TECHNICAL REPORT

7th ITS Cooperative Mobility Services Plugtests; Sophia Antipolis, FR; 8 – 11 November 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

Copyright Notification

Contents

Intellectual Property Rights

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 8 to 11 of November 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 present event:

[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 (V1.3.1): 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 302 637-2 (V1.4.1): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[8] ETSI EN 302 637-3 (V1.3.1): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".

[9] ETSI TS 103 600 (V1.1.1):"Intelligent Transport Systems (ITS); Interoperability test specifications; Test descriptions for security"

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

[11] ETSI TS 103 525 (V1.1.1): ITS Security; Conformance test specifications for ITS PKI management

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

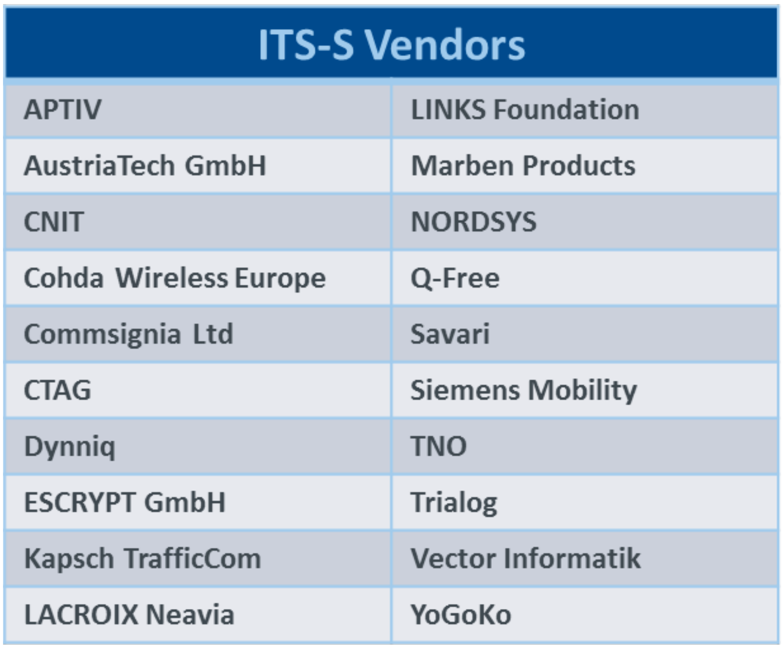
3 Abbreviations

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. 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

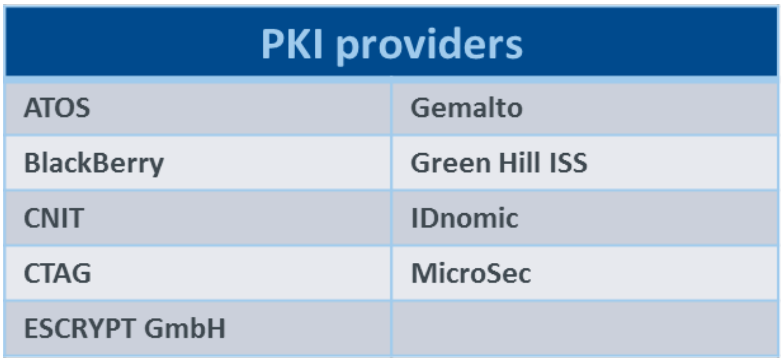
The ITS CMS7 event on ITS security was attended by 17 ITS-S device vendors, 12 PKI providers. Globally, ETSI hosted 70 participants, including observers.

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



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 1: List of ITS-S vendors



PKI providers	
ATOS	Gemalto
BlackBerry	Green Hill ISS
CNIT	IDnomic
CTAG	MicroSec
ESCRYPT GmbH	

Table 2: List of PKI providers

5 Technical and Project Management

5.1 Test Plan

ETSI CTI together with a team of experts developed the test plan containing 24 use cases. The test plan is published as a separated deliverable ETSI TS 103 600 v1.1.1 after CMS#6 event and was updated for this event in order to support ECTL and CPOC dedicated use-cases. The new version of the interoperability test specification will be published after the event.

5.2 Test Scheduling

The test schedule was developed before the Plugtests event 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. 158 test sessions were organized and up to 11 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 (2 hour session)
  Two ITS-S devices from different vendors play a role of sender and receiver in this test configuration

- ITS-S to PKI communication (2 hour session)
  ITS-S device communicates with the PKI provider. Another optional PKI plays a role of external AA.

