Test Scenarios based on ETSI TS 103 097 v1.1.15 Test send and receive

Functions that a IUT shall support in order to run the test scenarios 2

Test scenario 1 – Check trust chain 3

Test scenario 1.1 – Check trust chain with CA certs available when singing CAM 3

Test scenario 1.2 – Check trust chain with CA certs available and AT certificate request 4

Test scenario 1.3 – Check trust chain without CA certs available and AT certificate request 5

Test scenario 1.4 – Check trust chain after cert change 7

Test scenario 1.5 – Select certificate with appropriate permissions 8

Test scenario 1.6 – Check trust chain with CA certs available when singing DENM 8

Test scenario 2 – Check different root domains 9

Test scenario 3 – Compressed public keys 12

Test scenario 4 – ValidityRestriction – GeographicRegion 13

Test scenario 4.1 – Check test valid identified region 13

Test scenario 4.2 – Check test valid circular region 13

Test scenario 4.3 – Check test valid rectangular region 14

Test scenario 4.4 – Check test valid polygonal region 15

Functions that a IUT shall support in order to run the test scenarios

- Sending and receiving of secured C2X packets.
  - The security envelope shall be created according to the draft version of ETSI TS 103 097 v.1.1.15. This version is uploaded on the plugtest wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#SECURITY
  - The communication stack shall employ the security envelope on its Network layer.
  - In case of GN, 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). The draft version is uploaded on the plugtest wiki: http://www.etsi.org/deliver/etsi_en/302600_302699/3026360401/01.02.01_60/en_3026360401v010201p.pdf

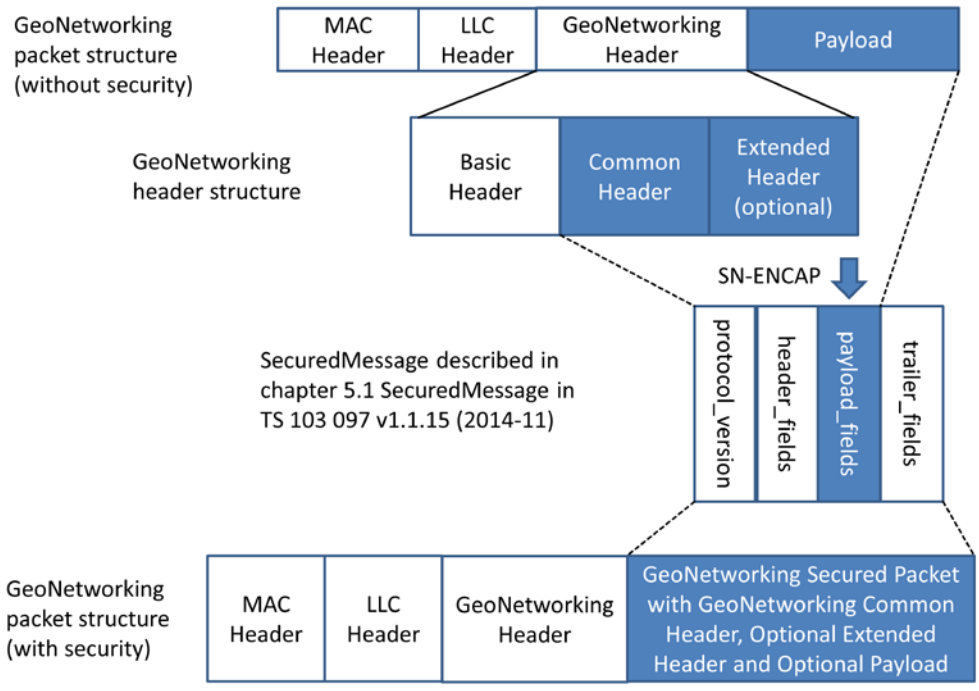

Figure 1: Integration of security header by GeoNetworking

- The face 2 face configuration shall be supported according to the plug test wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Face_2_Face_Configuration
- 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.

