PREparing SEcuRe VEhicle-to-X Communication Systems

Deliverable 3.3

Joined FOT Trial Results

Project:	PRESERVE
Project Number:	IST-269994
Deliverable:	D3.3
Title:	Joined FOT Trial Results
Version:	v1.0
Confidentiality:	Public
Editors:	Norbert Bißmeyer
Cont. Authors:	Norbert Bißmeyer, Frank Kargl
Date:	2015-06-25

Part of the Seventh Framework Programme

Funded by the EC - DG INFSO

Document History

Version	Status	Author	Date
0.1	Initial structure of document created	Norbert Bißmeyer (FhG SIT)	2015-04-01
0.2	Content of section 2 added	Norbert Bißmeyer (FhG SIT)	2015-04-29
0.3	Test Scenarios added	Norbert Bißmeyer (FhG SIT)	2015-05-14
0.9	Version prepared for review	Norbert Bißmeyer (FhG SIT)	2015-06-10
1.0	Final version	Norbert Bißmeyer (FhG SIT)	2015-06-25

Approval		
	Name	**Date**
Prepared	All Project Partners	2015-05-22
Reviewed	All Project Partners	2015-06-10
Authorised	All Project Partners	2015-06-30

Circulation	
Recipient	**Date of submission**
Project partners	2015-05-22
European Commission	2015-06-30

Glossary and Abbreviations

Abbreviation	Synonyms	Description	Details
API		Application Programming Interface	
CA		Certificate Authority	
CAM		Cooperative Awareness Message	CAMs are sent from vehicles, multiple times a second (typically up to 10 Hz), broadcast over a single-hop connection, and unencrypted and so receivable by any appropriate receiver within range. They contain the vehicle's current position and speed, along with information such as steering wheel orientation, brake state, and vehicle length and width.
DENM	DNM	Decentralized environmental Notification Message	A DENM transmission is triggered by a cooperative road hazard warning use case to provide information about a specific driving environment event or traffic event to other ITS stations. The ITS station that receives the DENM is able to provide appropriate HMI information to the end user, who makes use of these information or takes actions in its driving and traveling.
ECC		Elliptic Curve Cryptography	
FOT		Field Operational Test	
G5A		ITS road safety communication (802.11p)	Frequency band between 5.875 GHz and 5.905 GHz - reserved for ITS road safety communication
G5B		ITS non-safety communication (802.11p)	Frequency band between 5.855 GHz and 5.875 GHz - reserved for ITS road safety communication
G5C	C-WLAN	5GHz WLAN communication (802.11a)	
GNSS	GPS	Global navigation satellite system	Generic term for an Global navigation satellite system (GPS, GLONAS, Galileo)
HSM		Hardware Security Module	
I2V	I2C	Infrastructure-to-Vehicle	Communication between

			infrastructure components like roadside units and vehicles
I2I		Infrastructure-to-Infrastructure	Communication between multiple infrastructure components like roadside units
ITS		Intelligent Transportation Systems	Intelligent Transport Systems (ITS) are systems to support transportation of goods and humans with information and communication technologies in order to efficiently and safely use the transport infrastructure and transport means (cars, trains, planes, ships).
ITS-S		ITS Station	Generic term for any ITS station like vehicle station, roadside unit, ...
LTC		Long Term Certificate	PRESERVE realization of an ETSI Enrolment Credential
LTCA		Long Term Certificate Authority	PRESERVE realization of an ETSI Enrolment Credential Authority
OBU	IVS	On-board Unit	
PC		Pseudonym Certificate	
PCA		Pseudonym Certificate Authority	Instance that issues pseudonym certificates
PKI		Public Key Infrastructure	
UTC		Universal Time Coordinated	
V2I	C2I	Vehicle to Infrastructure	Direct vehicle to roadside infrastructure communication using a wireless local area network
V2V	C2C	Vehicle to Vehicle	Direct vehicle(s) to vehicle(s) communication using a wireless local area network
V2X	C2X	Vehicle-to-Vehicle (V2V) and /or Vehicle-to-Infrastructure (V2I)	
VSS		Vehicle Security Subsystem	Close-to-market implementation of the PRESERVE VSA

Table of Contents

List of Figures

List of Tables

1 Introduction

This deliverable aims to provide the evaluation results of joined trials and the integration of the V2X Security Subsystem (VSS) to an environment with different ITS security implementations that communicate with each other. Usually in a large Field Operational Test (FOT) with several companies from different areas, i.e. OEMs, suppliers, roadside infrastructure, etc., this environment is given. However, to test the functionality of security mechanisms and their interoperability with other implementations it is crucial having as many different relevant implementers as possible. The ETSI ITS Cooperative Mobility Services Event provides such an environment and allows to verify the functionality of the PRESERVE VSS under controlled conditions. In addition, testing with ETSI in a laboratory environment allows performing specific security operations that are usually not tested in a FOT setup.

This document focuses on presenting the test activities and results in the ETSI ITS Cooperative Mobility Services Event 4 which is also named ETSI plugtest in the following document. In the plugtest the security implementation of PRESERVE was successfully connected and tested with implementations and devices of other companies. Similar to a joint FOT where different devices communicate with each other the plugtest focused on valid normal behaviour. That means the main aspects of a joined FOT were considered by the tests in the ETSI plugtest.

In Section 2 the ETSI ITS Cooperative Mobility Services Event 4 is first introduced. Subsequently, in the subsections the test setup is described followed by a detailed description of the test scenarios that are specified by Fraunhofer SIT based on the security architecture defined in PRESERVE deliverable D1.3 [3]. In the last two subsections of Section 2 the PRESERVE results are presented.

