ETSI Plugtests Report V1.1.2 (2019-05)

# 6th ITS Cooperative Mobility Services Plugtest
# Sophia Antipolis, France
# 25th February – 1st March 2019


Keywords
Testing, Interoperability, ITS

***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 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 only prevailing document is the print of the Portable Document Format (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

# 1 Executive Summary

ETSI‘s ITS technical committee develops standards for communications between vehicles (e.g. car-to-car), and between vehicles and fixed locations (e.g. car-to-infrastructure). ITS is scheduled to be deployed in Europe. In order to meet this goal, the European Commission has financially supported the development of ETSI’s release 1 package of ITS standards. The existence of common European standards is paramount to ensure the interoperability of ITS services and applications as well as to accelerate their introduction for the car industry and road users.

Standard development should ideally undergo a cycle of specification development, followed by validation of the specification, followed by development of standardized test specifications. ETSI implements these best practices through organizing Plugtests™ interoperability events and creating standardized test specifications.

ETSI, in partnership with ERTICO, has organized the latest in a series of Plugtests™ interoperability events for Intelligent Transport Systems (ITS) Cooperative Systems. This event took place at ETSI headquarters in Sophia Antipolis, France from 25 February to 1st March 2019.

Participating companies from the automotive sector tested the interoperability of their security solutions. In addition they ran tests to assess their compliance with ETSI ITS Release 1 security developed by the ETSI ITS technical committee. This event was also technically supported by the European Commission, which provided the first versions of its ECTL to providers on this occasion

# 2 References

The following base specifications applied for the Plugtest.

[1] ETSI EN 302 636-4-1 (V1.3.1): "Intelligent Transport System (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to multipoint communications; Sub-part 1: Media independent functionalities".

[2] ETSI TS 103 097 (V1.3.1): ITS Security; Security header and certificate formats

[3] ETSI TS 102 941 (V1.2.2): ITS Security; Trust and Privacy Management

[4] ETSI TS 102 940 v1.3.1 :ITS Security; ITS communications security architecture and security management

[5] IEEE 1609.2a-2017 :IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages

[6] EU CP v1.1 :EU Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)

[7] ETSI EN 302 636-4-1 (V1.3.1): "Intelligent Transport System (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to multipoint communications; Sub-part 1: Media independent functionalities".

[8] ETSI EN 302 637-2 (V1.4.0, draft): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[9] ETSI EN 302 637-3 (V1.3.0, draft): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".

[10] ETSI TS 103 600 (V0.0.18, draft):"Intelligent Transport Systems (ITS); Interoperability test specifications; Test descriptions for security"

[11] ETSI TS 103 096 (V1.4.1): ITS Security; Conformance test specifications for ITS Security

[12] ETSI TS 103 525 (draft): ITS Security; Conformance test specifications for ITS PKI management

[13] ETSI TR 103 099 (V1.4.3, draft): Intelligent Transport Systems (ITS); Architecture of conformance validation framework (draft for PKI conformance tests)

# 3 Abbreviations

| | |
|---|---|
| AA | Authorization Authority |
| ATS | Abstract Test Suite |
| CA | Certification Authority |
| CAM | Cooperative Awareness Message |
| CMS | Cooperative Mobility Services |
| CRL | Certificate Revocation List |
| CTL | Certificate Trust List |
| DENM | Decentralized Environmental Notification Message |
| ECTL | European Certificate Trust List |
| EUT | Equipment Under Test |
| GPSD | Daemon that receives data from a GPS receiver. It provides a unified interface to receivers of different types, and allows concurrent access by multiple applications |
| GN | GeoNetworking |
| ITS | Intelligent Transport System |
| ITS-S | ITS Station. Can be either RIS or VIS. This acronym is used when the role of the ITS Station is not relevant for the scope of the test.<br>Note: When the role is relevant for the test, then RIS or VIS is used. |
| MAC | Media Access Control layer of the access layers |
| PHY | The Physical layer of the access layers |
| NO | Test is recorded as NOT successfully passed |
| NA | Test is not applicable |
| OK | Test is recorded as successfully passed |
| OT | Test is recorded as not being executed due to lack of time |
| PKI | Public Key Infrastructure |
| Test Session | A paring of vendors that test together during a given time slot |
| TSR | Test Session Report. Report created during a test session |
| TTCN-3 | Testing and Test Control Notation Version 3 |

# 4 Participants

The ITS CMS6 event on ITS security was attended by 20 ITS-S device vendors, 9 PKI providers. Globally, ETSI hosted 85 participants, including observers.

