

# Test Scenarios based on ETSI TS 103 097

## Test send and receive

---

Functions that a IUT shall support in order to run the test scenarios .....	2
Test scenario1 – Check trust chain.....	3
Test scenario 1.1 – Check trust chain with CA certs available .....	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 .....	6
Test scenario2 – Check different root domains .....	9
Test scenario 4 – Compressed public keys.....	12
Test scenario 5 – ValidityRestriction – GeographicRegion.....	13
Test scenario 5.1 – Check test valid identified region.....	13
Test scenario 5.3 – Check test valid circular region .....	15

## Functions that a **DUT-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 revised version of](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#SECURITY-) ETSI TS 103 097 v.1.1.1. This version is uploaded on the plugtest wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#SECURITY-](https://services.plugtests.net/wiki/ITS-CMS3/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: <https://services.plugtests.net/wiki/ITS-CMS3/images/a/a3/GN-ITS-0030035v051.doc>

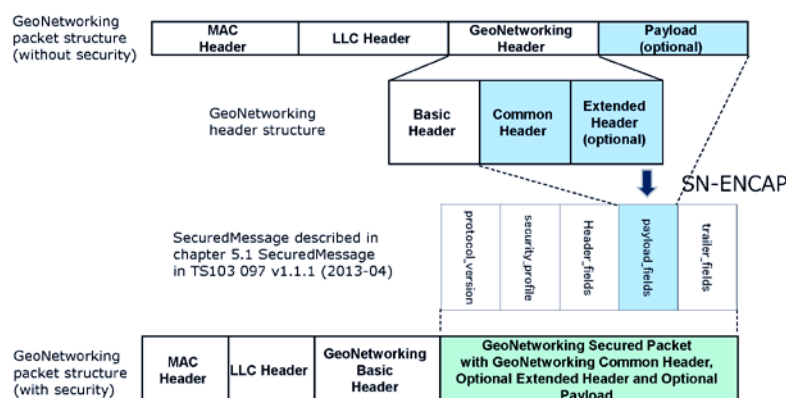


Figure 1: Integration of security header by GeoNetworking

- [The face 2 face configuration shall be supported according to the plug test wiki: https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#Face\\_2\\_Face\\_Configuration](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#Face_2_Face_Configuration)
- The communication stack shall only support the end-to-end security envelope according to [the revised version of](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#SECURITY-) ETSI TS 103 097 v.1.1.1.
- Checking whether a received message has been accepted or dropped by the security implementation.
- Possibility to trigger the transmission of CAM.
- Adding CA certificates from the **DUT's-IUT's** certificate store.
- Clearing the CA certificate store of the **DUT-IUT**.
- Clearing the neighbor cache of the **DUT-IUT**.


- Configure the location of the ~~DUT-IUT~~ (geographic region id according to ISO 3166 1 and geographic region location with latitude and longitude according to ETSI TS 103 097 v.1.1.1).

## Test scenario1 – Check trust chain

### Test scenario 1.1 – Check trust chain with CA certs available

This test scenario is mandatory.

#### PICS :

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

~~None~~

#### 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 = **83ca2168b784fc6c**) and AA cert (certId = **0ee6e51b5a7a722aa8ed6df65b0e6d6a**) on IUT-S and on IUT-R according to the wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#PKI\\_Setup\\_for\\_Security\\_Testing](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#PKI_Setup_for_Security_Testing)
- Install one authorization ticket cert with cert no **AT1** on IUT-S and on IUT-R according to the wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#Authorization\\_tickets\\_for\\_the\\_tests](https://services.plugtests.net/wiki/ITS-CMS3/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 and-including stored end-entity certs of neighbors end-entity cert store on IUT-R
- Configure IUT-S to automatically broadcast CAMs with 10 Hz
- 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 ~~the 10<sup>th</sup>~~ CAMs s after one second and that all subsequent CAMs are accepted as well.

#### Expected result

- IUT-R accepts CAMs from IUT-S at least after ~~the reception of the 10<sup>th</sup>~~ CAM one second

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

This test scenario is optional.

