ETSI TS 103 600 V1.2.1 (2022-02)

TECHNICAL SPECIFICATION

Intelligent Transport Systems (ITS); Testing; Interoperability test specifications for security

Reference

RTS/ITS-00565

Keywords

interoperability, ITS, security, testing

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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 https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document contains specification of interoperability test descriptions to validate implementations of ETSI TS 103 097 [1], ETSI TS 102 941 [3] and ETSI TS 102 940 [i.1].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 103 097 (V1.4.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

[2] IEEE Std 1609.2™-2016: "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2a™-2017 and EEE Std 1609.2b™-2019.

[3] ETSI TS 102 941 (V1.4.1): "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".

[4] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), (Release 1.1).

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 102 940 (V1.3.1): "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

[i.2] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security; Part 2: Security functional components".

[i.3] ETSI TR 103 415 (V1.1.1): "Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management".

[i.4] ETSI TS 102 731 (V1.1.1): "Intelligent Transport Systems (ITS); Security; Security Services and Architecture".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 097 [1], ETSI TS 102 940 [i.1], ETSI TS 102 941 [3], ISO/IEC 15408-2 [i.2] and the following apply:

current CA: CA possessing the certificate containing in the trusted chain for at least one of certificate currently used by the SUT

foreign CA: any CAs possessing the certificate, been never used in the trusted chain for any end entity certificates used by the SUT

3.2 Symbols

For the purposes of the present document, the symbols given in ETSI TS 103 097 [1], ETSI TS 102 940 [i.1], ETSI TS 102 941 [3], ISO/IEC 15408-2 [i.2] apply.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 103 097 [1], ETSI TS 102 941 [3], ETSI TS 102 940 [i.1], ISO/IEC 15408-2 [i.2] apply.

4 Requirements and configuration

4.1 Requirements

4.1.1 Overview

Clauses 4.1.2, 4.1.3 and 4.1.4 define mandatory and optional requirements for the implementation of ITS station, PKI or TLM. All EUT shall support mandatory requirements. Essential optional requirements defined in clause 5 and in use-case descriptions.

NOTE: Interoperability testing between two IUTs cover mandatory requirements and optional requirements supported by the IUTs.

4.1.2 ITS stations

Mandatory requirements:

- The ITS-S shall support data communication using security mechanisms described in ETSI TS 103 097 [1] and PKI communication described in ETSI TS 102 941 [3].
- The ITS-S shall support algorithms and key length according to the Certificate Policy [4].
- In order to participate in secured communication tests, the ITS-S shall be able to send CAMs and DENMs using V2X communication.

Optional requirements:

PICS	Description
PICS_ITSS_REGION_SUPPORT	The ITS-S supports region validity restrictions in AT certificates. The ITS-S shall support at least Circular and Identified region types in order to participate to use-cases dependent of the present PICS value. See IEEE Std 1609.2 [2], clause 6.4.17.
PICS_ITSS_REQUEST_AA	ITS-S is able to request unknown AA certificate using peer-2-peer certificate distribution mechanism without infrastructure involved.
PICS_ITSS_RESPOND_AA	ITS-S is able to answer for the request for unknown AA certificate using peer-2-peer certificate distribution mechanism without infrastructure involved.
PICS_ECTL_SUPPORT	ITS-S can handle information provided in ECTL.
PICS_CRL_SUPPORT_CURRENT	ITS-S can handle information provided in CRL of the currently active RootCA.
PICS_CRL_SUPPORT_FOREIGN	ITS-S can handle information provided in CRL from other RootCAs.
PICS_CTL_SUPPORT	ITS-S can handle information provided in CTL.
PICS_ITSS_PKI_COMMUNICATION	ITS-S supports the PKI communication protocol (ETSI TS 102 941 [3]). Otherwise, the ITS-S is unable to participate in PKI test scenarios (clause 6.3).
PICS_ITSS_PKI_ENROLMENT	ITS-S supports the enrolment procedure described in PKI communication protocol (ETSI TS 102 941 [3]). Otherwise, the EC certificate shall be installed on the ITS-S manually.
PICS_ITSS_PKI_RE_ENROLMENT	ITS-S supports the re-enrolment procedure described in PKI communication protocol (ETSI TS 102 941 [3]).