2 ETSI ITS Cooperative Mobility Services Event 4

In the continuous effort to support rapid ITS deployment and to validate the ETSI ITS Release 1 standards, a fourth Plugtest[1] has been organized in March 2015 focusing on Co-operative Mobile Systems standards from ETSI, CEN and ISO and to test the interoperability of ITS equipment from all key vendors.
The PRESERVE project participated to this event in order to validate the functional security implementation.

Two main activities were relevant for security testing.

- In an inter interoperability test event two devices of different companies were connected in order to verify that security functions are working properly under normal conditions.
  The PRESERVE inter interoperability test results are detailed in Section 2.3.

- In a conformance test event a single implementation of one company is connected with a test system that tests the correct behavior with respect to security in a semi-automated way. The conformance test considers also invalid behavior of a malicious sender which has to be detected by the implementation under test. The PRESERVE security conformance test results are detailed in Section 2.4.

[1] http://www.etsi.org/news-events/events/846-plugtests-2015-itscms4

2.1 Setup of Devices for ETSI Security Tests

The ITS device that should be tested is named in this document Implementation Under Test (IUT) and has to fulfill the following requirements.

The IUT has to be able to send and receive secured C2X packets.

- The security envelope shall be created according to the draft version of ETSI TS 103 097 v.1.1.15 [4].
- The communication stack shall employ the security envelope on its Network layer according to ETSI EN 302 636-4-1 v1.2.1 [5].
- In case of Geo Networking, the security envelope shall include GN Common and Extended Headers, and exclude GN Basic Header. For more information of the placement of the security header please have a look at the GeoNetworking Media Independent standard (section 8.4) [5].

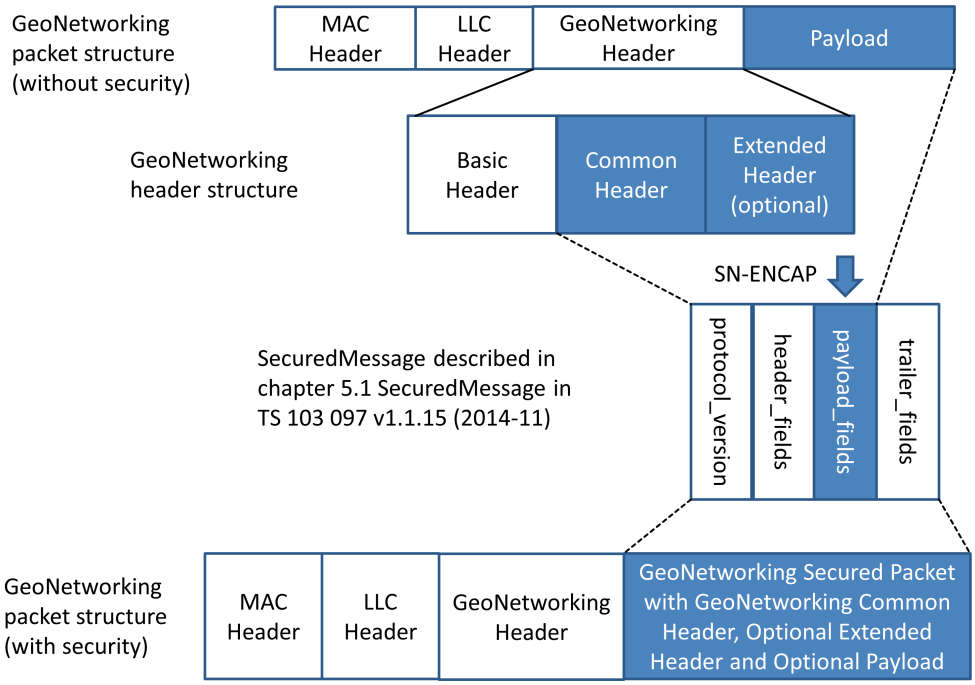

Figure 1: Integration of security header by GeoNetworking

- The face 2 face configuration shall be supported according to Figure 4. Two Entities Under Test (EUT) are connected with a cable instead of using the wireless interface with antennas.

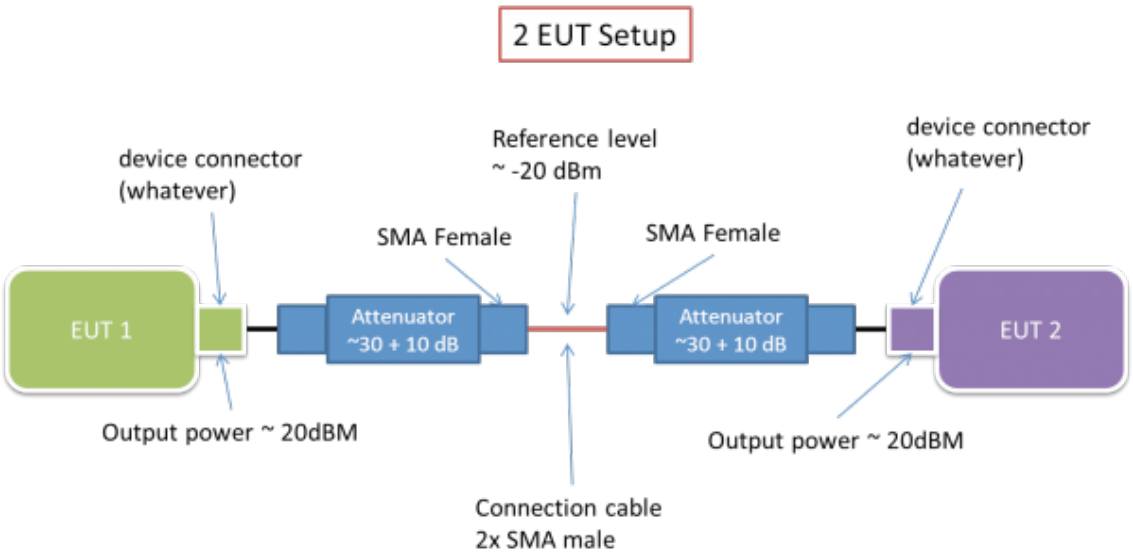

Figure 2: Face 2 Face configuation setup with two Entities Under Test (EUT)