#### PICS

- The IUT shall be configured to include the digest of the AT certificate instead of the AT cert into the security header of the first outgoing message after startup.
- 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 3<sup>rd</sup> CAM

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

This test scenario is optional.

#### PICS

- In addition According to the revised version of ETSI TS 103 097 v 1.1.1 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 = **83ca2168b784fc6c**) on IUT-S and on IUT-R according to the wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#PKI\\_Setup\\_for\\_Security\\_Testing](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#PKI_Setup_for_Security_Testing)
- Install the AA cert (certId = **0ec6e51b5a7a722aa8ed6df65b0e6d6a**) on IUT-S and AA cert (certId = **09e9bac26ccce3ed**) on IUT-R according to the wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#PKI\\_Setup\\_for\\_Security\\_Testing](https://services.plugtests.net/wiki/ITS-CMS3/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 AT6 on IUT-R according to the wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#Authorization\\_tickets\\_for\\_the\\_tests](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#Authorization_tickets_for_the_tests).
- Clearing the neighbor cache including stored end-entity certs of neighbors and end-entity cert store 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 = a8ed6df65b0e6d6a) 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 5<sup>th</sup> CAM

## Test scenario 1.4 – Check trust chain after cert change

This test scenario is optional.

### PICS

- The IUT supports the change of certificates
- 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 10<sup>th</sup> CAM.
6. Change at IUT-S the cert. Use now AT5 to sign CAMs.
7. IUT-S sends CAMs, signed with cert AT5, for at least one second.
8. Check that IUT-S includes within the following second the cert AT5 once instead of including the digest of the cert AT1.
9. 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—Check trust chain when IUT is sending the chain every time

### PICS

- In contrast to ETSI TS 103 097 v1.1.1 the IUT is signing all CAMs with a security header containing a HeaderField with signer\_info of type certificate\_chain

### Prerequisite

See prerequisites of test scenario 1.3

### 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 CAMs with a HeaderField containing signer\_info of type certificate\_chain. The chain of length 2 contains the root certificate (certId = 83ca2168b784fc6c), the AA certificate (certId = 0ec6e51b5a7a722a) and the AT1 certificate.
4. Check that IUT-R receives the CAM with HeaderField containing signer\_info of type certificate\_chain and accepts the CAM.

#### **Expected result**

- IUT-R accepts the first CAMs from IUT-S.



## Test scenario2 – Check different root domains

This test scenario is optional.

### PICS

- IUT shall broadcast CAMs with 10 Hz~~None~~

### 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 = **b5c3d48de571a1f5**) and the untrusted AA cert (certId = **1ead94971ca10baac7895077af013a80**) on IUT-S according to the wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#PKI\\_Setup\\_for\\_Security\\_Testing](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#PKI_Setup_for_Security_Testing)
- Install only the trusted root cert (certId = **83ca2168b784fc6c**) and the trusted AA cert (certId = **0ec6e51b5a7a722aa8ed6df65b0e6d6a**) on IUT-R according to the wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#PKI\\_Setup\\_for\\_Security\\_Testing](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#PKI_Setup_for_Security_Testing)
- Install one authorization ticket cert with cert no **AT7** on IUT-S and **AT1** on IUT-R according to the wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#Authorization\\_tickets\\_for\\_the\\_tests](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#Authorization_tickets_for_the_tests)
- Clearing the neighbor cache including stored end-entity certs of neighbors and end-entity cert store 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~~
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 AT71.
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 = c7895077af013a80) and the AT7 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 – Encrypted payload

### PICS

- IUT is able to send and receive other messages with `security_profile` value set to 3 according to ETSI TS 103 097 v1.1.1 section 7.3.
- IUT can be triggered to send an encrypted message via unicast to a specific neighbor, e.g. by using the MAC address of the neighbor.
- The payload type `signed_and_encrypted` is supported.

