ETSI TS 103 870 V2.1.1 (2025-11)

TECHNICAL SPECIFICATION

Intelligent Transport Systems (ITS);
Test Mode (TM) for operational devices in the field;
Release 2

Reference
DTS/ITS-005222

Keywords
H.F., ITS, security, testing, validation

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

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 defines the means to enable a test environment for verification of specific radio requirements and functional requirements of an ITS-S after deployment, most often when in a non-shielded environment. The present document addresses the security requirements to mitigate the risks identified in ETSI TR 103 971 [i.2].

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 in the ETSI docbox.

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 103 918 (V2.1.1): "Intelligent Transport Systems (ITS); Security; Testing; ITS Misbehaviour Reporting; Interoperability tests specification; Release 2".

[2] ETSI TS 103 868-3 (V2.1.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Misbehaviour Reporting service; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT); Release 2".

[3] ETSI TS 103 525-3 (V2.1.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT); Release 2".

[4] ETSI TS 103 096-3 (V2.1.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT); Release 2".

[5] ETSI TS 102 942: "Intelligent Transport Systems (ITS); Security; Access Control; Release 2".

[6] ETSI TS 103 601: "Intelligent Transport Systems (ITS); Security; Security management messages communication requirements and distribution protocols; Release 2".

[7] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2".

[8] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2".

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

[10] ETSI TS 102 943: "Intelligent Transport Systems (ITS); Security; Confidentiality services; Release 2".

[11] ETSI TS 103 759: "Intelligent Transport Systems (ITS); Security; Misbehaviour Reporting service; Release 2".

[12] ETSI EN 302 665: "Intelligent Transport Systems (ITS); Communications Architecture".

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TR 103 573: "Intelligent Transport Systems (ITS); Pre-standardization study of ITS test mode for operational devices in the field".

[i.2] ETSI TR 103 971: "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

operational mode: mode of an ITS-S

EXAMPLE: Infield test mode, laboratory test mode, active ITS-S mode.

test mode dynamic: infield test mode in which the SUT has dynamic position (i.e. can move in space)

NOTE: The regular message handling and user services are active. Specific ITM certificates are used.

test mode static: infield test mode in which the SUT has a static position (i.e. cannot move in space)

NOTE: The regular message exchange of the station is forbidden and only Messages based on the ITM protocol are received or sent. Specific ITM certificates are used.

3.2 Symbols

Void.

3.3 Abbreviations

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

AA	Authorization Authority
DTS	Dedicated Test System
ITM	Infield Test Mode
ITS-S	Intelligent Transport System Station
IUT	Implementation Under Test
PKI	Public Key Infrastructure
RF	Radio Frequency
SUT	System Under Test
TM	Test Mode
TMS	Test Mode Service
TVRA	Threat Vulnerability Risk Analysis

4 Infield testing essential requirements

As stated in the scope statement (clause 1) of ETSI TR 103 573 [i.1]: "*The test mode provides the ability of testing RF and functional requirements regarding the communication of devices. This includes but is not limited to over the air tests in non-shielded environments without affecting operational ITS stations not targeted by the message*".

The text of ETSI TR 103 573 [i.1] suggests that test and non-test traffic should be separated and this is further identified as essential from the results of a TVRA exercise documented in ETSI TR 103 971 [i.2].

The state of the SUT shall be determined as part of the decision to allow a test to be performed. This is required to assure the safety of the environment and operator as outlined in ETSI TR 103 971 [i.2] where risk of harm to the operator and the environment has priority over any other risk.

Thus where receiving behaviour needs an observer at the IUT there has to be assurance that the observer/observation does not interfere with the vehicle if the vehicle is in motion. If that assurance cannot be given the test shall not be carried out.

Similarly if sending behaviour requires an observer to provide the stimulus then there has to be assurance that the observer/stimulus does not interfere with the vehicle if the vehicle is in motion. If that assurance cannot be given the test shall not be carried out.

NOTE: The present document does not define how the determination of interference with vehicle operation is assessed, rather it assumes that any distraction from driving to attend to the test is a disqualifying interference.

It is assumed that prior to enabling any form of ITM tests that the basic electrical and functional tests have been carried out, i.e. that the ITS-S is powered and reports that it is able to transmit and receive messages. If the basic electrical and functional tests fail then ITM shall not apply (i.e. the equipment is required to have reasonable confidence that it can operate even if there is a reasonable probability that some additional conformance testing will identify a fault).

