TECHNICAL REPORT

3rd ITS Cooperative Mobility Services Plugtest; Essen, Germany; 25 - 29 November 2013 CAM, DENM, GN Interoperability in F2F configuration

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

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

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute yyyy.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Contents 3
Intellectual Property Rights 4
1 Executive Summary 4
2 Introduction 4
2 References 5
3 Abbreviations 5
4 Participants 5
5 Technical and Project Management 7
5.1 Test Plan 7
5.2 Test Scheduling 7
5.3 Test Infrastructure 8
5.3.1 Central Position Server 8
5.3.2 Face 2 Face Configuration 9
5.3.3 PKI Setup 10
5.4 Interoperability Test Procedure 11
5.5 Conformance Validation Framework 11
6 Achieved Interoperability Results 12
6.1 CAM, DENM, GN F2F configuration 12
6.1.1 Results per GN Tests 13
6.1.2 Results per CAM and DENM Tests 14
6.2 Security F2F configuration 14
6.2.1 Results per Security Tests 15
7 Base Specification Validation 16
7.1 GeoNetworking base specification 16
7.2 Security base specification 18
History 22

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.

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 2015. 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 collaboration with ERTICO, has organized the latest in a series of Plugtests™ interoperability events for Intelligent Transport Systems (ITS) Cooperative Systems. This event was held in parallel with the ITS PHY event and was hosted by CETECOM, from 25 to 29 November in Essen, Germany

Participating companies from the automotive sector tested the interoperability of their solutions. In addition they ran tests to assess their compliance with the latest standards developed by the ETSI ITS technical committee. The event also included a workshop on Future Perspectives of Car-to-X Communication, gathering experts from both public and private organizations specializing in ITS technologies and implementations.

2 Introduction

This event aimed to test the interoperability of ITS equipment from all key vendor implementations and to validate4 the base specifications of ITS protocols CAM, DENM and GeoNetworking. The new topics of Security Testing was added to the scope of the interoperability tests.

As in the previous events, conformance testing was conducted in order to allow vendors to assess the level of compliance to ETSI ITS Release 1.

At the end of each day a wrap-up meeting was held to discuss main interoperability points of the day.

A very detailed preparation was required in order to allow for a smooth and efficient test week. The following test tool and equipment providers supported the event:

- COHDA – ITS-G5 Modems for Conformance Test Setup
- VECTOR – Monitoring Tool
- TESTINGTECH – Conformance Test Software
- FRAUNHODER SIT – PKI Setup
- FRAUNHOFER FOKUS – TS103 097 Web Validator

The implementations were connected via a test network to the Central Position Server (CPS) which provide for each test scenario the appropriate GPS feed. The GPS server was provided by ETSI CTI.

ETSI CTI produced a Plugtests guide containing more than 40 interoperability tests. Also, the ETSI CTI interoperability tool suite consisting of WIKI, Scheduling Tool and Test Reporting Tool, was deployed.

More than 500 interoperability tests were executed during the course of this event.

93% of the executed tests indicated interoperability which shows the high level of interoperability and maturity of the ITS technology.

A blog and a press release were produced. They are accessible at http://www.etsi.org/news-events/events/665-plugtests-2013-itscms3?tab=4 and http://www.etsi.org/news-events/news/728-2013-12-press-release-its-interop-event

2 References

The following base specifications were validated in the Plugtest.

[i.1] ETSI EN 302 637-2 v1.3.0: CAM base specification

[i.2] ETSI EN 302 637-3 v1.2.0: DENM base specification

[i.3] ETSI EN 302 636-5-1 v1.1.1: BTP base specification

[i.4] ETSI EN 302 636-4-1 v1.2.0: GN base specification

[i.5] ETSI EN 302 636-6-1 v1.2.0: GN6 base specification

[i.6] ETSI TS 102 894-2 V1.1.1: Common Data Dictionary

[i.7] ETSI TS 103 097 V1.1.1: Security header and certificate formats

3 Abbreviations

CAM	Cooperative Awareness Message
CPS	Central Position Server
DENM	Decentralized Environmental Notification Message
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-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
Test Session	A paring of vendors that test together during a given time slot
TSR	Test Session Report. Report created during a test session

4 Participants

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

Table 1: List of teams

#	Teams
1	AUTOTALKS
2	COMMSIGNIA
3	Cohda /NXP
4	DENSO
5	FRAUNHOFER ESK
6	HITACHI/RENESAS
7	IMTECH
8	ITRI
9	KAPSCH
10	MARBEN
11	NEC
12	QMIC
13	TRIALOG
14	SIEMENS
15	UNEX

The test tool vendors which attended the Plugtests are listed in the table below.

Table 2: List of test tool vendors

#	Test Tool Vendor	Role
1	**Fraunhofer SIT**	PKI Setup for Security Testing
2	**Testing Technologies**	Conformance Validation Framework
3	**Vector Informatik**	Monitoring and Demo Tests

The following FOTs were represented by the companies.

Table 3: List of FOTs

#	Test Tool Vendor
1	**PRESERVE**
2	**DRIVE C2X**
3	**SCORE@F**

5 Technical and Project Management

5.1 Test Plan

The test plan containing 49 CAM, DENM, GN interoperability tests and 8 Security interoperability tests was developed by ETSI CTI together with a team of 3 experts. During the regular conference calls which were held as part of the event preparation, companies could propose additional tests. The tests were grouped in mandatory and optional tests. Refeer to the annex of this document for the link to the test plan.

5.2 Test Scheduling

The preliminary test schedule was developed before the Plugtest and was circulated to all the participants in advance for comments. The initial test schedule allowed for each company to test against a fair number of other companies.. The day was organized in a morning test session from 8.00 to 12.30 and in an afternoon test sessions from 13.30 to 18.00.

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.

The figure below shows the test schedule.