- PKI to PKI communication (unscheduled)
  CA of one PKI vendor prepares the CA certificate request to be treated by the RootCA of another PKI vendor. These sessions were run in ad-hoc manner in parallel with other sessions.

5.3 Test Infrastructure

5.3.1 Overview

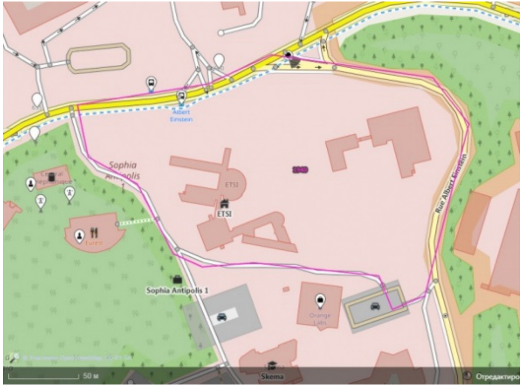
The event contains only laboratory based tests, so there no special requirements for infrastructure. Only GPSD server and Conformance validation framework was provided during the event.

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 2 types of tracks:

1. Short track around the ETSI headquarter



2. 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 .

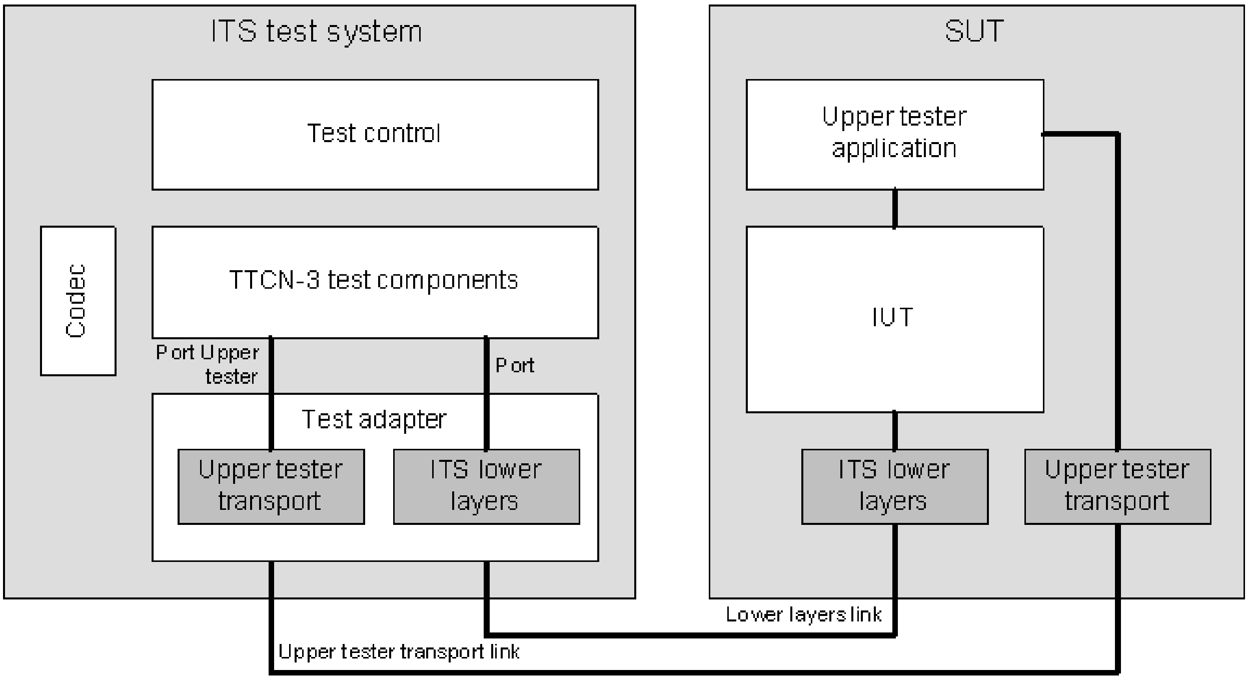


Figure 1: Conformance Validation Framework

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 Specifiction
ETSI TS 103 097 V1.3.1 [2]: Security header and certificate formats	ETSI TS 103 096-1,2,3 (V1.4.1) [10]
ETSI TS 102 941 V1.3.1 [3]: ITS Security; Trust and Privacy Management	ETSI TS 103 525-1,2,3 (V1.1.1) [11]