### 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 = **83ca2168b784fc6c**) and AA cert (certId = **0ec6e51b5a7a722a**) on IUT-S and on IUT-R according to the wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#PKI\\_Setup\\_for\\_Security\\_Testing](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#PKI_Setup_for_Security_Testing)
- Install one authorization ticket cert with cert no **AT5** on IUT-S and IUT-R according to the wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#Authorization\\_tickets\\_for\\_the\\_tests](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#Authorization_tickets_for_the_tests)
- Clearing the neighbor cache and end-entity cert store 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 and wait until it received the certificate of IUT-R with a signed CAM
3. Trigger IUT-S to generate a DENM and trigger the encryption of the DENM with the encryption key contained in the AT5 certificate of IUT-R.
4. Check that IUT-R is able to decrypt and verify the message

### Expected result

- IUT-R is able to decrypt and verify the message sent by IUT-S

### Note

- Message format of payload has to be specified for the test

## Test scenario 4 – Compressed public keys

This test scenario is optional.

### PICS

- IUT supports compressed public verification keys according to ETSI TS 103 097 v1.1.1 section 4.2.5.

### Prerequisite

See prerequisites of test scenario 1.1

- Instead of using **AT1**, install a single **AT2** cert on IUT-S and IUT-R according to the wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#Authorization\\_tickets\\_for\\_the\\_tests](https://services.plugtests.net/wiki/ITS-CMS3/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

- Certificates with `EccPointType = x_coordinate_only` will not be tested.

## Test scenario 5 – ValidityRestriction – GeographicRegion

### Test scenario 5.1 – Check test valid identified region

This test scenario is optional.

#### PICS

- Configuration of the location of the IUT is possible according to ETSI TS 103 097 v1.1.1 section 4.2.26.
- 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-CMS3/index.php/Testing\\_Information#Authorization\\_tickets\\_for\\_the\\_tests](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#Authorization_tickets_for_the_tests)

#### 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-CMS3/index.php/Testing\\_Information#Authorization\\_tickets\\_for\\_the\\_tests](https://services.plugtests.net/wiki/ITS-CMS3/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 CAMs for at least one second.
3. Check that IUT-S signs all outgoing CAMs with the cert AT3.
4. Check that IUT-S includes after 1 second the cert AT3 once instead of including the digest of the cert AT3.
5. Check that IUT-R accepts at least ~~the 10<sup>th</sup>~~-CAMs after one second and that all subsequent CAMs are accepted as well.

#### Expected result

• ~~See expected result of test scenario 1.1: IUT-R accepts CAMs from IUT-S at least after the reception of the 10<sup>th</sup>-CAM~~

Formatted: Indent: Left: 0 cm, First line: 1,25 cm

## Test scenario 5.2 – Check test invalid identified region

### PICS

Formatted: Indent: Left: 0 cm, First line: 1,25 cm

- Configuration of the location of the IUT is possible according to ETSI TS 103 097 v1.1.1 section 4.2.26.
- The location of the IUT can be configured to values that do not match with the real location of the IUT. For instance, set the region ID to “FR” although the IUT is located in “DE”.

### 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-CMS3/index.php/Testing\\_Information#Authorization\\_tickets\\_for\\_the\\_tests](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#Authorization_tickets_for_the_tests)

### Actions

See actions of test scenario 1.1

1. Configure IUT-R with the location **dictionary = ISO 3166-1; region ID = 250 = FR; local ID = 0**
2. Start IUT-R and wait until it is ready to receive messages.
3. Start IUT-S and send signed CAMs for at least one second.
4. Check that IUT-S signs all outgoing CAMs with the cert AT3.
5. Check that IUT-S includes after 1 second the cert AT3 once instead of including the digest of the cert AT3.
6. Check that IUT-R rejects all CAMs because the location specified in the cert is not matching with the location of the IUT-R.

### Expected result

- IUT-R rejects all CAMs from IUT-S

## Test scenario 5.3 – Check test valid circular region

This test scenario is optional.