		Radio Bench 1	Radio Bench 2	Security Session 1	Security Session 2	F-2-F Session 1	F-2-F Session 2	Conformance Session 1	Conformance Session 2	RF Test Session 1
Mon 25	13:30-16:00	ITRI ITS-Itri Marben ITS-Marben Siemens ITS-Siemens	Commsignia ITS-Commsignia DENSO ITS-Denso qmic ITS-Qmic	auto-talks ITS-Autotalks Cohda_NXP ITS-CohdaNxp		ESK ITS-Esk hitachi_ren ITS-HitachiRen	Kapsch ITS-Kapsch unex ITS-Unex	NEC ITS-Nec		Kapsch RF-Kapsch
	16:00-18:00	ESK ITS-Esk ITRI ITS-Itri Kapsch ITS-Kapsch	hitachi_ren ITS-HitachiRen Marben ITS-Marben Siemens ITS-Siemens	Cohda_NXP ITS-CohdaNxp Preserve ITS-Preserve	unex ITS-Unex Vector ITS-Vector	Commsignia ITS-Commsignia DENSO ITS-Denso	NEC ITS-Nec qmic ITS-Qmic	auto-talks ITS-Autotalks		qmic RF-Qmic
Tue 26	8:00-10:30	DENSO ITS-Denso imtech ITS-Imtech NEC ITS-Nec	auto-talks ITS-Autotalks Commsignia ITS-Commsignia Kapsch ITS-Kapsch	Cohda_NXP ITS-CohdaNxp hitachi_ren ITS-HitachiRen	Marben ITS-Marben Preserve ITS-Preserve		ESK ITS-Esk unex ITS-Unex	ITRI ITS-Itri	qmic ITS-Qmic	Siemens RF-Siemens
	10:30-12:30	DENSO ITS-Denso ESK ITS-Esk unex ITS-Unex	imtech ITS-Imtech Marben ITS-Marben qmic ITS-Qmic	Cohda_NXP ITS-CohdaNxp Kapsch ITS-Kapsch	NEC ITS-Nec Preserve ITS-Preserve		auto-talks ITS-Autotalks Siemens ITS-Siemens	hitachi_ren ITS-HitachiRen	ITRI ITS-Itri	Commsignia RF-Commsignia
	13:30-16:00	Cohda_NXP ITS-CohdaNxp Siemens ITS-Siemens	auto-talks ITS-Autotalks hitachi_ren ITS-HitachiRen ITRI ITS-Itri	auto-talks ITS-Autotalks NEC ITS-Nec	imtech ITS-Imtech Vector ITS-Vector	DENSO ITS-Denso ESK ITS-Esk	Kapsch ITS-Kapsch Marben ITS-Marben	unex ITS-Unex	Commsignia ITS-Commsignia	ITRI RF-Itri
	16:00-18:00	auto-talks ITS-Autotalks ESK ITS-Esk NEC ITS-Nec	imtech ITS-Imtech Kapsch ITS-Kapsch qmic ITS-Qmic	Cohda_NXP ITS-CohdaNxp Siemens ITS-Siemens	ITRI ITS-Itri Preserve ITS-Preserve	DENSO ITS-Denso	Commsignia ITS-Commsignia Marben ITS-Marben			unex RF-Unex
Wed 27	8:00-10:30	Cohda_NXP ITS-CohdaNxp ESK ITS-Esk imtech ITS-Imtech	Commsignia ITS-Commsignia DENSO ITS-Denso unex ITS-Unex	Marben ITS-Marben Vector ITS-Vector	Kapsch ITS-Kapsch Preserve ITS-Preserve	NEC ITS-Nec	hitachi_ren ITS-HitachiRen qmic ITS-Qmic	Siemens ITS-Siemens		hitachi_ren RF-Hitachi_Ren
	10:30-12:30	Cohda_NXP ITS-CohdaNxp qmic ITS-Qmic unex ITS-Unex	hitachi_ren ITS-HitachiRen ITRI ITS-Itri Siemens ITS-Siemens	imtech ITS-Imtech Preserve ITS-Preserve	ESK ITS-Esk Vector ITS-Vector	DENSO ITS-Denso Marben ITS-Marben	auto-talks ITS-Autotalks Commsignia ITS-Commsignia	Kapsch ITS-Kapsch		Cohda_NXP RF-CohdaNxp
	13:30-16:00	Commsignia ITS-Commsignia Cohda_NXP ITS-CohdaNxp Kapsch ITS-Kapsch	ITRI ITS-Itri NEC ITS-Nec unex ITS-Unex	Siemens ITS-Siemens Vector ITS-Vector	hitachi_ren ITS-HitachiRen Preserve ITS-Preserve	DENSO ITS-Denso imtech ITS-Imtech	ESK ITS-Esk qmic ITS-Qmic	hitachi_ren ITS-HitachiRen	Marben ITS-Marben	
	16:00-18:00	Cohda_NXP ITS-CohdaNxp ITRI ITS-Itri Marben ITS-Marben	auto-talks ITS-Autotalks Commsignia ITS-Commsignia qmic ITS-Qmic	Preserve ITS-Preserve unex ITS-Unex	ESK ITS-Esk imtech ITS-Imtech	DENSO ITS-Denso Siemens ITS-Siemens	hitachi_ren ITS-HitachiRen NEC ITS-Nec			auto-talks RF-Autotalks
Thu 28	8:00-10:30	Cohda_NXP ITS-CohdaNxp DENSO ITS-Denso hitachi_ren ITS-HitachiRen	ESK ITS-Esk Marben ITS-Marben NEC ITS-Nec	Preserve ITS-Preserve Vector ITS-Vector	auto-talks ITS-Autotalks Kapsch ITS-Kapsch		Commsignia ITS-Commsignia ITRI ITS-Itri	qmic ITS-Qmic		imtech RF-Imtech
	10:30-12:30	hitachi_ren ITS-HitachiRen Kapsch ITS-Kapsch unex ITS-Unex	Commsignia ITS-Commsignia imtech ITS-Imtech Siemens ITS-Siemens	Preserve ITS-Preserve	ITRI ITS-Itri NEC ITS-Nec	auto-talks ITS-Autotalks DENSO ITS-Denso	Cohda_NXP ITS-CohdaNxp Marben ITS-Marben	ESK ITS-Esk		qmic RF-Qmic
	13:30-16:00	auto-talks ITS-Autotalks Cohda_NXP ITS-CohdaNxp NordSys ITS-Nordsys	ESK ITS-Esk ITRI ITS-Itri qmic ITS-Qmic	hitachi_ren ITS-HitachiRen Vector ITS-Vector	imtech ITS-Imtech Marben ITS-Marben	Siemens ITS-Siemens unex ITS-Unex	Commsignia ITS-Commsignia Kapsch ITS-Kapsch	DENSO ITS-Denso		
	16:00-18:00	DENSO ITS-Denso Kapsch ITS-Kapsch Marben ITS-Marben	hitachi_ren ITS-HitachiRen NEC ITS-Nec unex ITS-Unex	auto-talks ITS-Autotalks Preserve ITS-Preserve	imtech ITS-Imtech Siemens ITS-Siemens	auto-talks ITS-Autotalks ITRI ITS-Itri	ESK ITS-Esk NordSys ITS-Nordsys	Cohda_NXP ITS-CohdaNxp		
Fri 29	8:00-10:30	Cohda_NXP ITS-CohdaNxp NEC ITS-Nec qmic ITS-Qmic	DENSO ITS-Denso hitachi_ren ITS-HitachiRen Kapsch ITS-Kapsch	ITRI ITS-Itri Vector ITS-Vector	auto-talks ITS-Autotalks unex ITS-Unex	Marben ITS-Marben Siemens ITS-Siemens	Commsignia ITS-Commsignia ESK ITS-Esk			
	10:30-12:30	auto-talks ITS-Autotalks Siemens ITS-Siemens unex ITS-Unex	Commsignia ITS-Commsignia ESK ITS-Esk ITRI ITS-Itri	Cohda_NXP ITS-CohdaNxp Vector ITS-Vector	hitachi_ren ITS-HitachiRen Kapsch ITS-Kapsch	Marben ITS-Marben	DENSO ITS-Denso qmic ITS-Qmic			