- The communication stack shall only support the end-to-end security envelope according to the draft version of ETSI TS 103 097 v.1.1.15 [4].
- The receiving station (IUT-R) shall check whether a received message has been accepted or dropped by the security implementation.
- The sending station (IUT-S) shall be able to trigger the transmission of CAMs and DENMs.
- The IUT shall support the import of CA certificates to the IUT's certificate store.
- The IUT shall support the clearing of the CA certificate store of the IUT.
- The IUT shall support the clearing of the neighbor cache of the IUT.
- The location of the IUT shall be configured (geographic region id according to ISO 3166 1 and geographic region location with latitude and longitude according to ETSI TS 103 097 v.1.1.15) [4] by connecting the GPSD client to port 1941 of the ETSI GPSD server.

2.2 Interoperability Test Scenarios

For the interoperability event there have been specified and tested 12 scenarios where normal sender behavior is tested. The scenarios are listed in Table 1.

Table 1: Overview of the test scenarios performed in the face to face security session

Test Scenario	Obligation
Check trust chain with CA certs available when singing CAM	mandatory
Check trust chain with CA certs available and AT certificate request	optional
Check trust chain without CA certs available and AT certificate request	optional
Check trust chain after certificate change	optional
Select certificate with appropriate permissions	optional

Check trust chain with CA certs available when singing DENM	optional
Check different root domains	optional
Compressed public keys	optional
Check test valid identified region	optional
Check test valid circular region	optional
Check test valid rectangular region	optional
Check test valid polygonal region	optional

All information and test scenario descriptions are documented in the ETSI Plugtest Wiki [1]. The basis for all tests is a device that is able to send and receive secured CAMs and DENMs according to Section 2.1. If one of the two devices shows an incorrect or unexpected result then the test is failed. That means even if the implementation of one company is correct for all tests but the implementation of the test partner is incorrect then the test is failed.

The definition of the test cases and the setup of the security credential management has been specified by Fraunhofer based on the security architecture defined in PRESERVE deliverable D1.3 [3]. In Figure 3 the PKI architecture is shown that was used in the plugtests. Two new instances of the PRESERVE PKI were used to create the certificates required for the tests. The first PKI instance with one root CA and two Authorization Authorities (AAs) is trusted by all devices in the plugtest. A set of authorization ticket certificates were issued by these two AAs which contained different contents. Based on different issuers of authorization tickets different scenarios were tested where the stations had to request CA certificates on demand. A second "untrusted" PKI instances was used containing of one root CA and one AA. This second PKI was used to test scenarios where ITS devices belong to different domains that are not able to except messages from each other.

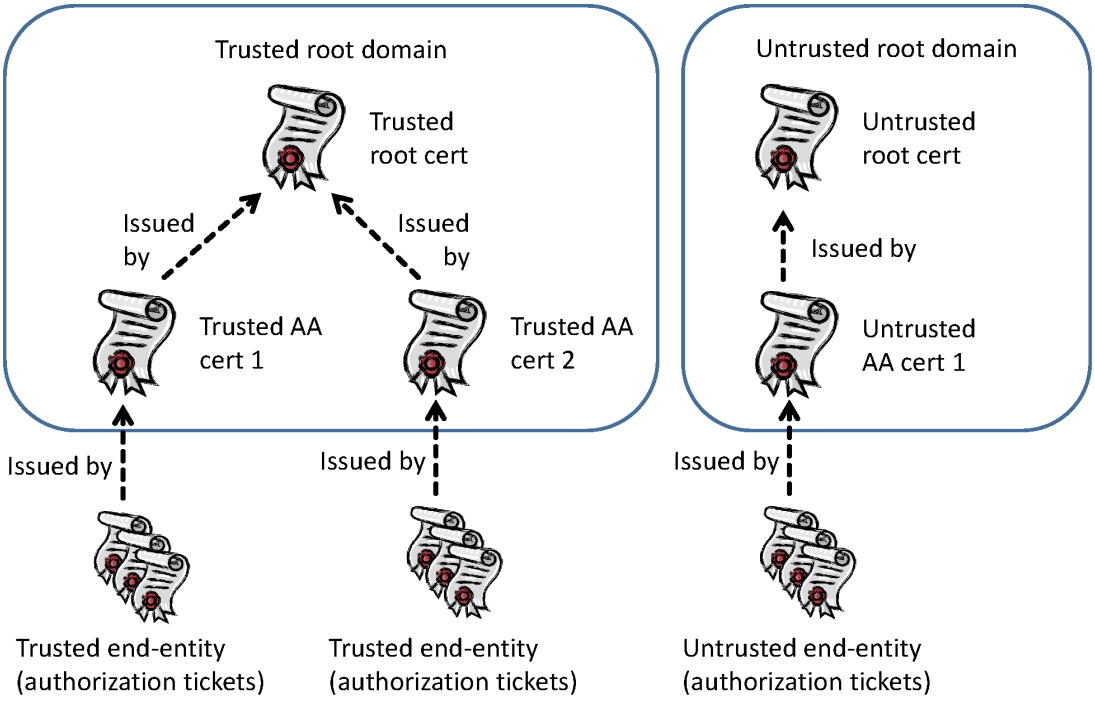

Figure 3: PKI setup of the ETSI plugtest based on the PRESERVE architecture

The CA certificates used in the interoperability test scenarios are listed in Table 2.