- 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 CAM and DENM.
- Adding CA certificates from the IUT's certificate store.
- Clearing the CA certificate store of the IUT.
- Clearing the neighbor cache of the IUT.
- Configure the location of the IUT (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). Configure the GPSD client to connect to port 1941 according to https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#GPSD_server

Table 1: Overview of test scenarios

Test scenario	Section	Obligation
Check trust chain with CA certs available when singing CAM	Section 1.1	mandatory
Check trust chain with CA certs available and AT certificate request	Section 1.2	optional
Check trust chain without CA certs available and AT certificate request	Section 1.3	optional
Check trust chain after cert change	Section 1.4	optional
Select certificate with appropriate permissions	Section 1.5	optional
Check trust chain with CA certs available when singing DENM	Section 1.6	optional
Check different root domains	Section 2	optional
Compressed public keys	Section 3	optional
Check test valid identified region	Section 4.1	optional
Check test valid circular region	Section 4.2	optional
Check test valid rectangular region	Section 4.3	optional
Check test valid polygonal region	Section 4.4	optional

Test scenario 1 – Check trust chain

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

This test scenario is mandatory.

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 cert (certId = **f5425279310c0379**) and AA cert (certId = **5388dec640c6e19e**) on IUT-S and on IUT-R according to the wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#PKI_Setup_for_Security_Testing
- Install one authorization ticket cert with certificate number**AT1** on IUT-S and on IUT-R according to the wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Authorization_tickets_for_the_tests. The AT1 cert installed on IUT-S should differ from the AT1 cert 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 cert AT1.
4. Check that IUT-S includes after 1 second the cert AT1 once instead of including the digest of the cert 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

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

This test scenario is optional.

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 cert 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

- 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 cert 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 cert ID of cert 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

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

This test scenario is optional.

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 cert (certId = **f5425279310c0379**) on IUT-S and on IUT-R according to the wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#PKI_Setup_for_Security_Testing

- Install the AA cert (certId = **5388dec640c6e19e**) on IUT-S and AA cert (certId = **a0f336b87f0794b0**) on IUT-R according to the wiki: **Error! Hyperlink reference not valid.**https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#PKI_Setup_for_Security_Testing
  - Install one authorization ticket cert with cert no **AT1** on IUT-S and one authorization ticket cert with cert no **AT10** on IUT-R according to the wiki:https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Authorization_tickets_for_the_tests.
  - 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 cert 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 cert ID of cert 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 cert 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 cert ID of AA cert.
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

Test scenario 1.4 – Check trust chain after cert change

This test scenario is optional.

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

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 cert AT1.
4. Check that IUT-S includes after 1 second the cert AT1 once instead of including the digest of the cert AT1.
5. Check that IUT-R accepts at least the 10th CAM.
6. Change at IUT-S the cert. 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 cert AT2, for at least one second.
9. Check that IUT-S includes within the following second the cert AT2 once instead of including the digest of the cert AT2
10. Check that IUT-R accepts the CAMs after the cert was included once.

Expected result

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

Test scenario 1.5 – Select certificate with appropriate permissions

This test scenario is optional as based on informative Annex B of TS 103 097 v1.1.15

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

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 cert AT1.
4. Check that IUT-S includes after 1 second the cert AT1 once instead of including the digest of the cert 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 cert change from **AT1** to **AT8.**
8. IUT-S sends CAMs, signed with cert AT8, for at least one second.
9. Check that IUT-S includes within the following second the cert AT8 once instead of including the digest of the cert AT8
10. Check that IUT-R accepts the CAMs after the cert was included once.

Expected result

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

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

This test scenario is optional.

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 cert (certId =) and AA cert (certId =) on IUT-S and on IUT-R according to the wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#PKI_Setup_for_Security_Testing
- Install one authorization ticket cert with certificate number**AT8** on IUT-S and on IUT-R according to the wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Authorization_tickets_for_the_tests. The AT1 cert installed on IUT-S should differ from the AT1 cert 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 cert 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

Test scenario 2 – Check different root domains

This test scenario is optional.