Figure 1: Test Schedule

5.3 Test Infrastructure

5.3.1 Central Position Server

The CPS provided an appropriate GPS feed for each test scenario. Each vendor connected to the CPS. The CPS was provided by ETSI CTI.

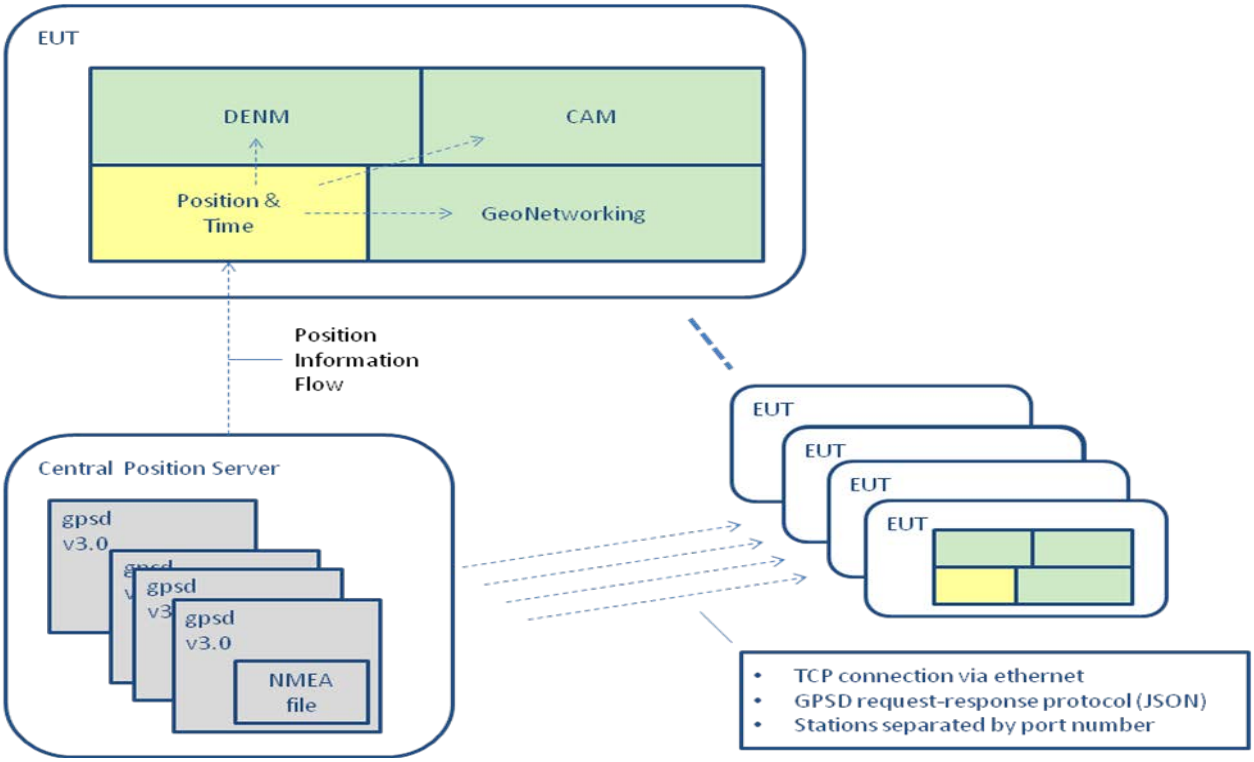

Figure 2: Central Position Server

5.3.2 Face 2 Face Configuration

The face 2 face configuration was the basic configuration used for the majority of the test. It was important to use radio cables and not to do OTA tests as there were multiple test sessions running in parallel. Each vendor had to bring its own attenuators and radio cables. CETECOM helped with additional equipment when needed.