Table 2: CA certificates used in the interoperability test scenarios

CA Type	Cert ID
Root CA certificate	f5425279310c0379
AA certificate issued by trusted Root CA	5388dec640c6e19e
AA certificate issued by trusted Root CA	a0f336b87f0794b0
Untrusted Root CA certificate	d30e8c02c886e433
Untrusted AA certificate issued by untrusted Root CA	d6dfbc3d713ffa0b

The differently parametrized pseudonym certificates (Authorization Tickets, AT) used in the interoperability test scenarios are listed in Table 3.

Table 3: Authorization ticket certificates used in the interoperability test scenarios

Cert No.	Public verification key ECC point type	Geographic Region	Permissions	Private encryption key
AT1	uncompressed	none	default	not contained
AT2	uncompressed	none	default	not contained

AT3	**compressed_lsb_y_0 or compressed_lsb_y_1**	none	default	not contained
AT4	uncompressed	**Id; dictionary = ISO 3166 1; region ID = 528 = NL; local ID = 0**	AID = 0x25 with **SSP = 0x01FFFFFF (certificate allowed to sign all DENM containers)**	not contained
AT5	uncompressed	**Circle; lat = 514744200; long = 56240500; radius = 10000**	AID = 0x25 with **SSP = 0x01FFFFFF (certificate allowed to sign all DENM containers)**	not contained
AT6	uncompressed	**Rectangular; nw-lat = 514968550; nw-long = 55805300; se-lat = 514394730; se-long = 57263860**	AID = 0x25 with **SSP = 0x01FFFFFF (certificate allowed to sign all DENM containers)**	not contained
AT7	uncompressed	**Polygonal; nw-lat = 514968550; nw-long = 55805300; ne-lat = 514991540; ne-long = 57179290; se-lat = 514394730; se-long = 57263860; sw-lat = 514274030; sw-long = 55913130**	AID = 0x25 with **SSP = 0x01FFFFFF (certificate allowed to sign all DENM containers)**	not contained
AT8	uncompressed	none	AID = 0x24 with **SSP = 0x012000 (certificate allowed to sign specialTransport)**; AID = 0x25 with **SSP = 0x01FFFFFF (certificate allowed to sign all DENM containers)**	not contained
AT9	uncompressed	none	default	**contained**
AT10	uncompressed	none	default	not contained
AT11	uncompressed	none	default	not contained

In the following subsections the 12 test scenarios are detailed by listing the PICS, prerequisites, actions and expected results. In every test scenario the behaviour of the sender (IUT-S) and receiver (IUT-R) is described.

2.2.1 Test scenario 1.1 – Check trust chain with CA certs available when singing CAM

PICS

- IUT-R shall be configured to only receive CAMs and not to send CAMs

Prerequisite

- Place sender ITS station (IUT-S) in communication range of receiver ITS station (IUT-R) and configure both stations to receive and process incoming CAMs.
- Install root certificate (certId = **f5425279310c0379**) and AA certificate (certId = **5388dec640c6e19e**) on IUT-S and on IUT-R according to Table 2
- Install one authorization ticket certificate with cert number **AT1** on IUT-S and on IUT-R according to Table 3. The AT1 certificate installed on IUT-S should differ from the AT1 certificate installed on IUT-R.
- Clearing the neighbor cache including stored end-entity certs of neighbors on IUT-R
- Configure IUT-S to automatically broadcast CAMs
- IUT-R shall be configured to only receive CAMs and not to send CAMs

Actions

1. Start IUT-R and wait until it is ready to receive messages.
2. Start IUT-S and send signed CAMs for at least one second.
3. Check that IUT-S signs all outgoing CAMs with the certificate AT1.
4. Check that IUT-S includes after 1 second the certificate AT1 once instead of including the digest of the certificate AT1.
5. Check that IUT-R accepts at least CAMs after one second and that all subsequent CAMs are accepted as well.

Expected result

- IUT-R accepts CAMs from IUT-S at least after one second

2.2.2 Test scenario 1.2 – Check trust chain with CA certs available and AT certificate request

PICS

- First message received by IUT-R contains the digest of the AT certificate of IUT-S instead of the certificate
  - Configure IUT-S to include the digest of the AT certificate instead of the AT certificate into the security header of the first outgoing message after startup.
  - Try to connect IUT-S with IUT-R while IUT-S is sending secured messages that contain only the digest of the AT certificate.
- IUT shall broadcast CAMs with 10 Hz

Prerequisite

See prerequisites of test scenario 1.1 described in Section 2.2.1.

- Configure IUT-R to automatically broadcast CAMs with 10 Hz

Actions

1. Start IUT-R and wait until it is ready to receive messages
2. Start IUT-S
3. Check that IUT-S signs the first CAMs with a HeaderField containing signer_info of type certificate_digest_with_ecdsap256
4. Check that IUT-R receives the CAM with HeaderField containing signer_info of type certificate_digest_with_ecdsap256 and rejects the CAM as the certificate associated to the digest is unknown.
5. Check that IUT-R signs the next CAM with a security header that contains a HeaderField of type request_unrecognized_certificate and the HashedId3 related to the signer_info of the first received CAM
6. Check that IUT-S receives the CAM with the security header containing a HeaderField of type request_unrecognized_certificate and that the HashedId3 is matching the certificate ID of certificate AT1.
7. Check that IUT-S signs the next CAM with a security header containing a HeaderField with signer_info of type certificate.
8. Check that IUT-R receives the signed CAM with a security header containing a HeaderField with signer_info of type certificate and check that the CAM is accepted now.