All conformance and interoperability tests defined in ETSI TS 103 525-3 [3] and ETSI TS 103 096-3 [4] for ITS security and PKI management, and those defined in ETSI TS 103 918 [1] and ETSI TS 103 868-3 [2] for misbehaviour reporting shall, be enabled provided the above conditions are satisfied.

It is assumed for the purposes of the present document that the SUT has been approved for installation and has previously passed all required tests for placement on the market. With this assumption the following requirements apply for all ITM use:

- ITM shall be exclusive, i.e. whilst ITM is enabled the ITS-S acting as SUT shall not act on any other ITS messaging.
- ITM shall be disabled by default in all ITS-Ss.
- ITM shall be enabled by an activation message from an authorized test system.
- Activation messages shall be addressed to a specific ITS-S.
- ITM shall be disabled by a deactivation message from an authorized test system to a specific ITS-S, or shall deactivate on expiry of the ITM timer.
- ITM shall be able to be deactivated by direct command of the user of the SUT.
- The ITM timer maximum value shall not exceed 1 hour and shall be reset on receipt of an authenticated and authorized ITM message.
- A receiving ITS-S shall not act on a received ITM message if ITM has not been enabled.

5 Security Architecture of ITM

ITM shall follow the core security models, data structures, protocols and certificate formats from each of ETSI TS 102 942 [5], ETSI TS 103 601 [6], ETSI TS 103 097 [7], ETSI TS 102 940 [8], ETSI TS 102 941 [9], ETSI TS 102 943 [10] and ETSI TS 103 759 [11].

As identified in both ETSI TR 103 573 [i.1] and ETSI TR 103 971 [i.2] there has to be authoritative separation of ITM from any normal ITS operation. Every received ITS message is expected to be signed and the signature verified before processing. In ETSI TS 102 942 [5] as all assets are required to be considered as protected with a default access control result of DENY it is essential that the access control model is able to clearly distinguish an access attempt from an ITM service or message from any non-ITM service or message access attempt. All ITM messaging shall be authorized by a recognized ITM authority.

In the context of pre-conditions for assuring ITM authority separation the test keys identified in clause 5.3.2 of ETSI TS 103 096-3 [4] shall be augmented as follows. The certificates that shall be installed in order to run the mandatory tests are variants of those defined in [4] and need to be clearly identifiable as being part of the ITM authorization tree.

- CERT_IUT_A_ITM_RCA
- CERT_IUT_A_ITM_AA

At least the CERT_IUT_A_ITM_RCA and CERT_IUT_A_ITM_AA certificates shall be installed onto the IUT to be able to validate messages sent by the DTS (see clause 6 below). All certificates used in mandatory tests are derived from the CERT_IUT_A_ITM_RCA certificate.

The AA used to distribute the certs used in ITM shall be identifiable as an ITM authority.

6 Physical architecture of ITM

The physical architecture of the ITM is shown in Figure 1. It consists of two main components.

- The Dedicated Test System (DTS).
- The ITS-S acting as the System Under Test (SUT).

In respect of the exclusive nature of ITM the following additional requirements in respect of activation of ITM apply.

- The DTS shall be able to request an ITM session with a specific ITS-S.
- Any ITS-S invited to join an ITM session shall be able to reject the invitation with a clear indication of why the invitation is being rejected.
- On acceptance of an invitation to join the ITM session only the key hierarchy of the ITM shall apply.