4.1.3 PKI

Mandatory requirements:

- The CAs (RCA, EA, AA) shall support algorithms and key length according to the Certificate Policy [4].

Optional requirements:

PICS	Description
PICS_PKI_ITSS_NO_PRIVACY_REQ	ITS-S supports optional privacy requirement, e.g. RSU. The present PICS does not apply to most vehicular ITS-S.
PICS_PKI_ITSS_RENEW_AT	ITS-S is able to start the AT renewal procedure when all ATs in the pool are expired or about to be expired.
PICS_PKI_CA_MANAGEMENT	The CA (EA, AA) supports CA certificate request procedure. The RootCA supports certificate generation base on CA certificate request procedure.

4.1.4 TLM

Mandatory requirements:

- The TLM shall support algorithms and key length according to the Certificate Policy [4].

4.2 Configurations

4.2.1 CFG_SEC - ITS-S secured communication

This clause describes the configuration used to execute secure communication test scenarios. The configuration contains the following entities:

- Sender - The ITS-S playing a sender role.
- Receiver - The ITS-S playing a receiver role.
- Sender AA - The authorization authority that issued the sender's AT.

- Receiver AA - The authorization authority that issued the receiver's AT.

NOTE: The AA is involved to pre-test conditions only. The way how ATs are installed on the SUT are out of scope of this configuration. The same AA can issue ATs for both sender and receiver if not defined otherwise in the use-case description.

In order to participate in the test with the present configuration, ITS-S shall be configured as following if it is not explicitly defined in the use-case description:

- The ITS-S shall be configured to send CAMs in high frequency (more than one CAMs/second) so that the ITS-S sends some of the CAMs with digest instead of ATs.
- All participating ITS-Ss are in the "authorized" state (equipped with valid ATs).
- All ATs of participating ITS-Ss allow the transmission of CAMs and DENMs in the time and place of UC execution.
- All ATs of participating ITS-Ss shall be signed using a valid AA certificate issued by a trusted root certificate authority (RCA).
- All AA certificates used for signing ATs participating ITS-Ss shall be valid for the time and location of the UC execution.
- All RCA certificates used for signing AA certificates shall be valid for the time and location of the UC execution.
- All AA and RCA certificates shall permit issuing of AT certificates containing CAM and DENM PSID.
- No EA, AA or RCA certificates shall be revoked.
- All RCA certificates shall be included in the ECTL.
- All involved CA certificates shall be known and trusted by all participating ITS-S.

4.2.2 CFG_PKI - PKI communication

This clause describes the configuration used to execute PKI communication scenarios. The configuration contains the following entities:

- ITS-S - the ITS station triggering the scenario execution.
- EA - enrolment authority by which the ITS-S is enrolled.
- AA - authorization authority by which the ITS-S is authorized.
- RCA - root certificate authority issuing the EA and AA certificates.
- DC - distribution centres to provide RCA CTL and CRL.
- TLM/CPOC - trust list manager and central point of contacts.
- Observer - the ITS-S (or a network sniffer) allowing to detect that ITS-S is starting to send CAM messages.

NOTE 1: The RCA can be the issuer of both EA and AA.

The ITS-S shall be configured as following if another is not specified in the use-case description:

- The ITS-S shall be configured to send and receive CAMs using V2X communication.
- The ITS-S shall support the PKI communication protocol (see PICS_PKI_COMMUNICATION) defined in ETSI TS 102 941 [3].

The CAs (RCA, AA and EA) shall be configured as following if another is not specified in the use-case description:

- All participating RCA shall have RCA certificates included in the ECTL.

- All AA and EA shall have CA certificates signed by trusted RCA certificate.
- All CA certificates shall be valid for the time and location of the UC execution.
- All CA certificates shall permit issuing of certificates containing CAM and DENM PSID.
- No EA, AA or RCA certificates shall be revoked.
- All sub-CAs certificates shall be included in the CTL.

The TLM/CPOC shall be configured as following:

- TLM shall issue the ECTL containing all participating RCA.