Expected result

- IUT-R accepts CAMs from IUT-S at least after the reception of the 3rd CAM

2.2.3 Test scenario 1.3 – Check trust chain without CA certs available and AT certificate request

PICS

- According to the draft version of ETSI TS 103 097 v 1.1.15 the security profile for CAMs (section 7.1) the IUT supports the signer info type certificate_chain(3) in the security header field signer_info
- IUT shall broadcast CAMs with 10 Hz

Prerequisite

- Place sender ITS station (IUT-S) in communication range of receiver ITS station (IUT-R) and configure both stations to receive and process incoming CAMs.
- Install only the root certificate (certId = **f5425279310c0379**) on IUT-S and on IUT-R according to Table 2.
- Install the AA certificate (certId = **5388dec640c6e19e**) on IUT-S and AA certificate (certId = **a0f336b87f0794b0**) on IUT-R according to Table 2.

- Install one authorization ticket certificate with cert number **AT1** on IUT-S and one authorization ticket certificate with cert number **AT10** on IUT-R according to Table 3.
- Clearing the neighbor cache including stored end-entity certs of neighbors on IUT-R
- Configure IUT-S and IUT-R to automatically broadcast CAMs with 10 Hz

Actions

1. Start IUT-R and wait until it is ready to receive messages
2. Start IUT-S
3. Check that IUT-S signs the first CAMs with a HeaderField containing signer_info of type certificate_digest_with_ecdsap256
4. Check that IUT-R receives the CAM with HeaderField containing signer_info of type certificate_digest_with_ecdsap256 and rejects the CAM as the certificate associated to the digest is unknown.
5. Check that IUT-R signs the next CAM with a security header that contains a HeaderField of type request_unrecognized_certificate and the HashedId3 related to the signer_info of the first received CAM
6. Check that IUT-S receives the CAM with the security header containing a HeaderField of type request_unrecognized_certificate and that the HashedId3 is matching the certificate ID of certificate AT1.
7. Check that IUT-S signs the next CAM with a security header containing a HeaderField with signer_info of type certificate.
8. Check that IUT-R receives the signed CAM with a security header containing a HeaderField with signer_info of type certificate and rejects the CAM as the certificate associated to the digest is unknown.
9. Check that IUT-R signs the next CAM with a security header that contains a HeaderField of type request_unrecognized_certificate and the HashedId3 related to the signer_info of AT1.
10. Check that IUT-S receives the CAM with the security header containing a HeaderField of type request_unrecognized_certificate and that the HashedId3 is matching the certificate ID of AA certificate.
11. Check that IUT-S signs the next CAM with a security header containing a HeaderField with signer_info of type certificate_chain. The chain of length 2 contains the AA certificate (certId = **5388dec640c6e19e**) and the AT1 certificate of IUT-S.
12. Check that IUT-R receives the signed CAM with a security header containing a HeaderField with signer_info of type certificate_chain and check that the CAM is accepted now.

Expected result

- IUT-R accepts CAMs from IUT-S at least after the reception of the 5th CAM

2.2.4 Test scenario 1.4 – Check trust chain after certificate change

PICS

- The IUT supports the change of certificates
  - MAC address

  - GN address
    - MIB attribute itsGnLocalAddrConfMethod is set to ANONYMOUS (2) and the address is provided by the security (SN-SAP) according to ETSI EN 302 636-4-1 V1.2.1 section 9.2.1.4 and ETSI TS 102 723-8
  - Station ID
    - Shall use least significant bytes of the pseudonym ID provided by the security
- IUT shall broadcast CAMs with 10 Hz

Prerequisite

See prerequisites of test scenario 1.1 described in Section 2.2.1.

Actions

1. Start IUT-R and wait until it is ready to receive messages.
2. Start IUT-S and send signed CAMs for at least one second.
3. Check that IUT-S signs all outgoing CAMs with the certificate AT1.
4. Check that IUT-S includes after 1 second the certificate AT1 once instead of including the digest of the certificate AT1.
5. Check that IUT-R accepts at least the 10th CAM.
6. Change at IUT-S the certificate. Use now AT2 to sign CAMs.
7. Check that GN address and station ID consist of the certID of AT2.
8. IUT-S sends CAMs, signed with certificate AT2, for at least one second.
9. Check that IUT-S includes within the following second the certificate AT2 once instead of including the digest of the certificate AT2
10. Check that IUT-R accepts the CAMs after the certificate was included once.

Expected result

- IUT-R accepts CAMs from IUT-S after the certificate has been included once.

2.2.5 Test scenario 1.5 – Select certificate with appropriate permissions

PICS

- The IUT supports the change of certificates
- IUT supports handover of ITS-AID-SSP from message generator (facilities) to security
- IUT shall broadcast CAMs with 10 Hz

Prerequisite

See prerequisites of test scenario 1.1 described in Section 2.2.1.

Actions

1. Start IUT-R and wait until it is ready to receive messages.
2. Start IUT-S and send signed CAMs for at least one second. The CAM should contain no specialTransportContainer or any other special container that requires special permission.
3. Check that IUT-S signs all outgoing CAMs with the certificate AT1.