The tests used for the pre-testing activity (see Table 3), are available at:

https://forge.etsi.org/gitlab/ITS/ITS/tree/STF525

Scope – Pre-testing & Conformance Tests:

- ATS Security (Secured CAM, DENM)
  - Almost 3 companies
  - Focused on secured CAM and DENM tests
  - using ETSI certificates
- ATS PKI (PKI side)
  - 4 PKI providers
  - Enrolment
  - Authorization
  - Authorization Validation
- ATS PKI (OBU side)
  - 1 company
  - Enrolment / Authorization

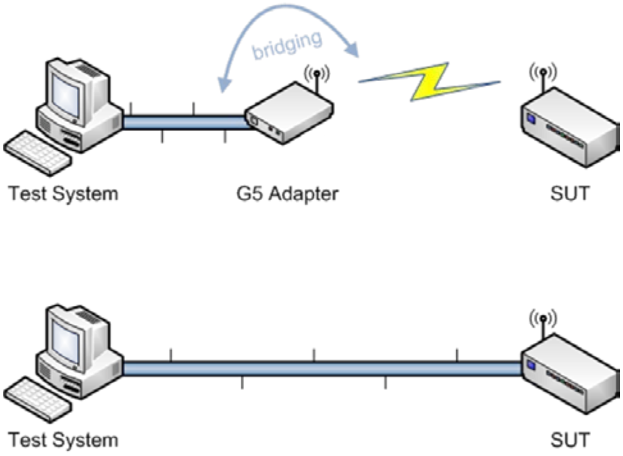


Figure 2: Conformance Validation setup

6.3 Interoperability Use Cases

The interoperability test cases are described in ETSI TS 103 600 [9]. They are divided in three parts, based on their scope, as described below.