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 cert (certId = **d30e8c02c886e433**) and the untrusted AA cert (certId = **d6dfbc3d713ffa0b**) on IUT-S according to the wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#PKI_Setup_for_Security_Testing
    - Install only the trusted root cert (certId = **f5425279310c0379**) and the trusted AA cert (certId = **5388dec640c6e19e**) on IUT-R according to the wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#PKI_Setup_for_Security_Testing
    - Install one authorization ticket cert with cert no **AT11** on IUT-S and **AT1** on IUT-R according to the wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Authorization_tickets_for_the_tests
    - 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 cert 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 cert ID of cert 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 cert 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 cert ID of AA cert.
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 cert is not trusted.

Expected result

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

Test scenario 3 – Compressed public keys

This test scenario is optional.

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

- Instead of using **AT1**, install a single **AT3** cert on IUT-S and IUT-R according to the wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Authorization_tickets_for_the_tests

Actions

See actions of test scenario 1.1

Expected result

See expected result of test scenario 1.1

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.

Test scenario 4 – ValidityRestriction – GeographicRegion

Test scenario 4.1 – Check test valid identified region

This test scenario is optional.

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 in the wiki (column “geographic_region” in table “Authorization tickets for the tests”): https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Authorization_tickets_for_the_tests

Prerequisite

See prerequisites of test scenario 1.6

- Install a single **AT4** cert on IUT-S and IUT-R according to the wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Authorization_tickets_for_the_tests

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 cert AT4.
4. Check that IUT-S includes the cert 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

Test scenario 4.2 – Check test valid circular region

This test scenario is optional.

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 in the wiki (column “geographic_region” in table “Authorization tickets for the tests”): https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Authorization_tickets_for_the_tests

Prerequisite

See prerequisites of test scenario 1.6

- Install a single **AT5** cert on IUT-S and IUT-R according to the wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Authorization_tickets_for_the_tests

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 cert AT5.
4. Check that IUT-S includes the cert 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

Test scenario 4.3 – Check test valid rectangular region

This test scenario is optional.

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 in the wiki (column “geographic_region” in table “Authorization tickets for the tests”): https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Authorization_tickets_for_the_tests

Prerequisite

See prerequisites of test scenario 1.6

- Install a single **AT6** cert on IUT-S and IUT-R according to the wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Authorization_tickets_for_the_tests

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 cert AT6.
4. Check that IUT-S includes the cert 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

Test scenario 4.4 – Check test valid polygonal region

This test scenario is optional.

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 in the wiki (column “geographic_region” in table “Authorization tickets for the tests”): https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Authorization_tickets_for_the_tests

Prerequisite

See prerequisites of test scenario 1.6

- Install a single **AT7** cert on IUT-S and IUT-R according to the wiki: https://services.plugtests.net/wiki/ITS-CMS4/index.php/Testing_Information#Authorization_tickets_for_the_tests

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 cert AT7.
4. Check that IUT-S includes the cert 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

Document history		
0.1	12.01.2015	First draft based on ETSI plugtest 2013
0.2	27.01.2015	Test scenarios 1.5, 1.6, 4.3, and 4.4 added. Figure 1 updated
0.3	10.02.2015	Test scenario 1.4 changed by adding requirements for GN address and station ID Cert IDs of Root and AA added
0.4	20.02.2015	Clarification of 1.5 Information about the GPSD port added
0.5	04.03.2015	Clarification of 1.4, MAC address should also change Clarification of 4.x regarding configuration of location.
0.6	09.03.2015	Sending DENMs in test scenarios 4.x instead of CAMs. The security profile for
0.7	12.03.2015	Usage of AT8 instead of AT1 in test scenario 1.6. Info added to test scenario 1.6 that the certificate has permissions for all cause codes.