### PICS

- Configuration of the location of the IUT is possible according to ETSI TS 103 097 v1.1.1 section 4.2.23.
- 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-CMS3/index.php/Testing\\_Information#Authorization\\_tickets\\_for\\_the\\_tests](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#Authorization_tickets_for_the_tests)

### Prerequisite

See prerequisites of test scenario 1.1

- Instead of using **AT1**, install a single **AT4** cert on IUT-S and IUT-R according to the wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#Authorization\\_tickets\\_for\\_the\\_tests](https://services.plugtests.net/wiki/ITS-CMS3/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 CAMs for at least one second.
3. Check that IUT-S signs all outgoing CAMs with the cert AT4.
4. Check that IUT-S includes after 1 second the cert AT4 once instead of including the digest of the cert AT4.
5. Check that IUT-R accepts at least ~~the 10<sup>th</sup>~~ CAMs after one second and that all subsequent CAMs are accepted as well.

### Expected result

- ~~See expected result of test scenario 1.1~~ IUT-R accepts CAMs from IUT-S at least after the reception of the 10<sup>th</sup> CAM

Formatted: Indent: Left: 0 cm, First line: 1,25 cm

## Test scenario 5.4 – Check test invalid circular region

### PICS

- Configuration of the location of the IUT is possible according to ETSI TS 103 097 v1.1.1 section 4.2.23.
- The location of the IUT can be configured to values that do not match with the real location of the IUT.

### Prerequisite

See prerequisites of test scenario 1.1

- Instead of using **AT1**, install a single **AT4** cert on IUT-S and IUT-R according to the wiki: [https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing\\_Information#Authorization\\_tickets\\_for\\_the\\_tests](https://services.plugtests.net/wiki/ITS-CMS3/index.php/Testing_Information#Authorization_tickets_for_the_tests)

### Actions

See actions of test scenario 1.1

1. Configure IUT-R with the location: **Circle; latitude = 43616436; longitude = 7052972**
2. Start IUT-R and wait until it is ready to receive messages.
3. Start IUT-S and send signed CAMs for at least one second.
4. Check that IUT-S signs all outgoing CAMs with the cert AT4.
5. Check that IUT-S includes after 1 second the cert AT4 once instead of including the digest of the cert AT4.
6. Check that IUT-R rejects all CAMs because the location specified in the cert is not matching with the location of the IUT-R.

### Expected result

- IUT-R rejects all CAMs from IUT-S



Document history		
0.1	07.2013	First draft
0.2	21.08.2013	Added statement of certificate_chain in the signer_info in test scenario 3 Modified test scenario 5 to support only compressed keys with the two type compressed_lsb_y_0 or compressed_lsb_y_1
0.3	03.09.2013	- List of content added - New structure of tests with PICS, Prerequisites, Actions and expected results - Productive IUTs expected that are working according to ETSI TS 103 097 and cannot be fully operated manually.
0.4	18.09.2013	- <u>Clarifications in prerequisites</u> - <u>Information added in action 11 of scenario 1.3</u> - <u>Correction of typo in process of scenario 1.4 and 1.5</u> - <u>Correction of typo in process of scenario 2: AT1 -&gt; AT7</u> - <u>AA cert with digest of root certificate not allowed according to TS 103 097. Consequently new AA certificate created. AA cert ID "0ec6e51b5a7a722a" and "1ead94971ca10baa" exchanged by AA cert ID "75b949656e6901e6" and "221d6604f8e92c50" respectively</u>
0.5	02.10.2013	- <u>In test scenario 1.1 the requirement deleted that CAMs must be sent with 10 Hz</u> - <u>In test scenario 1.2, 1.3, 1.4 and 2 PICS added</u>
	10.10.2013	- <u>Test scenario 1.5, 3, 5.2, and 5.3 deleted</u> - <u>Information added whether test scenario is mandatory or optional</u> - <u>Requirement added: regarding face 2 face configuration</u>
	21.10.2013	- <u>Figure added regarding the integration of the security header into the packet.</u>
0.6	05.11.2013	- <u>Substitution of trusted AA cert: 75b949656e6901e6 by AA cert: a8ed6df65b0e6d6a</u> - <u>Substitution of untrusted AA cert: 221d6604f8e92c50 by AA cert: c7895077af013a80</u> - <u>Change of test scenario 1.3. IUT-R is equipped with a AA cert that is issued by the trusted root CA.</u> - <u>Support of revised version of ETSI TS 103 097 expected</u>