The companies which attended the Plugtests are listed in the table below.

**Table 1: List of ITS-S vendors**

| | |
|---|---|
| APTIV | LINKS Foundation |
| AustriaTech GmbH | Marben Products |
| CNIT | NORDSYS |
| Cohda Wireless Europe | Q-Free |
| Commsignia Ltd | Savari |
| CTAG | Siemens Mobility |
| Dynniq | TNO |
| ESCRYPT GmbH | Trialog |
| Kapsch TrafficCom | Vector Informatik |
| LACROIX Neavia | YoGoKo |

**Table 2: List of PKI providers**

| | |
|---|---|
| ATOS | Gemalto |
| BlackBerry | INTEGRITY Security Services |
| CNIT | IDnomic |
| CTAG | MicroSec |
| ESCRYPT GmbH | |


# 5 Technical and Project Management

## 5.1 Test Plan

The test plan containing 22 use cases was developed by ETSI CTI together with a team of experts. The test plan will be published as a separated deliverable ETSI TS 103 600 v1.1.1.

## 5.2 Test Scheduling

The test schedule was developed before the Plugtest and was circulated to all the participants. Each day was organized in two morning test sessions from 9.00 to 13.00 and in two afternoon test sessions from 14.00 to 18.00. Up to 12 simultaneous sessions between different vendors were organised at the same time.

During the test event the test schedule was constantly updated according to the progress of the test sessions. This was done during the daily wrap-up meetings at the end of each day and during face-to-face meetings with the participants.

Three types of test configuration were used:

- ITS-S to ITS-S secured communication
    - Two ITS-S devices from different vendors play a role of sender and receiver in this test configuration
- ITS-S to PKI communication
    - ITS-S device communicates with the PKI provider. Another optional PKI plays a role of external AA.
- PKI to PKI communication
    - CA of one PKI vendor prepares the CA certificate request to be treated by the RootCA of another PKI vendor.

## 5.3 Test Infrastructure

### 5.3.1 Overview

The event contains only laboratory based tests, so there no special requirements for infrastructure. Only GPSD server and Conformance validation framework was provided during the event.

### 5.3.2 GPSD Server

The GPSD server emulates the movement of cars to run the pseudonym changing use-case. Participants can use any track provided by the server.

There were 3 types of tracks:

1. Short track around the ETSI headquarter

**Figure 1: Short track around the ETSI headquarter**

2. Long track near ETSI headquarter to emulate pseudonym changing strategy

**Figure 2: Long track near ETSI headquarter to emulate pseudonym changing strategy**

3. Track outside the certificate validity region (in the port of Livorno, IT).

### 5.3.3 Conformance Validation Framework

The ETSI ITS Conformance Validation Framework is a test software to assess the base standard compliance of a vendor implementation, as shown in the figure below. The Conformance Validation Framework was used in parallel with the interoperability activity, see clause 6.2.