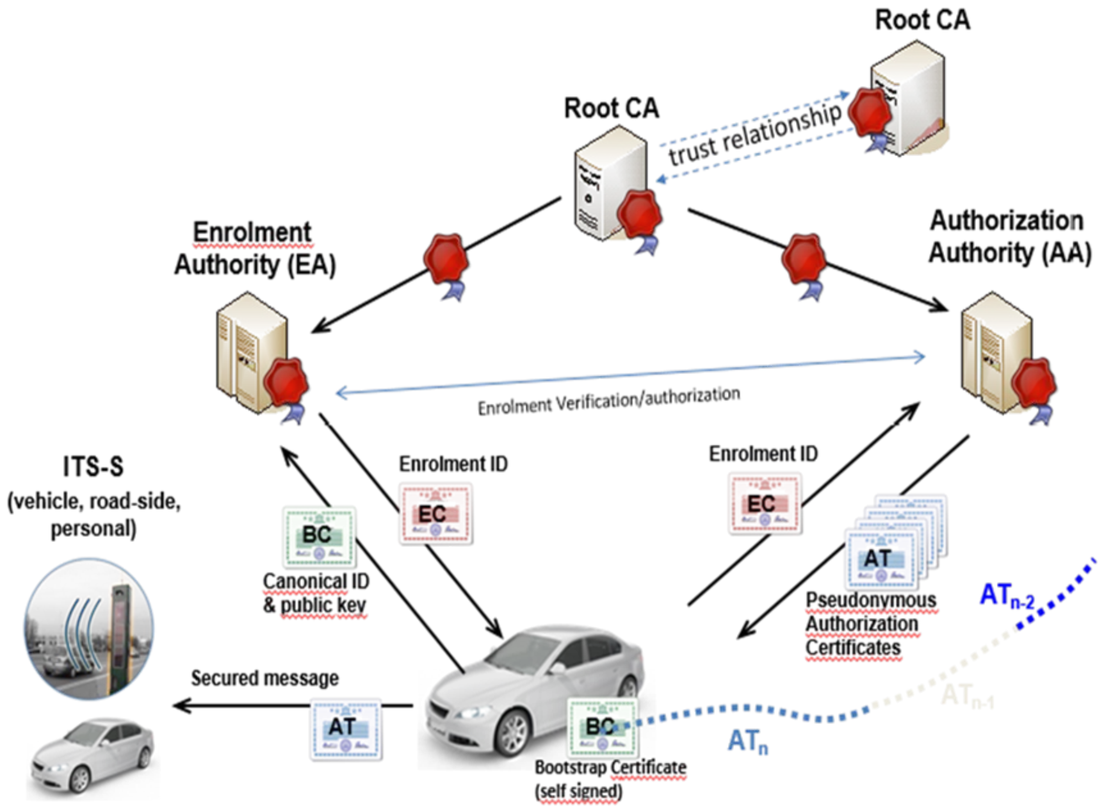

Root CA
Root CA
trust relationship
Enrolment Authority (EA)
Authorization Authority (AA)
Enrolment Verification/authorization
Enrolment ID
Enrolment ID
EC
EC
ITS-S
(vehicle, road-side, personal)
BC
Canonical ID & public key
AT
Pseudonymous Authorization Certificates
AT_{n-2}
AT_{n-1}
AT_n
Secured message
AT
BC
Bootstrap Certificate (self signed)

Figure 3: 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
    - usage of ECTL, CTL and CRL.
- PKI to PKI/CPOC communication
    - authorization validation
    - CA certificate request
    - re-keying and revocation of RCA

6.4 Achievements – Interoperability Testing

- ITS-S devices can communicate securely basing on the IEEE 1609.2a [5] and TS 103 097 v1.3.1 [2].
- ITS-S and PKI can communicate with the protocol described in TS 102 941 v1.3.1 [3].
- Usage of CAM v1.4.1 [7], DENM v1.3.1 [8] and GeoNetworking v1 [1] over ITS G5 were validated.
- There are no blocking issues 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.
- 4 ECTL signing sessions were organized and 4 version of ECTL were provided for tests. Many participants successfully parsed, verified and actually used by the ECTL.

The level of maturity is significantly increased since the previous Plugtests event in February 2019. Many companies having cancelled their participation in the previous Plugtests event now were able to successfully participate and execute test cases.

Table 4 presents the overall use-case execution summary of the event:

Use-case execution		Not Executed		Totals	
OK	Not OK	Not applicable	Out of Time	Run	Results
694 (93.7%)	47 (6.3%)	632 (46.0%)	(0.0%)	741 (54.0%)	1373

Table 4: Overall use-case execution results

Table 5 presents the results of test execution for every group of tests:

Use-case group	Interoperability Use-case execution		Not Executed		Totals
	OK	Not OK	Not applicable	Out of Time	Run / Total
ITS-S communication	230 (92.7%)	18 (7.3%)	301 (54.8%)	0 (0.0%)	248 /549 (45.2%)
ITS to PKI communication	461 (94.1%)	29 (5.9%)	331 (40.3%)	0 (0.0%)	490 / 821 (59.7%)
PKI to PKI and CPOC communication	3 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	3 / 3 (100.0%)

Table 5: Group use-case execution results

On average 6 use-cases per session were executed, 5 of them successfully.

In summary, the general feedback from participants was that the permanent remote Plugtests for PKI communication would be highly appreciated.

7 Base Specification Validation

7.1 Overview

The ITS security base specifications, ETSI ITS 103 097 V1.3.1 [] and ETSI TS 102 941 V1.3.1 [] were validated during the event and evaluated as sufficient for the ITS deployment. However, some issues were identified during the test sessions.

7.2 ETSI TS 103 097 and IEEE 1609.2 issues

7.2.1 Certificate canonicalization

It was proposed to exclude the canonicalization of public keys and signature of the certificate for the hash calculation. The common conclusion of participants was that the necessity of this approach is not clear. The certificate, once issued, shall be treated as fixed sequence of bytes. This requirement can be removed in the future versions of either IEEE 1609.2 or ETSI TS 103 097 [2].

7.2.2 PsidGroupPermissions of type ‘enrol’ in ETSI architecture

The ETSI TS 103 097 [2] shall clearly specify that including of the PsidGroupPermissions of type ‘enrol’ in the certIssuePermission field of certificate is useless in the ETSI ITS PKI architecture and should be avoided.

7.2.3 Certificate issuing identifier improvement

Link certificate makes the liaison between two self-signed certificates. The link certificate shall be signed using the verification key of the first self-signed certificate, but the content of the link certificate shall be identical to the second self-signed certificate. This means that certificate validation rules of the link certificate are broken if validation restrictions of the second certificate are not inside the validation restriction of the first certificate.