4. Check that IUT-S includes after 1 second the certificate AT1 once instead of including the digest of the certificate AT1.
5. Check that IUT-R accepts at least the 10th CAM.
6. Generate CAM with specialTransportContainer which requires special permission. CAM generator should transmit the ITS-AID for CAM and ITS-AID-SSP special specialTransport bit set to 1 to the security of IUT-S.
7. IUT-S selects certificate with appropriate permissions (**AT8**) and performs certificate change from **AT1** to **AT8.**
8. IUT-S sends CAMs, signed with certificate AT8, for at least one second.
9. Check that IUT-S includes within the following second the certificate AT8 once instead of including the digest of the certificate AT8
10. Check that IUT-R accepts the CAMs after the certificate was included once.

Expected result

- IUT-R accepts CAMs from IUT-S after the certificate has been included once.

2.2.6 Test scenario 1.6 – Check trust chain with CA certs available when singing DENM

PICS

- IUT-S shall be configured to send no CAMs and no secured GeoNet Beacons
- IUT-R shall be configured to only receive DENMs and not to send CAMs or DENMs

Prerequisite

- Place sender ITS station (IUT-S) in communication range of receiver ITS station (IUT-R) and configure both stations to receive and process incoming CAMs.
- Install root certificate (certId = **f5425279310c0379**) and AA certificate (certId = **5388dec640c6e19e**) on IUT-S and on IUT-R according to Table 2.
- Install one authorization ticket certificate with cert number**AT8** on IUT-S and on IUT-R according to Table 3. The AT1 certificate installed on IUT-S should differ from the AT1 certificate installed on IUT-R.
- Clearing the neighbor cache including stored end-entity certs of neighbors on IUT-R
- Trigger IUT-S broadcast a DENM. The DENM could contain any cause code because the certificate has permissions for containers.
- IUT-R shall be configured to only receive DENMs and not to send CAMs or DENMs

Actions

1. Start IUT-R and wait until it is ready to receive messages.
2. Start IUT-S and send a signed DENM.
3. Check that IUT-S signs the outgoing DENM with the certificate AT1 and includes the certificate to the signer info.
4. Check that IUT-R successfully verified the DENM and accepts it

Expected result

- IUT-R accepts DENM from IUT-S even if no previous messages has been received from IUT-S

2.2.7 Test scenario 2 – Check different root domains

PICS

- IUT shall broadcast CAMs with 10 Hz

Prerequisite

- Place sender ITS station (IUT-S) in communication range of receiver ITS station (IUT-R) and configure both stations to receive and process incoming CAMs.
- Install only the untrusted root certificate (certId = **d30e8c02c886e433**) and the untrusted AA certificate (certId = **d6dfbc3d713ffa0b**) on IUT-S according to Table 2.
- Install only the trusted root certificate (certId = **f5425279310c0379**) and the trusted AA certificate (certId = **5388dec640c6e19e**) on IUT-R according to Table 2.
- Install one authorization ticket certificate with certificate number **AT11** on IUT-S and **AT1** on IUT-R according to Table 3.
- Clearing the neighbor cache including stored end-entity certs of neighbors on IUT-R
- Configure IUT-S and IUT-R to automatically broadcast CAMs with 10 Hz

Actions

1. Start IUT-R and wait until it is ready to receive messages
2. Start IUT-S
3. Check that IUT-S signs the first CAMs with a HeaderField containing signer_info of type certificate_digest_with_ecdsap256
4. Check that IUT-R receives the CAM with HeaderField containing signer_info of type certificate_digest_with_ecdsap256 and rejects the CAM as the certificate associated to the digest is unknown.
5. Check that IUT-R signs the next CAM with a security header that contains a HeaderField of type request_unrecognized_certificate and the HashedId3 related to the signer_info of the first received CAM
6. Check that IUT-S receives the CAM with the security header containing a HeaderField of type request_unrecognized_certificate and that the HashedId3 is matching the certificate ID of certificate AT11
7. Check that IUT-S signs the next CAM with a security header containing a HeaderField with signer_info of type certificate.
8. Check that IUT-R receives the signed CAM with a security header containing a HeaderField with signer_info of type certificate and rejects the CAM as the certificate associated to the digest is unknown.
9. Check that IUT-R signs the next CAM with a security header that contains a HeaderField of type request_unrecognized_certificate and the HashedId3 related to the signer_info of AT11.

10. Check that IUT-S receives the CAM with the security header containing a HeaderField of type request_unrecognized_certificate and that the HashedId3 is matching the certificate ID of AA certificate.
11. Check that IUT-S signs the next CAM with a security header containing a HeaderField with signer_info of type certificate_chain. The chain of length 2 contains the AA certificate (certId = **d6dfbc3d713ffa0b**) and the AT11 certificate of IUT-S.
12. Check that IUT-R receives the signed CAM with a security header containing a HeaderField with signer_info of type certificate_chain and check that the CAM is rejected as the root certificate is not trusted.

Expected result

- IUT-R rejects the CAMs from IUT-S because the root certificate used by ITS-S is not trusted by IUT-R

2.2.8 Test scenario 3 – Compressed public keys

PICS

- IUT supports compressed public verification keys according to ETSI TS 103 097 v1.1.15 section 4.2.5.

Prerequisite

See prerequisites of test scenario 1.1 described in Section 2.2.1.

- Instead of using **AT1**, install a single **AT3** certificate on IUT-S and IUT-R according to Table 3.

Actions

- See actions of test scenario 1.1 described in Section 2.2.1.

Expected result

- See expected result of test scenario 1.1 described in Section 2.2.1.