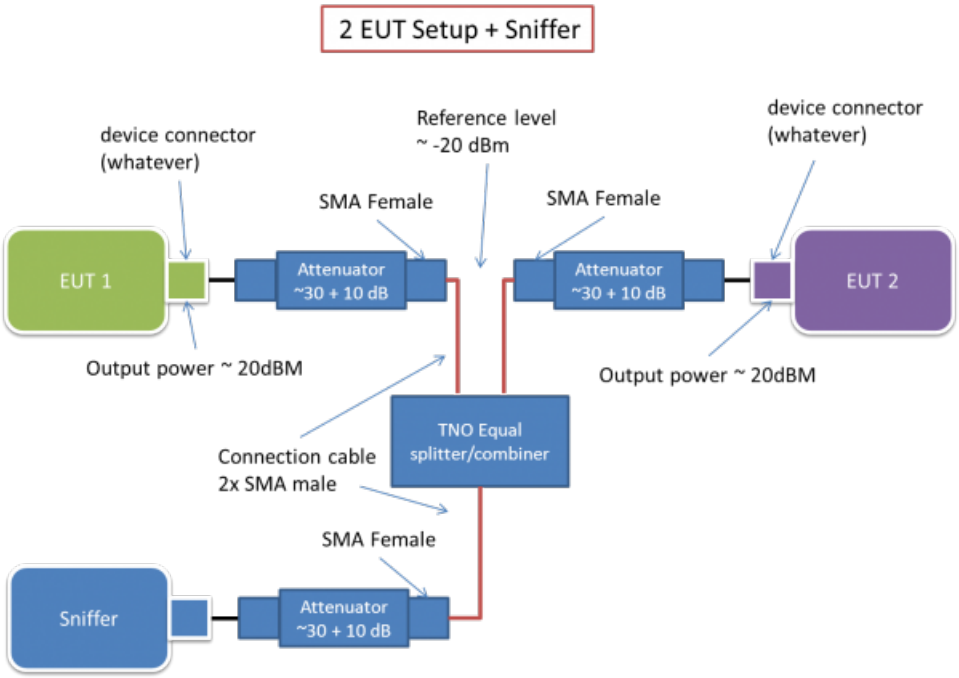

Figure 3: Face 2 Face Configuration

5.3.3 PKI Setup

The PKI setup was created for the Plugtest only by Fraunhofer SIT. Consequently, the root certificate and CA certificates were not used for other purposes. The PKI setup consisted of the following CAs as shown in the figure:

- Trusted and untrusted Root CA
- Trusted and untrusted AA

Certificates to perform positive and negative tests were created. All provided certificates follow the specifications of ETSI TS 103 097 v.1.1.1 and contain the following elements:

- One uncompressed verification key and one encryption key
- One assurance level that contains the maximum value 7 = 0xE0 according to the revised version of ETSI TS 103 097 v.1.1.1
- One validity restriction of type "time_start_and_end". The validity of the root and the AA cert will be defined for one year.
    - Start time = 01.01.2013 UTC
    - End time = 31.12.2013 UTC
- One signer info is included of type "certificate_digest_with_ecdsap256" or "certificate"
- One validity restriction of type "region" with a geographic region of type "none"

The AT certs in the table below follow the specifications of the revised version of ETSI TS 103 097 v.1.1.1 and contain in general the following elements:

- One assurance level that contains the maximum value 7 = 0xE0 according to ETSI TS 103 097 v.1.1.1
- One ITS-AID-SSP list with two entries:
    - AID = 16512 (CAM processor) according to ETSI TR 102 965 v 0.1.0 and SSP = 0
    - AID = 16513 (DENM processor) according to ETSI TR 102 965 v 0.1.0 and SSP = 0
- One validity restriction of type "time_start_and_end". The validity of the root and the AA cert will be defined for one year.
    - Start time = 01.08.2013 UTC
    - End time = 29.12.2013 UTC
- One signer info is included of type "certificate_digest_with_ecdsap256"

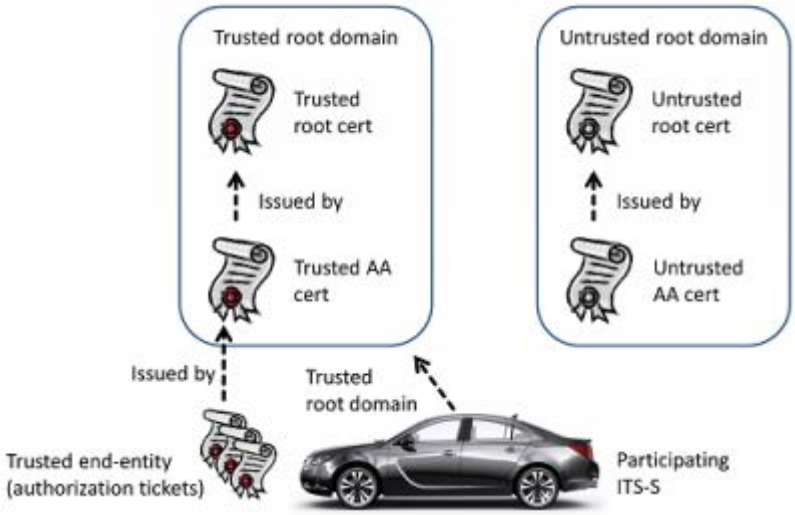

Figure 4: PKI Setup

5.4 Interoperability Test Procedure

Each test was executed in the same manner as listed below:

1) Connect two or three devices from different vendors

2) Check connectivity between devices

3) Perform tests according to Plugtest Guide

4) Check if devices can send/receive frames from each other

5) Check if data is handled correctly in the network and facility layers

6) Check if implemented algorithms work correctly

7) Result determination and reporting

8) Result OK: run next test

9) Result NOK: check monitor tools to identify source of error

10) Report results in ETSI Test Reporting Tool

11) Once all tests executed swap receiver / sender roles and run all tests again

5.5 Conformance Validation Framework

The ETSI ITS Conformance Validation Framework is available at http://forge.etsi.org/websvn/listing.php?repname=ITS.ITS&path=/tags/v1.2.1/ and can be used to assess the compliance of implementations with the ETSI standards. The development of test suites and test systems are part of the ETSI Test Methodology. With its high degree of flexibility, it can be also used for company internal testing.