One of proposed solution is to introduce third type of certificate issuer identification using the hash of public key instead of the certificate digest as it is possible for message signing. In this case only the signature validation shall be done to validate the certificate.

7.2.4 Authorization Ticket content recommendations

The specification shall provide recommendations for AT certificate contents. Particularly to avoid inclusion of encryption key when it is not necessary for requested applications.

7.3 ETSI TS 102 941 issues

7.3.1 Message description pictures improvement

Figures 8, 9, 14, 15, 17, 18, 19, 21 shall be improved in order to include the Ts103097-UnsecuredData envelop holding the Ts102941Data structure.

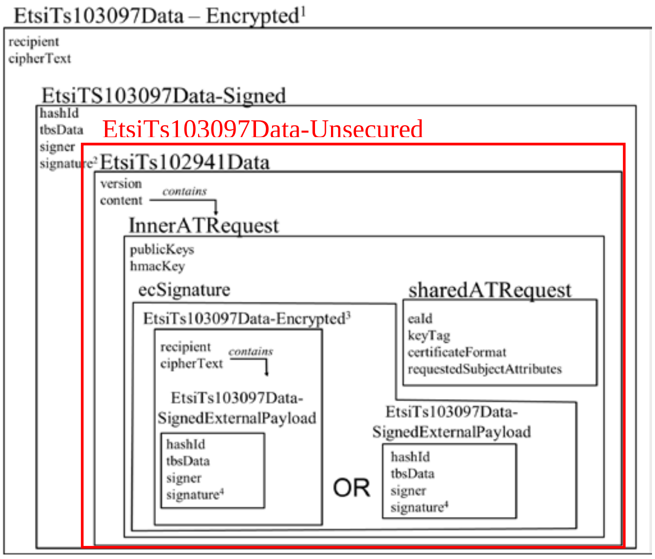


Figure 4: TS102941 Message description improvement

7.3.2 Link certificate description

Link certificate definition is absent in ETSI architecture. It shall be provided either in ETSI TS 102 940 [4] or in ETSI TS 102 941 [3].

7.3.3 Error descriptions and expected error behaviour shall be provided

The ETSI TS 102 941 [3] ASN.1 code contains multiple lists of error codes. These error codes are not mentioned in the text of the specification and no description and no expected behaviour is provided. There are some error-related issues found:

- some Authorization Validation error codes cannot be delivered to the requester using Authorization error codes,
- the CA is unable to answer with encrypted answer if it was unable to decrypt the request and determine the encryption key.

Future work of error handling is necessary in the future version of the protocol.

7.3.4 Handling of repeated initial enrollment requests

Handling of re-enrollment requests shall be better described in the specification.

Particularly, the already enrolled ITS-S shall be able to re-run the enrolment procedure even if the previously received EC certificate was lost on the ITS-S side.

7.3.5 RCA access point URL distribution

This topic is described in the clause 7.4.3 of the present document.

7.4 EU Certificate or Security policy issues

7.4.1 Link certificate role and content

The content and usage of RCA and TLM link certificates shall be better described in the policy.

7.4.3 RCA access point URL distribution

In order to allow the validation of all subordinate certificates, the RCA shall publish the CRL and all entities shall be able to have an access to this CRL information. However, the DC URL of foreign PKI is formally unknown for ITS-Ss enrolled in other PKIs. There are no formal way to ensure that CRL information of each RCA is accessible by all entities enrolled in the single trust domain.

This issue was addressed on the dedicated workshop during the event where four different solutions were discussed:

1. Do not centralize any CRL distribution and let RCAs to contact another RCAs from ECTL and distribute foreign CRLs
2. Collect RCA DC information on the JRC CPOC web site
3. Include RCA access point information in the ECTL
    a. As a DC entry
    b. Add accessPoint URL in the RootCAEntry
4. Distribution through peer-2-peer communication

All these options requires additional investigation, development and standardization efforts.

7.5 The ETSI TS 103 600 Interoperability test specifications issues

The interoperability test specifications contains SSP definitions of type ‘opaque’ instead of ‘bitmapSsp’. CAM and DENM specifications defines the type of SSP as ‘bitmapSsp’.

History

Document history		
V1.1.1		Initial version of the report