Note

According to ETSI TS 103 097 v1.1.15 section 4.2.4 of certificates must not contain EccPointType = x_coordinate_only in a public key.

2.2.9 Test scenario 4.1 – Check test valid identified region

PICS

- Configuration of the location of the IUT as specified in Section 2.1 of this document.
- The location of the IUT can be configured according to the values specified Table 3 (column “geographic_region”).

Prerequisite

See prerequisites of test scenario 1.6 described in Section 2.2.6.

- Install a single **AT4** certificate on IUT-S and IUT-R according to Table 3.

Actions

1. Start IUT-R and wait until it is ready to receive messages.
2. Start IUT-S and send signed DENMs for at least one second.
3. Check that IUT-S signs all outgoing DENMs with the certificate AT4.
4. Check that IUT-S includes the certificate AT4.
5. Check that IUT-R accepts at least DENMs after one second and that all subsequent DENMs are accepted as well.

Expected result

- See expected result of test scenario 1.6 described in Section 2.2.6.

2.2.10 Test scenario 4.2 – Check test valid circular region

PICS

- Configuration of the location of the IUT as specified in the first section of this document.
- The location of the IUT can be configured according to the values specified Table 3 (column “geographic_region”).

Prerequisite

See prerequisites of test scenario 1.6 described in Section 2.2.6.

- Install a single **AT5** certificate on IUT-S and IUT-R according to Table 3.

Actions

1. Start IUT-R and wait until it is ready to receive messages.
2. Start IUT-S and send signed DENMs for at least one second.
3. Check that IUT-S signs all outgoing DENMs with the certificate AT5.
4. Check that IUT-S includes the certificate AT4.
5. Check that IUT-R accepts at least DENMs after one second and that all subsequent DENMs are accepted as well.

Expected result

- See expected result of test scenario 1.6 described in Section 2.2.6.

2.2.11 Test scenario 4.3 – Check test valid rectangular region

PICS

- Configuration of the location of the IUT as specified in the first section of this document.
- The location of the IUT can be configured according to the values specified Table 3 (column “geographic_region”).

Prerequisite

See prerequisites of test scenario 1.6 described in Section 2.2.6.

- Install a single **AT6** certificate on IUT-S and IUT-R according to Table 3.

Actions

1. Start IUT-R and wait until it is ready to receive messages.
2. Start IUT-S and send signed DENMs for at least one second.
3. Check that IUT-S signs all outgoing DENMs with the certificate AT6.
4. Check that IUT-S includes the certificate AT6.
5. Check that IUT-R accepts at least DENMs after one second and that all subsequent DENMs are accepted as well.

Expected result

- See expected result of test scenario 1.6 described in Section 2.2.6.

2.2.12 Test scenario 4.4 – Check test valid polygonal region

PICS

- Configuration of the location of the IUT as specified in the first section of this document.
- The location of the IUT can be configured according to the values specified Table 3 (column “geographic_region”).

Prerequisite

See prerequisites of test scenario 1.6

- Install a single **AT7** certificate on IUT-S and IUT-R according to Table 3.

Actions

1. Start IUT-R and wait until it is ready to receive messages.
2. Start IUT-S and send signed DENMs for at least one second.
3. Check that IUT-S signs all outgoing DENMs with the certificate AT7.
4. Check that IUT-S includes the certificate AT7.
5. Check that IUT-R accepts at least DENMs after one second and that all subsequent DENMs are accepted as well.

Expected result

- See expected result of test scenario 1.6

2.3 Interoperability Test Event Results

In the interoperability test event PRESERVE tested its security implementation with 8 other companies. At the ETSI ITS Cooperative Mobility Services Event 4 in sum 23 companies participated but 15 companies had no security implementation available. The results of the PRESERVE security tests are summarized in Table 4.

The PRESERVE security implementation was able to perform all 12 test scenarios with 100 % success rate, as shown by the results with the test partner company 2, 6, and 7 in Table 4. Since the implementations of some test partner companies were faulty or not fully implemented not all test sessions resulted in a fully successful result.

Table 4: PRESERVE Interoperability Security Test Results

Test Partner	Successful tests	Failed tests	Not applicable tests	Tests out of	Success rate

				time	
Company 1	5	1	6	0	42 %
Company 2	12	0	0	0	100 %
Company 3	4	6	2	0	33 %
Company 4	10	1	0	1	84 %
Company 5	11	1	0	0	92 %
Company 6	12	0	0	0	100 %
Company 7	12	0	0	0	100 %
Company 8	9	0	3	0	75 %
Average	**9.375**	**1.125**	**1.375**	**0.125**	**78.25 %**

2.4 Conformance Test Setup

In the conformance test event a single Device Under Test (DUT) is evaluated in an automated fashion using an a Conformance Validation Framework as depicted in Figure 4. The DUT on the right hand side of the figure implements the different functions for CAM and DENM message generation, Position, Timing (POTI), and security (SEC). In addition an Upper Tester is used to trigger different operations on the DUT by the Conformance Validation Framework or results are gathered. PRESERVE used in the conformance tests the communication stack and the message generator provided by Hitachi. The PRESERVE VSS was connected to this stack and performed all security operations that were tested by the ETSI Conformance Validation Framework.