At the Plugtests, the conformance tests have been executed based on the TTCN-3 environment, provided by Testing Technologies, and the ITS-G5 modems provided by Cohda Wireless.

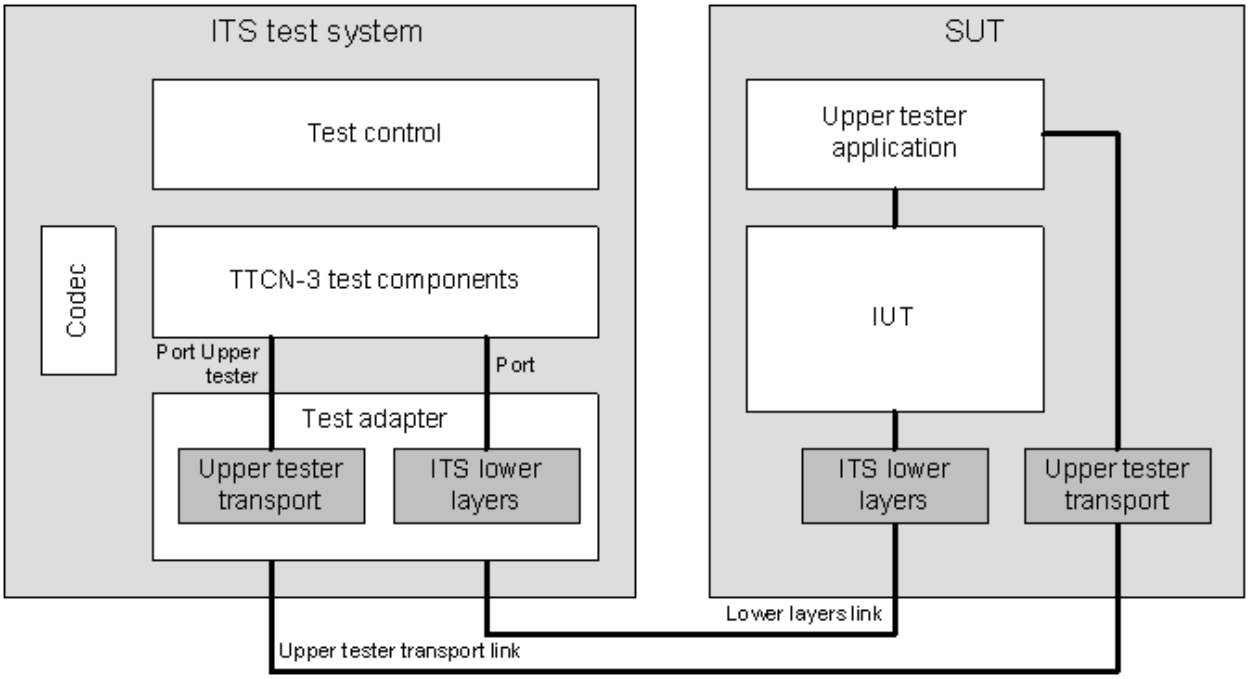

Figure 5: Conformance Validation Framework

6 Achieved Interoperability Results

6.1 CAM, DENM, GN F2F configuration

This clause presents the achieved interoperability results of the tests executed in the F2F configuration. 14 different devices (DUT) attended the tests. The following base specifications were validated:

- CAM base specification (EN 302637-2 v1.3.0)
- DENM base specification (EN 302637-3 v1.2.0)
- Common Data Dictionary (TS 102 894-2 V1.1.1)
- GN base specification (EN 302636-4-1 v1.2.0)

There were 6 CAM, 3 DENM, 11 GN mandatory tests, and 2 CAM, 2 DENM, 13 GN optional tests.

GN6 tests were available, but were not run. The reason being that GN6 is not relevant for Day 1 deployment.

Test activities contributed to the base spec validation by identifying ~ 10 GeoNetworking base spec issues.

The achieved results show that all implementations have been compatible on a basic level, i.e. sent data could be decoded and interpreted properly by receivers. Furthermore the vast majority of equipment performed well on the physical layer.

The table below provides the overall result. The PASS rate (Executed - OK) of ~93 % does not show a significant improvement compared with last Plugtest in 2012. However, since the last Plugtest various base spec changes were applied and thus results are not really comparable. The execution rate of ~49% is low. Out of Time (OT) is the main reason for not executed tests. This is an indicator that the 2 hr time slots were probably too short.

Table 4: Results Overview for CAM, DENM, GN in F2F configuration

Executed		Not Executed		Totals
OK	NO	NA	OT	Run
513 (93.1%)	38 (6.9%)	167 (14.9%)	404 (36.0%)	551 (49.1%)

6.1.1 Results per GN Tests

The table below provides the GN test results. As a summuary it can be said that the results of basic GN features are very good, and that advanced GN features need more testing.

- GN_DAD_01 Duplicate Address Detection: The issues discovered with this were that it was not clear if MAC address needs to change as well. Also, DAD detection in multi hop does not work and in the wrap-up sessions it was proposed to limit DAD only to SHB and Beacon. DAD detection in multi hop should be handled by Security.
- GN_GUC_01 Unicast: The main interop issues were issues with MAC layer unicast handling
- TD_GN_GBC_FW_02 GeoBroadcast Forwarding: Some vendors did not buffer the packets correctly. Also, MAC layer interop issues, as well as issues with nextHop detection were observed.
- TD_GN_GBC_SCF_XX Store Carry &Forward: The base spec described this feature in an ambiguous way and hence different interpretations of SCF procedure were implemented.
- Duplicate Packet Detection: An issue was discovered in the case where several consecutive SHB packets, containing different data, are discarded on the basis of the same timestamp. Another issue was reply attacks. To protect against replay attacks, the security header processing itself should be doing the timestamp check.

