transport Systems (ITS); Security; Security Services and Architecture".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 097 [1], ETSI TS 102 940 [i.1], ETSI TS 102 941 [3], ISO/IEC 15408-2 [i.2] and the following apply:

current CA: CA possessing the certificate containing in the trusted chain for at least one of certificate currently used by the SUT

foreign CA: any CAs possessing the certificate, been never used in the trusted chain for any end entity certificates used by the SUT

3.2 Symbols

For the purposes of the present document, the symbols given in ETSI TS 103 097 [1], ETSI TS 102 940 [i.1], ETSI TS 102 941 [3], ISO/IEC 15408-2 [i.2] apply.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 103 097 [1], ETSI TS 102 941 [3], ETSI TS 102 940 [i.1], ISO/IEC 15408-2 [i.2] apply.

4 Requirements and configuration

4.1 Requirements

4.1.1 Overview

In order to participate in interoperability tests based on the present document, the implementation shall be compatible with the requirements defined in clauses 4.1.2, 4.1.3 and 4.1.4.

4.1.2 ITS stations

Mandatory requirements:

- The ITS-S shall support data communication using security mechanisms described in ETSI TS 103 097 [1] and PKI communication described in ETSI TS 102 941 [3].
- The ITS-S shall support algorithms and key length according to the Certificate Policy [4].
- In order to participate in secured communication tests, the ITS-S shall be able to send CAMs and DENMs using V2X communication.

Optional requirements:

PICS	Description
PICS_ITSS_REGION_SUPPORT	The ITS-S supports region validity restrictions in AT certificates. The ITS-S shall support at least Circular and Identified region types in order to participate to use-cases dependent of the present PICS value. See IEEE Std 1609.2 [2], clause 6.4.17.
PICS_ITSS_REQUEST_AA	ITS-S is able to request unknown AA certificate using peer-2-peer certificate distribution mechanism without infrastructure involved.
PICS_ITSS_RESPOND_AA	ITS-S is able to answer for the request for unknown AA certificate using peer-2-peer certificate distribution mechanism without infrastructure involved.
PICS_ECTL_SUPPORT	ITS-S can handle information provided in ECTL.
PICS_CRL_SUPPORT_CURRENT	ITS-S can handle information provided in CRL of the currently active RootCA.
PICS_CRL_SUPPORT_FOREIGN	ITS-S can handle information provided in CRL from other RootCAs.
PICS_CTL_SUPPORT	ITS-S can handle information provided in CTL.
PICS_ITSS_PKI_COMMUNICATION	ITS-S is supporting the PKI communication protocol (ETSI TS 102 941 [3]). Otherwise, the ITS-S is unable to participate in PKI test scenarios (clause 6.3 PKI communication).
PICS_ITSS_PKI_ENROLMENT	ITS-S is supporting the enrolment procedure described in PKI communication protocol (ETSI TS 102 941 [3]). Otherwise, the EC certificate shall be installed on the ITS-S manually.
PICS_ITSS_PKI_RE_ENROLMENT	ITS-S is supporting the re-enrolment procedure described in PKI communication protocol (ETSI TS 102 941 [3]).

4.1.3 PKI

Mandatory requirements:

The CAs (RCA, EA, AA) shall support algorithms and key length according to the Certificate Policy [4].

Optional requirements:

PICS	Description
PICS_PKI_ITSS_NO_PRIVACY_REQ	ITS-S supports optional privacy requirement, e.g. RSU. The present PICS does not apply to most vehicular ITS-S.
PICS_PKI_ITSS_RENEW_AT	ITS-S is able to start the AT renewal procedure when all ATs in the pool are expired or about to be expired.
PICS_PKI_CA_MANAGEMENT	The CA (EA, AA) supports CA certificate request procedure. The RootCA supports certificate generation base on CA certificate request procedure.

4.1.4 TLM

Mandatory requirements:

The TLM shall support algorithms and key length according to the Certificate Policy [4].