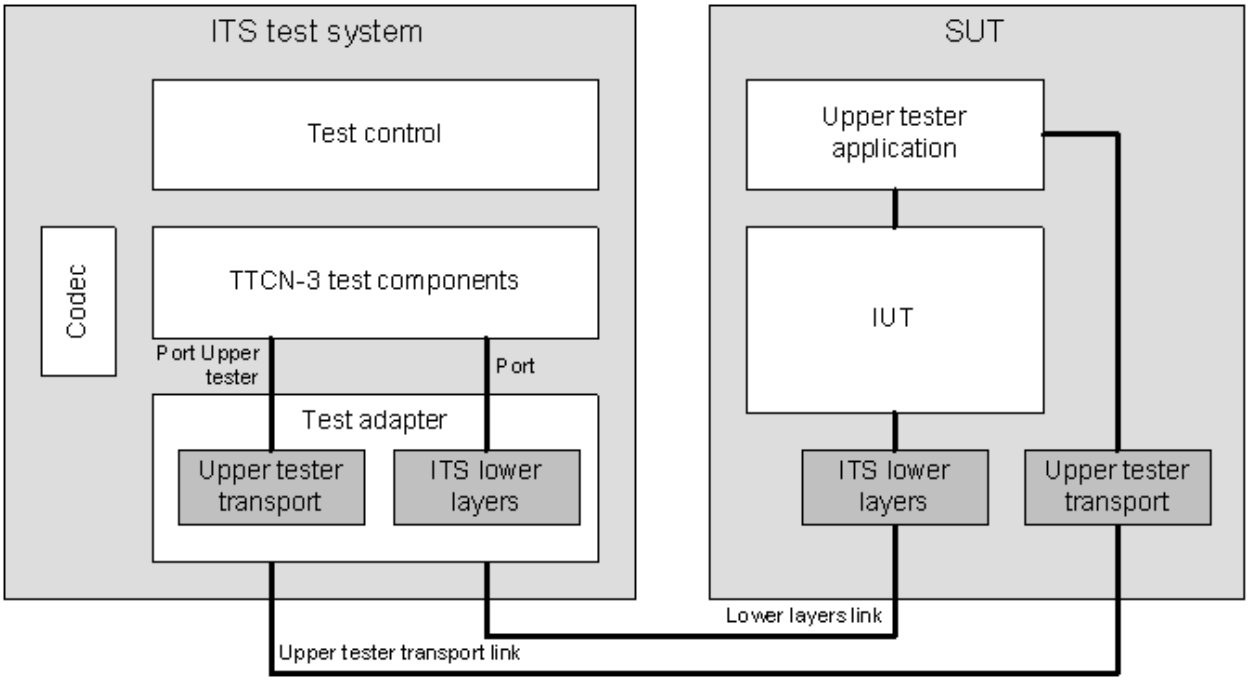


**Figure 3: Conformance Validation Framework**

# 6 Achieved Interoperability Results

## 6.1 Overview

The ETSI ITS Conformance Validation Framework is presented in clause 5.3.3.

Before attending the Plugtest the participants were offered the possibility to validate their compliance to the ETSI PKI. This step, before the Plugtest, was important, as it helped to detect and mitigate potential errors early on, rather than having to debug these issues in the field on the Plugtest.

## 6.2 Conformance

The tests are developed in TTCN-3 (see www.ttcn-3.org) and cover the following ETSI standards:

**Table 3: List of available test specifications**

| Base Standard | ETSI Test Specification |
|---|---|
| ETSI EN 302 637-2 v1.3.2: CAM base specification | ETSI TS 102 868-1,2,3 (V1.4.1 available in Feb 2017) |
| ETSI EN 302 637-3 v1.2.2: DENM base specification | ETSI TS 102 869-1,2,3 (V1.5.1 available in Feb 2017) |
| ETSI EN 302 636-4-1 v1.2.1: GN base specification | ETSI TS 102 871-1,2,3 (V1.4.1 available in Feb 2017) |
| ETSI TS 103 097 V1.2.1: Security header and certificate formats | ETSI TS 103 096-1,2,3 (V1.3.1 available in Feb 2017) |
| ITS Security; Trust and Privacy Management | ETSI TS 102 941 v1.2.2 |
| The specification ERRATA | ERRATA TS 102 941 |
| ETSI TS 103 301 V1.1.1: Infrastructure Services | ETSI TS 103 191-1,2,3 (V1.2.1 available in Feb 2017) |

NOTE The latest builds of Wireshark provides support of the latest version of ETSI ITS protocols and IEEE 1609.2a-2017 protocol

**Scope – Pre-testing & Conformance Tests:**

- ATS Security (Secured CAM, DENM)
  - Almost 10 companies
  - Focused on secured CAM and DENM tests
  - using ETSI certificates
- ATS PKI (PKI side)
  - 9 PKI providers
  - Enrolment
  - Authorization
  - Authorization Validation
- ATS PKI (OBU side)
  - 1 company
  - Enrolment / Authorization