The above configurations can be organized into three groups depending on the participants involved:

Configuration group	Participants involved
CFG_PKI_ENROLMENT	ITS-S, EA, Observer, [DC, TLM/CPOC]
CFG_PKI_AUTHORIZATION	ITS-S, EA, AA, Observer, [DC, TLM/CPOC]
CFG_PKI_CAs	EA, AA, RCA, [DC, TLM/CPOC]

NOTE 2: Connections to DCs and TLM/CPOC are optional in the scope of these tests. Information from ECTL and CTLs/CRLs can be delivered to participating devices using some other particular way.

5 Requirements to be tested

5.1 Overview

The clauses below collect and enumerate the requirements that can be tested with the present interoperability test specification.

5.2 ITS-S communication messages

NN	Requirement	References	UCs
1.1.	A sending ITS-S shall be able to correctly sign CAMs using valid AT certificates	ETSI TS 102 941 [3]	UC-1-1 UC-1-2 UC-1-3 UC-1-4 UC-1-5 UC-2-4 UC-2-5
1.2.	A receiving ITS-S shall be able to verify CAMs signed using valid AT certificates	ETSI TS 102 941 [3]	UC-1-1 UC-1-2 UC-1-3 UC-1-4 UC-1-5
1.3.	ITS-S shall be able to correctly handle (send and receive) CAMs signed with digests before and after transmission of the AT certificate	ETSI TS 102 941 [3]	UC-1-1 UC-1-2 UC-1-3 UC-1-4 UC-1-5
1.4.	ITS-S shall be able to check the timestamp of messages including the validity period of the used ATs	ETSI TS 102 941 [3]	UC-1-1 UC-1-2 UC-1-3 UC-1-4 UC-1-5 UC-2-2 UC-2-4 UC-2-5

NN	Requirement	References	UCs
1.5.	ITS-S shall be able to support peer-2-peer AA certificate distribution: • P2P request of AA certificate • P2P distribution of the requested AA certificate • Accepting of AA certificate received using P2P distribution	ETSI TS 102 941 [3] IEEE 1609.2a [2], clause 8	UC-1-3 UC-2-5
1.6.	ITS-Ss shall not transmit certificates using P2P distribution if another ITS-S already answered the request (discoverable by the sender)	ETSI TS 102 941 [3] IEEE 1609.2a [2], clause 8	UC-1-3 UC-2-5
1.7.	ITS-Ss shall be able to handle and verify DENMs signed with ATs containing certificate regional restrictions: id and circular	ETSI TS 102 941 [3]	UC-2-1
1.8.	ITS-Ss shall consider PSIDs and correspondent SSPs	ETSI TS 102 941 [3]	UC-1-1 UC-1-2 UC-1-3 UC-1-4 UC-1-5 UC-2-2 UC-2-5
1.9.	The ITS-S shall support algorithms and key length according to the EU Certificate Policy. This includes signing, verification, encryption and decryption	EU CP [4], clause 6.1.4	UC-1-1 UC-1-2 UC-1-3 UC-1-4 UC-1-5 UC-2-4 UC-2-5
1.10.	ITS-Ss shall consider CRLs	ETSI TS 102 941 [3]	UC-2-4
1.11.	ITS-Ss shall consider the whole certificate chain when verifying certificates	ETSI TS 102 941 [3]	UC-1-3 UC-2-5
1.12.	Correct change of pseudonyms, with respect to procedure, parameters, place and time	ETSI TR 103 415 [i.3] Table 4, EC CP/SP	UC-1-5

5.3 ECTL Handling

NN	Requirement	References	UCs
2.1.	Check the existence of the ECTL	ETSI TS 102 941 [3] EU Certificate Policy [4]	UC-1-4 UC-2-5 UC-2-3
2.2.	Check the expiration of the ECTL	ETSI TS 102 941 [3] EU Certificate Policy [4]	UC-1-4 UC-2-5 UC-2-3
2.3.	Check the delta ECTL handling	ETSI TS 102 941 [3] EU Certificate Policy [4]	
2.4.	Check the presence of the current root CA[1] certificate in the ECTL	ETSI TS 102 941 [3] EU Certificate Policy [4]	UC-1-4 UC-2-5 UC-2-3
2.5.	Check the presence of foreign root CA[1] certificate in the ECTL	ETSI TS 102 941 [3] EU Certificate Policy [4]	UC-1-4 UC-2-5 UC-2-3
2.6.	Handling ECTL signed using Brainpool P384r1 curve	ETSI TS 102 941 [3] EU Certificate Policy [4], clause 6.1.4	UC-1-4 UC-2-5 UC-2-3
NOTE: The meaning of current and foreign CA is defined in clause 3.1.			