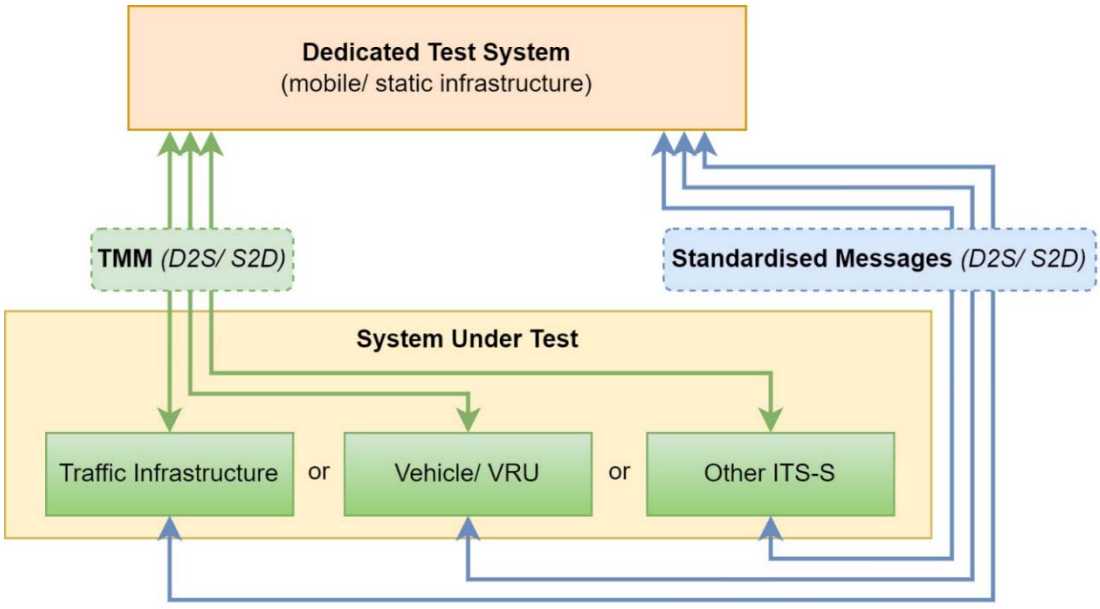

Figure 1: ITM system physical architecture

7 TMS functional specification

7.1 SUT ITS-S operational modes

The specification of the ITS communication architecture from ETSI EN 302 665 [12] applies.

As shown in figure 2 a distinction is made between three different operating modes, where the "Active ITS-S Mode" includes the general specification for an ITS-S as described above.