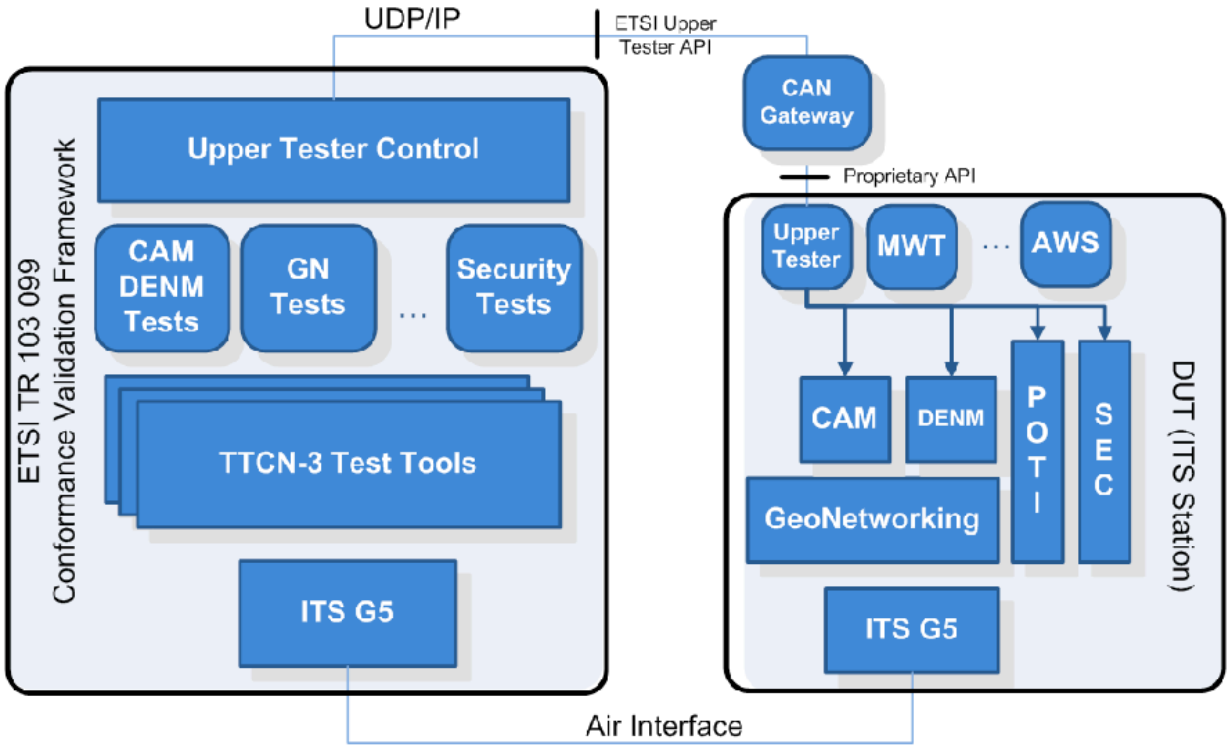

Figure 4: Conformance test setup of the ETSI Cooperative Mobility Services event

In total 64 security test cases were performed. The test cases, described in ETSI TS 103 096-2 [2] contain a list of preconditions and expected results. The preconditions are automatically established by the Conformance Validation Framework using the Upper Tester API. In the same way the results are requested within and after the test from the DUT via the Upper Tester interface.

2.5 Conformance Test Results

Besides PRESERVE 8 other companies participated to the ETSI security conformance tests as listed in Table 5. The average success rate was about 72.18 % considering all companies. PRESERVE had a success rate of 89.06 %.

Table 5: Security Conformance Test Results

Test Partner	Successful tests	Failed tests	Not applicable tests	Tests out of time	Success rate
PRESERVE	**57**	**5**	**2**	**0**	**89.06 %**
Company 2	26	1	23	14	40.63 %
Company 3	12	3	0	49	18.75 %
Company 4	55	3	4	0	88.71 %
Company 5	35	2	14	13	54.69 %

Company 6	64	0	0	0	100 %
Company 7	59	5	0	0	92.19 %
Company 8	62	0	1	1	96.88 %
Company 9	44	4	3	13	68.75 %
Average	**46**	**2.56**	**5.23**	**10**	**72,18 %**

3 Conclusions

In this document we focus on presenting the participation to the ETSI ITS Cooperative Mobility Services Event 4, short ETSI plugtest.

After presenting the test setup and the test scenarios the results in the two categories *Interoperability Tests* and *Conformance Tests* are discussed. With respect to interoperability testing the PRESERVE security implementation was able to perform all test scenarios with 100% success rate. In the conformance tests the PRESERVE VSS had a success rate of 89.06% which is clearly above the average success rate.

References

[1] I. Passchier, F. Fischer, and S. Muller. (2015, March) Its cms 2015 wiki. Online. ETSI. [Online]. Available: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Base_Specs_and_Test_Plans#IOP_Test_Plans

[2] ETSI - European Telecommunications Standards Institute, “Intelligent transport systems (ITS); testing; conformance test specification for security; part 2: Test suite structure and test purposes (TSS&TP),” ETSI, Technical Standard TS 103 096-2, February 2015, v0.0.1.

[3] N. Bißmeyer, S. Mauthofer, J. Petit, M. Lange, M. Moser, D. Estor, M. Sall, M. Feiri, R. Moalla, M. Lagana, and F. Kargl, “PRESERVE d1.3 v2x security architecture v2,” PREparing SEcuRe VEhicle-to-X Communication Systems Consortium, Deliverable, January 2014.

[4] ETSI - European Telecommunications Standards Institute, “Intelligent Transport Systems (ITS); Security; Security header and certificate formats,” ETSI, Draft of Technical Standard TS 103 097, November 2014, v1.1.15.

[5] ETSI - European Telecommunications Standards Institute, “Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality,” ETSI, Draft of European Norm EN 302 636-4-1, July 2014, v1.2.1.