4.2 Configurations

4.2.1 CFG_SEC - ITS-S secured communication

This clause describes the configuration used to execute secure communication test scenarios. The configuration contains the following entities:

- Sender - The ITS-S playing a sender role.
- Receiver - The ITS-S playing a receiver role.
- Sender AA - The authorization authority that issued the sender's AT.

- Receiver AA - The authorization authority that issued the receiver's AT.

NOTE: The AA is involved to pre-test conditions only. The way how ATs are installed on the SUT are out of scope of this configuration. The same AA can issue ATs for both sender and receiver if not defined otherwise in the use-case description.

In order to participate in the test with the present configuration, ITS-S shall be configured as following if it is not explicitly defined in the use-case description:

- The ITS-S shall be configured to send CAMs in high frequency (more than one CAMs/second) so that the ITS-S sends some of the CAMs with digest instead of ATs.
- All participating ITS-Ss are in the "authorized" state (equipped with valid ATs).
- All ATs of participating ITS-Ss allow the transmission of CAMs and DENMs in the time and place of UC execution.
- All ATs of participating ITS-Ss shall be signed using a valid AA certificate issued by a trusted root certificate authority (RCA).
- All AA certificates used for signing ATs participating ITS-Ss shall be valid for the time and location of the UC execution.
- All RCA certificates used for signing AA certificates shall be valid for the time and location of the UC execution.
- All AA and RCA certificates shall permit issuing of AT certificates containing CAM and DENM PSID.
- No EA, AA or RCA certificates shall be revoked.
- All RCA certificates shall be included in the ECTL.
- All involved CA certificates shall be known and trusted by all participating ITS-S.

4.2.2 CFG_PKI - PKI communication

This clause describes the configuration used to execute PKI communication scenarios. The configuration contains the following entities:

- ITS-S - the ITS station triggering the scenario execution.
- EA - enrolment authority by which the ITS-S is enrolled.
- AA - authorization authority by which the ITS-S is authorized.
- RCA - root certificate authority issuing the EA and AA certificates.
- DC - distribution centers to provide RCA CTL and CRL.
- TLM/CPOC - trust list manager and central point of contacts.
- Observer - the ITS-S (or a network sniffer) allowing to detect that ITS-S is starting to send CAM messages.

NOTE 1: The RCA can be the issuer of both EA and AA.

The ITS-S shall be configured as following if another is not specified in the use-case description:

- The ITS-S shall be configured to send and receive CAMs using V2X communication.
- The ITS-S shall support the PKI communication protocol (see PICS_PKI_COMMUNICATION) defined in ETSI TS 102 941 [3].

The CAs (RCA, AA and EA) shall be configured as following if another is not specified in the use-case description:

- All participating RCA shall have RCA certificates included in the ECTL.

- All AA and EA shall have CA certificates signed by trusted RCA certificate.
- All CA certificates shall be valid for the time and location of the UC execution.
- All CA certificates shall permit issuing of certificates containing CAM and DENM PSID.
- No EA, AA or RCA certificates shall be revoked.
- All sub-CAs certificates shall be included in the CTL.

The TLM/CPOC shall be configured as following:

- TLM shall issue the ECTL containing all participating RCA.

The above configurations can be organized into three groups depending on the participants involved:

Configuration group	Participants involved
CFG_PKI_ENROLMENT	ITS-S, EA, Observer, [DC, TLM/CPOC]
CFG_PKI_AUTHORIZATION	ITS-S, EA, AA, Observer, [DC, TLM/CPOC]
CFG_PKI_CAs	EA, AA, RCA, [DC, TLM/CPOC]

NOTE 2: Connections to DCs and TLM/CPOC are optional in the scope of these tests. Information from ECTL and CTLs/CRLs can be delivered to participating devices using some other particular way.

5 Requirements to be tested

5.1 Overview

The clauses below collect and enumerate the requirements that can be tested with the present interoperability test specification.