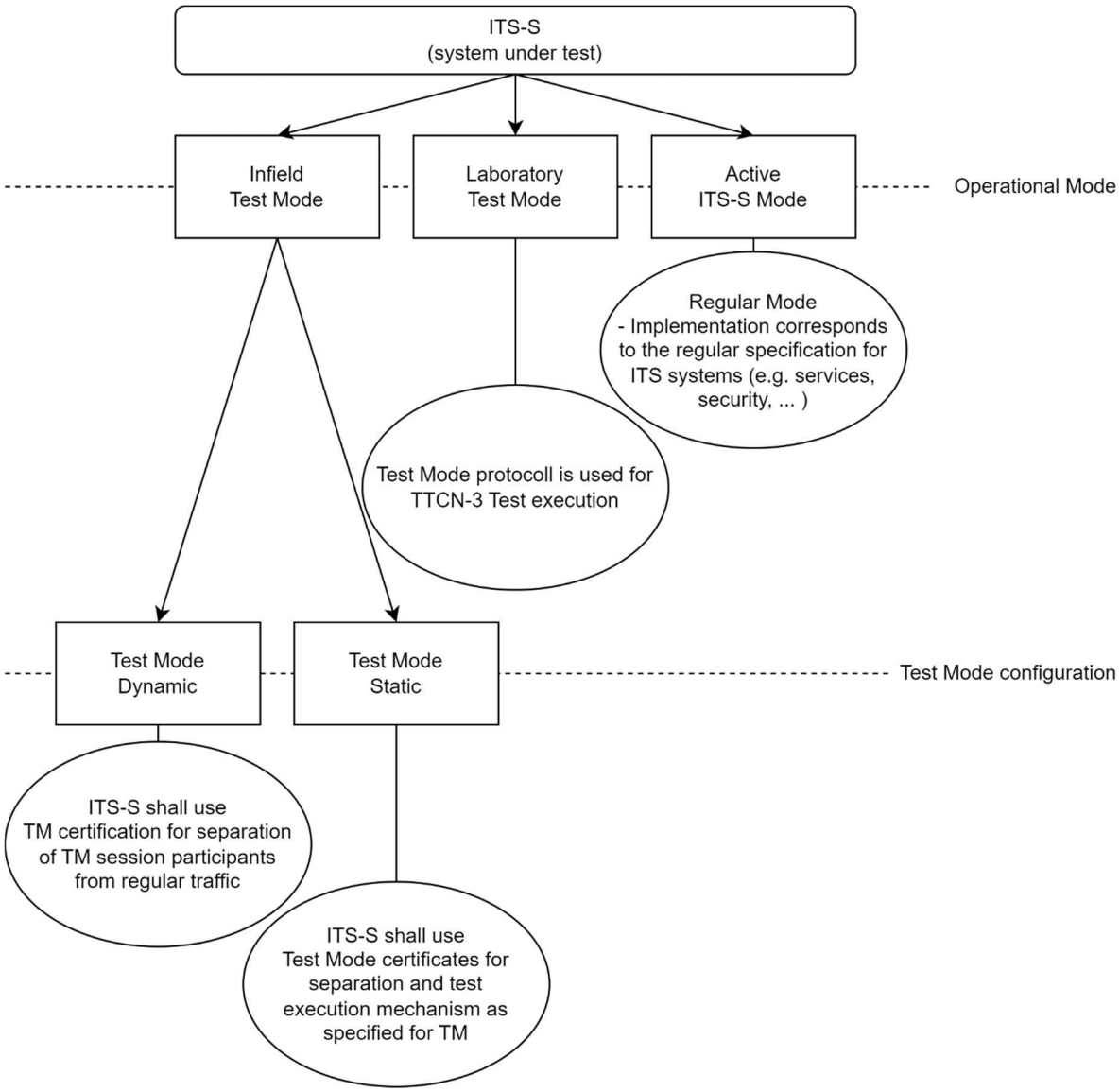

Figure 2: Operational modes of a SUT ITS-S

7.2 Test architecture

7.2.1 General architecture

The Test Mode architecture for ITM shall follow the model in clause 5 of ETSI TS 103 096-3 [4].

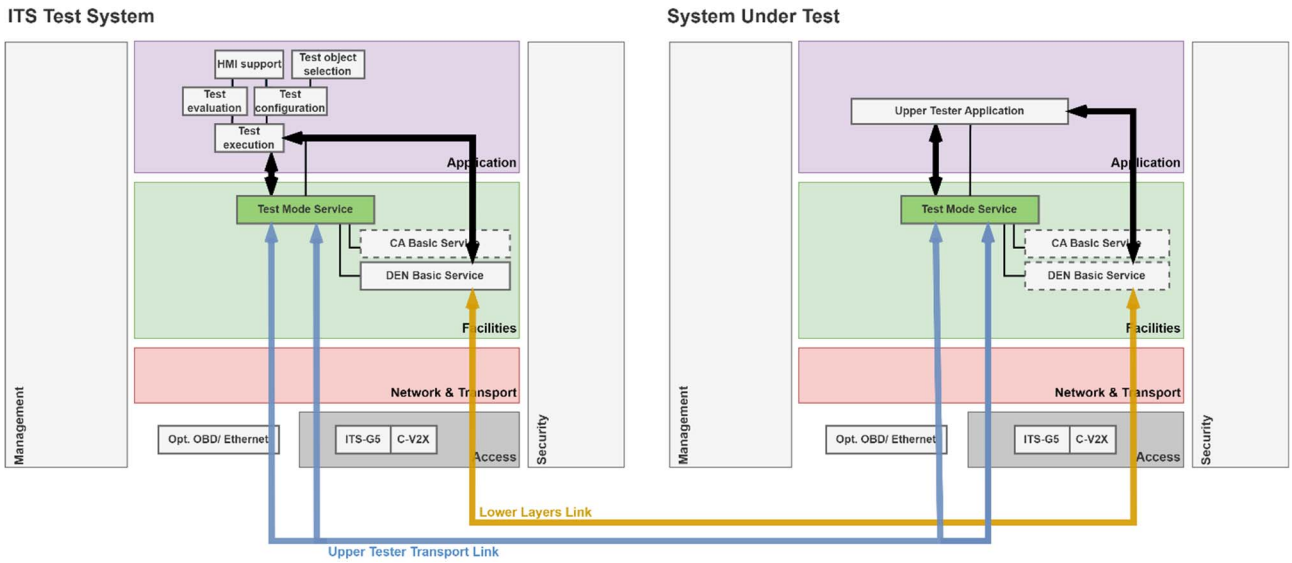

Figure 3: TM general architecture

7.2.2 Upper tester

The upper tester shall be as defined in clause 5 of ETSI TS 103 096-3 [4].

7.2.3 Lower tester

The lower tester shall be as defined in clause 5 of ETSI TS 103 096-3 [4].

7.3 Initialization and termination

7.3.1 Initialization of ITM

ITM shall only be activated by an authorized ITS-S DTS and shall follow the general process defined in clause 7.2 of ETSI TS 103 096-3 [4].

7.3.2 Termination of ITM

ITM shall only be deactivated by an authorized ITS-S DTS and shall follow the general process defined in clause 7.2 of ETSI TS 103 096-3 [4].

Annex A (informative): Bibliography

ETSI TS 102 165-1: "Cyber Security (CYBER); Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

ETSI TR 102 638 (V1.1.1): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions".

ETSI TS 102 965 (V2.1.1): "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration; Release 2".

History

Document history		
V2.1.1	November 2025	Publication