Table 5: Results per GN test

	Executed		Not Executed		Total
Test ID	OK	NO	NA	OT	Run
TD_GN_BEA_01	50 (100.0%)	0 (0.0%)	1 (2.0%)	0 (0.0%)	50 (98.0%)
TD_GN_SHB_01	50 (100.0%)	0 (0.0%)	1 (2.0%)	0 (0.0%)	50 (98.0%)
TD_GN_DAD_01	31 (79.5%)	8 (20.5%)	8 (15.7%)	4 (7.8%)	39 (76.5%)
TD_GN_GUC_01	14 (87.5%)	2 (12.5%)	19 (37.3%)	16 (31.4%)	16 (31.4%)
TD_GN_GBC_01	46 (100.0%)	0 (0.0%)	1 (2.0%)	4 (7.8%)	46 (90.2%)
TD_GN_GBC_03	42 (100.0%)	0 (0.0%)	1 (2.0%)	8 (15.7%)	42 (82.4%)
TD_GN_GBC_FW_02	27 (77.1%)	8 (22.9%)	1 (2.0%)	15 (29.4%)	35 (68.6%)
TD_GN_GBC_SCF_03	8 (53.3%)	7 (46.7%)	5 (9.8%)	31 (60.8%)	15 (29.4%)
TD_GN_GBC_SCF_04	5 (62.5%)	3 (37.5%)	6 (11.8%)	37 (72.5%)	8 (15.7%)
TD_GN_GBC_FW_03	33 (97.1%)	1 (2.9%)	1 (2.0%)	16 (31.4%)	34 (66.7%)
TD_GN_GBC_SCF_02	8 (80.0%)	2 (20.0%)	6 (11.8%)	35 (68.6%)	10 (19.6%)
TD_GN_GBC_05	11 (100.0%)	0 (0.0%)	6 (11.8%)	34 (66.7%)	11 (21.6%)
TD_GN_GBC_06	11 (100.0%)	0 (0.0%)	6 (11.8%)	34 (66.7%)	11 (21.6%)

6.1.2 Results per CAM and DENM Tests

The tables below show the results of the CAM and DENM tests. The PASS rates of teh tests are satisfying. However, it must be stated that teh execution rate is too low. Probably this is due to the fact that many test activities were scheduled during the week and time slots were too short.

Table 6: Results per CAM test

	Executed		Not Executed		Total
Test ID	**OK**	NO	**NA**	OT	Run
TD_CAM_05	**42 (97.7%)**	1 (2.3%)	**4 (7.8%)**	4 (7.8%)	43 (84.3%)
TD_CAM_06	**24 (100.0%)**	0 (0.0%)	**5 (9.8%)**	**22 (43.1%)**	24 (47.1%)
TD_CAM_07	**4 (100.0%)**	0 (0.0%)	18 (35.3%)	**29 (56.9%)**	4 (7.8%)
TD_CAM_08	**29 (100.0%)**	0 (0.0%)	**7 (13.7%)**	**15 (29.4%)**	29 (56.9%)
TD_CAM_09	**21 (100.0%)**	0 (0.0%)	14 (27.5%)	**16 (31.4%)**	21 (41.2%)
TD_CAM_10	**20 (90.9%)**	2 (9.1%)	14 (27.5%)	**15 (29.4%)**	22 (43.1%)
TD_CAM_11	**19 (100.0%)**	0 (0.0%)	14 (27.5%)	**18 (35.3%)**	19 (37.3%)
TD_CAM_12	**15 (83.3%)**	3 (16.7%)	14 (27.5%)	**19 (37.3%)**	18 (35.3%)

Table 7: Results per DENM test

	Executed		Not Executed		Total
Test ID	**OK**	NO	**NA**	OT	Run
TD_DENM_05	3 (75.0%)	1 (25.0%)	15 (29.4%)	**32 (62.7%)**	4 (7.8%)

Figure 6: Results Overview for DENM in F2F configuration

6.2 Security F2F configuration

This clause presents the achieved interoperability results of the tests executed in the F2F configuration. 12 different devices (DUT) attended the tests. A test spec with 8 tests based on revised ETSI TS 103 097 v1.1.1 was provided, containing 1 mandatory and 7 optional tests with security applied on GN level. The PKI setup was provided by Fraunhofer SIT.

A pre-validation of secure Messages and certificates was conducted prior to the event. The tool called "TS 103 097 Web Validator" was provided by Fraunhofer FOKUS. It is available at https://werkzeug.dcaiti.tu-berlin.de/etsi/ts103097/

Test activities contributed to the validation of ETSI TS 103 097 v1.1.1 by identifying ~ 20 issues.

The overall results of the Security tests are shown in the table below. For a first plugtest the PASS rate (Executed - OK) of ~85 % is better than expected. The execution rate of ~43 % is low, but normal for a first Plugtest. However, for a next Plugtest more optional tests should be supported by the DUTs. An industry profile such as a C2C CC Profile could help to identify the applicable features to be tested.

Table 8: Results Overview for Security Tests in F2F configuration

Executed		Total Tests	
OK	NO	NA	Run
190 (85.6%)	32 (14.4%)	290 (56.6%)	222 (43.4%)

6.2.1 Results per Security Tests

The table below lists the results per test. The following issues were experienced:

- Testing the request of unrecognized certificates from communication neighbor has been identified to be challenging since high CAM frequency was required
- Unspecific base spec with respect to request of unrecognized certificates caused some not successful tests, e.g. results of TD_SEC_13 and e.g. results of TD_SEC_20
- Faulty implementations caused some not successful tests, e.g. results of TD_SEC_51

Table 9: Results per Security Test

Test Id	OK	NO
TD_SEC_11	56 (94.9%)	3 (5.1%)
TD_SEC_12	18 (78.3%)	5 (21.7%)
TD_SEC_13	11 (50.0%)	11 (50.0%)
TD_SEC_14	34 (91.9%)	3 (8.1%)
TD_SEC_20	10 (76.9%)	3 (23.1%)
TD_SEC_40	40 (95.2%)	2 (4.8%)
TD_SEC_51	10 (66.7%)	5 (33.3%)
TD_SEC_53	11 (100.0%)	0 (0.0%)

7 Base Specification Validation

7.1 GeoNetworking base specification

The table below lists the discovered base spec issues of ETSI EN 302 636-4-1 v1.2.0.