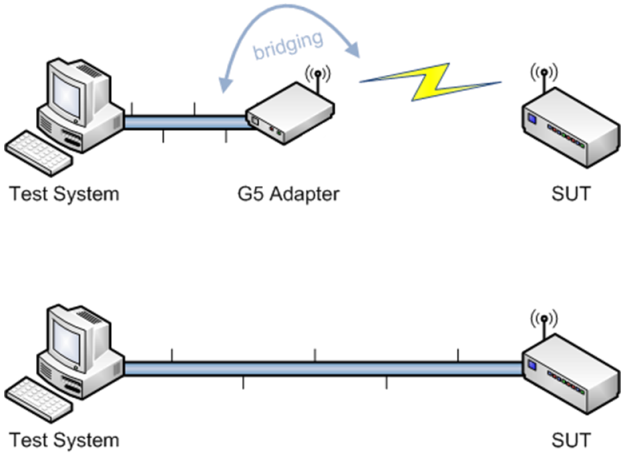


**Figure 4: Conformance Validation setup**

## 6.3 Interoperability Use Cases

The interoperability test cases are described in ETSI TS 103 600 [i.10]. They are divided in three parts, based on their scope, as described below.

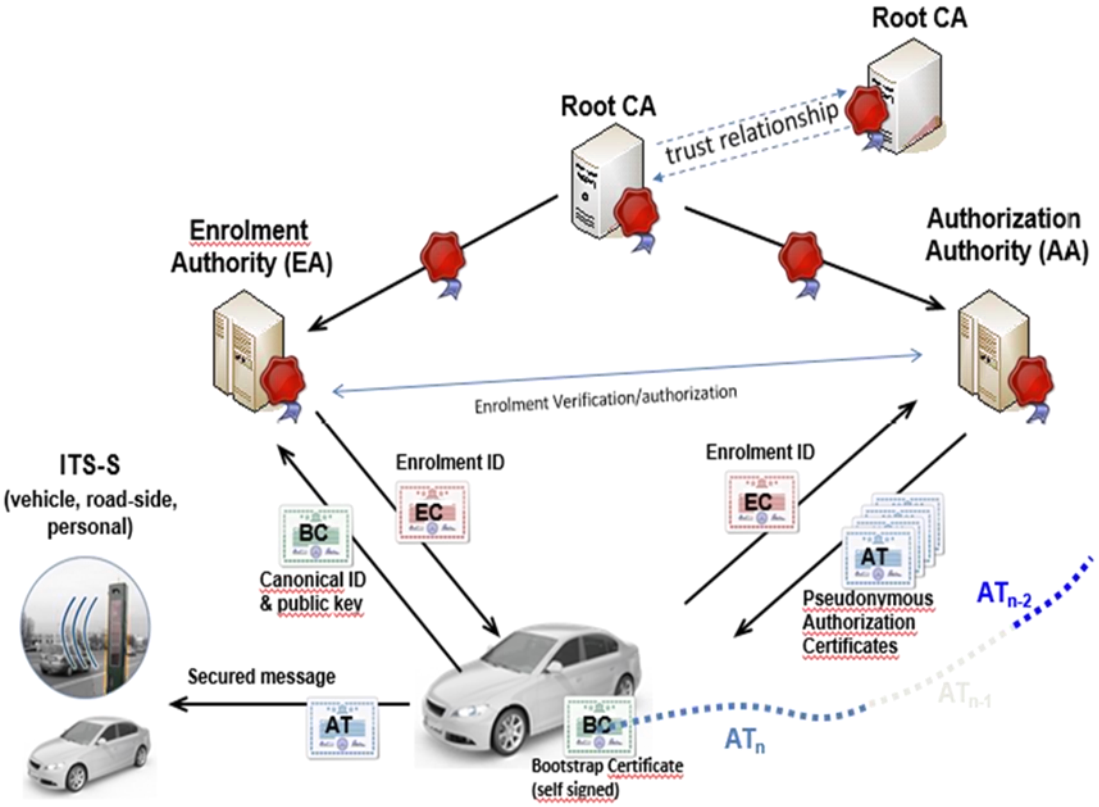


**Figure 5: Interoperability tests architecture**

Scope of Interoperability Tests

- ITS-S to ITS-S secured communication
  - been enrolled in the same PKI
  - using certificates from different PKIs
  - exceptional cases (out of region, expired or not yet valid certificates, revoked AA, …)
  - usage of ECTL, CTL and CRL.
- ITS-S to PKI communication
  - Enrolment, re-enrolment
  - authorization
- PKI to PKI communication
  - Authorization validation
  - CA certificate request