5.2 ITS-S communication messages

NN	Requirement	References	UCs
1.1.	A sending ITS-S shall be able to correctly sign CAMs using valid AT certificates	ETSI TS 102 941 [3]	UC-1-1 UC-1-2 UC-1-3 UC-1-4 UC-1-5 UC-2-4 UC-2-5
1.2.	A receiving ITS-S shall be able to verify CAMs signed using valid AT certificates	ETSI TS 102 941 [3]	UC-1-1 UC-1-2 UC-1-3 UC-1-4 UC-1-5
1.3.	ITS-S shall be able to correctly handle (send and receive) CAMs signed with digests before and after transmission of the AT certificate	ETSI TS 102 941 [3]	UC-1-1 UC-1-2 UC-1-3 UC-1-4 UC-1-5
1.4.	ITS-S shall be able to check the timestamp of messages including the validity period of the used ATs	ETSI TS 102 941 [3]	UC-1-1 UC-1-2 UC-1-3 UC-1-4 UC-1-5 UC-2-2 UC-2-4 UC-2-5

NN	Requirement	References	UCs
1.5.	ITS-S shall be able to support peer-2-peer AA certificate distribution: • P2P request of AA certificate • P2P distribution of the requested AA certificate • Accepting of AA certificate received using P2P distribution	ETSI TS 102 941 [3] IEEE 1609.2a [2] clause 8	UC-1-3 UC-2-5
1.6.	ITS-Ss shall not transmit certificates using P2P distribution if another ITS-S already answered the request (discoverable by the sender)	ETSI TS 102 941 [3] IEEE 1609.2a [2] clause 8	UC-1-3 UC-2-5
1.7.	ITS-Ss shall be able to handle and verify DENMs signed with ATs containing certificate regional restrictions: id and circular	ETSI TS 102 941 [3]	UC-2-1
1.8.	ITS-Ss shall consider PSIDs and correspondent SSPs	ETSI TS 102 941 [3]	UC-1-1 UC-1-2 UC-1-3 UC-1-4 UC-1-5 UC-2-2 UC-2-5
1.9.	The ITS-S shall support algorithms and key length according to the EU Certificate Policy. This includes signing, verification, encryption and decryption	EU CP [4] clause 6.1.4	UC-1-1 UC-1-2 UC-1-3 UC-1-4 UC-1-5 UC-2-4 UC-2-5
1.10.	ITS-Ss shall consider CRLs	ETSI TS 102 941 [3]	UC-2-4
1.11.	ITS-Ss shall consider the whole certificate chain when verifying certificates	ETSI TS 102 941 [3]	UC-1-3 UC-2-5
1.12.	Correct change of pseudonyms, with respect to procedure, parameters, place and time	ETSI TR 103 415 [i.3] Table 4, EC CP/SP	UC-1-5

5.3 ECTL Handling

NN	Requirement	References	UCs
2.1.	Check the existence of the ECTL	ETSI TS 102 941 [3] EU Certificate Policy [4]	UC-1-4 UC-2-5 UC-2-3
2.2.	Check the expiration of the ECTL	ETSI TS 102 941 [3] EU Certificate Policy [4]	UC-1-4 UC-2-5 UC-2-3
2.3.	Check the delta ECTL handling	ETSI TS 102 941 [3] EU Certificate Policy [4]	
2.4.	Check the presence of the current root CA[1] certificate in the ECTL	ETSI TS 102 941 [3] EU Certificate Policy [4]	UC-1-4 UC-2-5 UC-2-3
2.5.	Check the presence of foreign root CA[1] certificate in the ECTL	ETSI TS 102 941 [3] EU Certificate Policy [4]	UC-1-4 UC-2-5 UC-2-3
2.6.	Handling ECTL signed using Brainpool P384r1 curve	ETSI TS 102 941 [3] EU Certificate Policy [4], clause 6.1.4	UC-1-4 UC-2-5 UC-2-3
NOTE: The meaning of current and foreign CA is defined in clause 3.1.			