Table 10: Discovered base spec issues

Item	Reference	Issue Description	Corrective Proposal
Timestamp	Leap seconds	TAI == GPS (different epoch) UTC = TAI + sync to earth rotation POSIX = UTC transalated into a number (single integer) except for leap seconds 1) If your time source is UTC based (POSIX timestamp, windows time, etc), you'll have to add leap seconds in 2005, 2008, 2012 (3 seconds at the moment) and all future ones. T-ITS = Tcur - Tepoch + Tleap, where Tepoch = 1072915200 sec,Tleap=3 2) If your time source is a monotonic time counter (GPS time for example) you don't need to add leap seconds, but the Epoch timestamp must correspond to the UTC Time. T-ITS = Tgps - Tepoch, where Tepoch = 757382413 (including 13 sec correction for 01/01/2014 UTC)	Remove the acronym TAI from spec. TAI is not defined as integer value, it is a time standard in the same form as UTC. It should be mentioned that leap seconds are not taken into account. A clarifying example could be added in the standard.
Timestamp	Source	In the Gn protocol the TST field timestamps the acquisition of position coordinate, and therefore it should change in accordance with the periodicity of position updates.	The special case of stationary roadside unit must be clarified with respect to timestamp generation. See note in clause 7.2.3
packet data rate control	Annex B.2	weight factor (0 < β < 1), set to 0,5. This value seems to low	To set β value at least to 0,9
DAD duplicate address detection	Section 9.2.1.2	Phrasing could be clearer on exact procdure of modes, ie it reads that in AUTO mode DAD is not possible. Is this wanted?	make a note in DAD section to say that DAD only works for non-AUTO mode
DAD duplicate address detection	Section 9.2	when DAD happens and GN address changes. Should MAC address change as well?	add note to say 'when GN @ changes, then MAC @ change accordingly' add note that anonymous is used for security
PAI bit		Position Accuracy indicator. Vendors use different settings (nextHop selection difficult).	For plugtest set it to 1
Duplicate Packet	Test TD_GN_GBC_04	Source operation defines to create packet, and conditions to buffer. There is a missing step to say that SOPV needs to be updated before flushing the source buffer	define what happens when flushing the buffer, ie which fields need to be updated
DAD duplicate address detection in multi hop		In multi hop scenarios DAD does not work	Limit DAD only for SHB and beacon. For secured packets, Security should handle DAD, ie to check: was this message signed by me?
SCF		Different interpretations on how SCF shall work	Make clearer wording for source and forward processing, as well as for'no neighbour' and' no suitable neighbour'
DPD in single hop		According to the current Gn standard, single hop DPD is done on the basis of timestamp information (there is no sequence number). This is problematic, because there could be several consecutive SHB packets, containing different data, which are then discarded on the basis of same timestamp. (see above the timestamp updating comment) Current profile defines 10Hz. This is not high enough update rate. 10Hz CAM + TOPO + SPAT you sen dwith more than 10Hz. In SEC the timestamp is in microsec and it is the genrationTime of the message.	DPD must not be done on single hop broadcast; corresponding clauses are to be removed. To protect against replay attacks, the security header processing itself must be doing the timestamp check

Gn repetition	I.2	Is there a consensus that packet repetition procedure is not needed at all in a networking standard? RSU whichs generates POI messages and does not change the contents. Using GN rep would simplify the implementation of the Facility layer	all vendors agree that GN repetition is not needed. However, th\is feature is optional and hence no change required
granularity of CBF algo		if position delta between 2 forwarders is too small, then the CBF timer differences becomes too short.	TC ITS should define the granularity in which the CBF algorithm can work

SCF correction		a) The check of SCF (step 2 in 9.3.8.2) should either be done in step 4) (after next hop determination) or it should be done directly in the algorithm in annex D + E.
		`Actual algo:`
		`ADD P TO B`
		`SET NH_LL_ADDR ← 0 # Indicates that packet is buffered`
		
		`New proposed algo:`
		`IF (SCF == 1) THEN`
		`  ADD P TO B`
		`  SET NH_LL_ADDR ← 0 # Indicates that packet is buffered`
		`ELSE`
		`  SET NH_LL_ADDR ← BCAST`
		`ENDIF`	

Problem with flushing SO UC forwarding buffer -	9.3.10.3 step 9)	buffers are only flushed if destination becomes a neighbour. But the case, where a neighbor appears and could be a suitable nextHop for another destination Dx, is not described. And hence Dx UC buffer is never flushed! Conformance test TP/GEONW/PON/FPB/BV-02 is at the moment no longer valid, but reflects a real situation to be tested.	Update the base spec
forwarder operation to be restructured	9.3.8.3	in this chapter there is a mix up of loctable update and message update. None of the IUTs passed the tests on DEPV update in the message because of the unclear oder of notes.	Update the base spec
SOPV		SOPV is contained now in all extend header types, and in source/forwarder operastions each time the SOPV processing is duplicated with slight differences. Moving SOPV in common header would allow to have a single clause on CommonHeader Processing.	add SOPV to common header

7.2 Security base specification

The table below lists the discovered base spec issues of ETSI TS 103 097 V1.1.1: Security header and certificate formats.