## 6.4 Achievements – Interoperability Testing

- ITS-S devices can communicate securely basing on the IEEE 1609.2a and TS 103 097 v1.3.1
- ITS-S and PKI can communicate with the protocol described in TS 102 941 v1.3.1
- Usage of CAM v1.4.0, DENM v1.3.0 and GeoNetworking v1 over ITS G5 was validated
- There are no blocking issues that were found for ITS-S secured communication and for PKI communication
- The count of PKI implementations is more than predicted and the level of maturity is well enough to be operational
- A lot of debugging was done during testing sessions, many bugs and misunderstandings were resolved
- A lot of consultancy was provided by security experts
- The ECTL was generated and provided for tests multiple times. It was parsed, verified and actually used by 4 participants
- Support of ECTL by ITS-S devices and PKI providers should be improved

Furthermore, the following were noted during the Plugtests event:

- 10 / 39 companies canceled their participation just before the event
- 5 / 29 companies arrived but were not able to test because of implementation problems
- Only 60% of companies were able to test PKI communications scenarios
- Only 40% of use-cases per sessions were executed during the event
- Brainpool curves are not yet supported by all participants
- ECTL/CTL/CRL were not widely supported

In summary, the general feedback from participants was that another Plugtests event is highly requested!

## 6.5 Issues found during the Interoperability Testing

Some issues were found and will be provided to TC ITS and EC as an outcome of the event:

- Proposal to exclude the combination of 0/0 in SSP value/bitmask in CA certificates
- All fields of RequestedSubjectAttributes shall be kept optional
- The BinaryId field of the CertificateId structure shall be allowed in TS 103 097 to store technical keys
- Better explication about the identification of Hash algorithm is required in IEEE1609.2 or TS 103 097
- Specification of actual field for the SSP bitmask is required in TS 103 097
- Proposal to allow the presence of RCA DC entries in the ECTL
- Some potential ASN.1 improvements were found (Version type, etc)
- Avoiding of encryption key in AT certificate without particular reasons
- Accepting of the subsequent EC requests
- Verification procedure of assurance level is not defined

# 7 Base Specification Validation

## 7.1 Trust and Privacy Management specification

The table below lists the issues discovered in the base specification ETSI TS 102 941 V1.2.2 [i.3].

**Table 4: Discovered PKI spec issues**

| | |
|---|---|
| 1 | Optional fields in enrolment request:<br>All fields of RequestedSubjectAttributes shall be kept optional. AA and EA may use information from this field but shall not require it. |
| 2 | Allowance of binaryId in CertificateId. It was recommended to add the possibility to use binary id in the CertificateId field in order to store the canonical id of the ITS-S. |
| 3 | Usage of various hash algorithms in the message shall be clarified in IEEE 1609.2 |
| 4 | Facility standards shall specify the message field where SSP information is stored. |
| 5 | RCA DC URL is unknown for others. It was proposed to allow including of RCA DC in the ECTL. |
| 6 | ASN.1 encoding of 'Version' type. The type Version is used multiple times and encoded differently. It was proposed to generalise it encoding. |
| 7 | Encryption key in AT shall be avoided if not used |
| 8 | Facility layer shall describe the behaviour of message validation if the message generation position is not required |
| 9 | Handling of repeated initial enrollment requests (e.g. in case of a reset device) |
| 10 | Acknowledgements/feedback (from AA to EA) of successful or failed issuance of ATs |
| 11 | Possibility of repeated (unchanged) AT requests, asking for the expected results, in case of delayed AT issuance or sporadic internet connection |

# History

| Document history | | |
|---|---|---|
| V1.1.1 | 02/05/2019 | Publication |
| V1.1.2 | 21/05/2019 | removed links to WIKI pages |