Table 11: Discovered base spec issues

Item	Reference	Issue Description	Corrective Proposal
Signer Info		Signer info type certificate_chain in the security header field signer_info should be allowed	Correct in base spec
arbitrary AIDs and SSPs		Root CA cert and AA cert contain no element of type its_aid_list indicating that the CAs are permitted to issue certificates with arbitrary AIDs and SSPs	rethink if CA certs should contain its_aid_list. This would mean that for each new AID a complete set of CA certs would have to be created and deployed The revised standard specification introduces a new problem. A receiver is not able to check if the AA was allowed to issue certificates with a service specific permission (e.g. emergency vehicle). This has to be discussed again
EccPointType = x_coordinate_only		Certificates with EccPointType = x_coordinate_only shall not be supported	Instead of 'should', it must be 'shall' to make it a requirement
region_identifier		The type Int16 of the element region_identifier is not defined in TS 103 097 v1.1.1	For the ETSI security plug tests this type is interpreted as uint16
its_aid_ssp_list		AT certs shall contain its_aid_ssp_list instead of its_aid_list	Correct in base spec
AIDs		AID = 16512 (CAM processor) and AID = 16513 (DENM processor) are taken from ETSI TR 102 965. There is TS 102 942 which defines that AIDs shall follow the format defined in 1609.2; and 1609.2 does not define a value	The values 16512 and 16513 are used for the security plug test
DENM security Profile	7.2	Add refernce to ITSPduHeader or CDD similar to how it was done in chapter 7.1	Correct in base spec
Security profiles		Security profiles required for GEO-NET beacon messages and location services	Correct in base spec
field digests<var> in the structure of request_unrecognized_certificate	Page 27	On page 27 of TS 103 097 the "The HeaderField element request_unrecognized_certificate shall be included if an ITS-S received CAMs from other ITS-Ss, which the ITS-S has never encountered before and which included only a signer_info field of type certificate_digest_with_ecdsap256 instead of a signer_info TrailerField of type certificate. In this case, the signature of the received CAMs cannot be verified because the verification key is missing. The field digests<var> in the structure of request_unrecognized_certificate shall be filled with a list of HashedId3 elements of the missing ITS-S certificates. " An unauthorised sender may poison all neighbours to send the Header Field request unrecognized certificate. This is very serious, because anyone is able to force all vehicles to send an unlimited size list of HashedId3s.	The list has to be limited in size and additionally it is not specified how long to append the request unrecognized certificates. Sender shall only request once for unrecognized certs after that unknown certID is received. Many problems may be mitigated by clever implementations. Maybe, we should add an informative section to the standard which gives hints how to implement this mechanism in a way, that it is not that easy to misuse it? A list of potential problems should be prepared. - If a ITS-S requests only an AA certificate then the receivers should

			check if other neighbors have already answered with a chain containing the AA cert then the receiver could omit sending its own certificate chain containing the requested AA cert.
Epoch Time	Page 14	The epoch time for time32 and time64 differs from all other ITS standards around the globe.	It shall be aligned to 1.1.2004. Ideally a reference to the common data dictionary standard is made
TAI		TAI == GPS (different epoch) UTC = TAI + sync to earth rotation POSIX = UTC transalated into a number (single integer) execpt for leap seconds 1) If your time source is UTC based (POSIX timestamp, windows time, etc), you'll have to add leap seconds in 2005, 2008, 2012 (3 seconds at the moment) and all future ones. T-ITS = Tcur - Tepoch + Tleap, where Tepoch = 1072915200 sec,Tleap=3 2) If your time source is a monotonic time counter (GPS time for example) you don't need to add leap seconds, but the Epoch timestamp must correspond to the UTC Time. T-ITS = Tgps - Tepoch, where Tepoch = 757382413 (including 13 sec correction for 01/01/2014 UTC)	Remove the acronym TAI from spec. TAI is not defined as integer value, it is a time standard in the same form as UTC. It should be mentioned that leap seconds are not taken into account. A clarifying example could be added in the standard.
Version Number		Currently there is no chance to distinguish between an TS 103 097 secured message / certificate and an IEEE 1609.2-2006 secured message /certificate, because both use version number 1. If we go for version number 2, we'll have again no chance to distinguish between TS 103 097 1.2.1 and IEEE 1609.2-2013.	Even if no one is going to mix 1609.2 with European standards, there is absolutely no need to intentionally use the same version number. We could go for a number that is very different, e.g. starting to count from 128 upwards
Longitude		There is a small bug to coorect range of longitude from 1 800 000 000 to -1 799 999 999	Correct in base spec
DAD and DPD		Countermeasures for DAD and DPD issues have to be specified	
Unrecognized certificate		Request of unrecognized certificates has to be specified in more detail	

8 Feedback on organizational issues

8.1 Review of organizational issues from Plugtest#2

- There was an important ramp up time of 2 days. For a next event the ramp up time should be reduced.

- For a next event it is recommended to propose to newcomers and prototype implementations to pre test 2 – 3 days before the start of the Plugtests, in order to bring them to the same stage of interoperability level.
  Pre testing was not done in Plugtests#3. And the ramp up tiem was again at least 2 days. See chapter 8.2 for more details.

- The prototype implementations from this event should run in a next event all mandatory tests in the face 2 face as well as in the radio bench configurations. **This was not achieved in Plugtests#3 because the base sopecifications had changed too much.**

- The test infrastructure worked well. However optimizations can be done, especially in the following fields:

  - For a next event it is recommended to provide more wireshark monitoring support for the face 2 face configurations. **This was realized in Plugtests#3 with the support from VECTOR monitoring stations.**

8.2 Organizational issues from Plugtest#3

- There was a lot of interest for Security tests. The fact that 12 DUTs had security implemented exceeded the expectation (3 – 4 DUTs initially planned). This high number of DUTs would justify a Plugtest dedicated on Security only.

- The TS 103 097 Web Validator provided by Fraunhofer FOKUS was essential for pre testing prior to the event, and has shown that more Conformance tests are needed to preprare better for a next event.

- It would be benfical to improve the ramp-up time of the plugtest. Changes to the format of the Plugtest coud be

  - New format of Plugtest with first 2 days Conformance Testing only
  - Extended Validation activities at ETSI in preparation of next Plugtest
  - More rigorous compliance self- assessment by vendors before a Plugtest
  - Variable time slots during the week (e.g. Extra setup/adaptation time slots of 30 minutes between the test slots could be helpful in the first days)
  - To make setup part on Monday is mandatory for all

- In general the execution rate of test was too low. Probably this is due to the fact that many test activities were scheduled during the week and time slot was too short. To eb able to have longer time slots, less topics should be included in a Plugtest. Itwas discussed whether to run two Plugtests per year with smaller scopes, rather than having one big event.

History

Document history		
V001	9.01.2014	First draft