5.4 RCA CTL Handling

NN	Requirement	References	UCs
3.1.	The ITS-S checks the RCA CTL for the Access Point of the EA	ETSI TS 102 941 [3]	UC-3-1 UC-3-2 UC-3-3 UC-3-4
3.2.	Handling CTL signed using any present crypto domain (NIST-P256, Brainpool P256r1, Brainpool P384r1)	ETSI TS 102 941 [3]	UC-3-1 UC-3-2 UC-3-3 UC-3-4 UC-4-1 UC-4-2 UC-4-3 UC-4-4 UC-4-5
3.3.	Check the RCA CTL for the Access Point of the AA	ETSI TS 102 941 [3]	UC-4-1 UC-4-2 UC-4-3 UC-4-4 UC-4-5

5.5 RCA CRL Handling

NN	Requirement	References	UCs
4.1.	Check the presence of the CRL from the current root CA	ETSI TS 102 941 [3]	UC-3-4 UC-4-4
4.2.	Check the presence of the CRL from the foreign root CA (different RCA case)	ETSI TS 102 941 [3]	UC-1-4 UC-3-4 UC-4-4
4.3.	Check the presence of the currently used AA certificate in the CRL from the current root CA	ETSI TS 102 941 [3]	UC-4-4
4.4.	Check the presence of the AA from remote ITS-S in the CRL of foreign root CA		UC-4-4
4.5.	Check the expiration of CRLs of current and foreign root CA		
4.6.	Check the presence of the current EA in the CRL of the EA's RCA		UC-3-4
4.7.	Handling CRL signed using any present crypto domain (NIST-P256, Brainpool P256r1, Brainpool 384r1)	ETSI TS 102 941 [3]	UC-1-4 UC-3-4 UC-4-4

5.6 PKI communication - Enrolment Management

NN	Requirement	References	UCs
5.1.	The EA shall be able to track the ITS-S lifecycle	ETSI TS 102 941 [3]	
5.2.	The EA shall be able to verify the presence of the ITS-S technical key in the local database	ETSI TS 102 941 [3]	UC-3-1 UC-3-2
5.3.	The EA shall be able to handle a correct Enrolment Request (valid enrolment behaviour)	ETSI TS 102 941 [3]	UC-3-1 UC-3-2
5.4.	The EA shall be able to handle an incorrect Enrolment Request (Canonical identity unknown - User not permitted to enrol - User authentication failed)	ETSI TS 102 941 [3] ETSI TS 102 731 [i.4]	UC-3-3
5.5.	The ITS-S is able to handle the CTL EA parameters in order to send requests to the *itsAccessPoint* URL if it is defined in the CTL	ETSI TS 102 941 [3]	UC-3-1 UC-3-2
5.6.	The ITS-S shall be able to do an initial Enrolment Request at the initialization of the ITS-S or after expiration of the previous EC	ETSI TS 102 941 [3]	
5.7.	The ITS-S shall be able to do a Re-enrolment Request using its current EC	ETSI TS 102 941 [3]; EU Certificate Policy [4] clause 7.2, Table 11	UC-3-2

5.7 PKI communication - Authorization Management

NN	Requirement	References	UCs
6.1.	The AA shall be able to handle the authorization request sent by an ITS-S	ETSI TS 102 941 [3]	UC-4-1 UC-4-2 UC-4-3 UC-4-5
6.2.	The AA shall only accept authorization requests with pop (proof of possession) signature in case of ITS-S with privacy requirements	ETSI TS 102 941 [3]	UC-4-1 UC-4-3 UC-4-5
6.3.	The AA shall be able to build and send the authorization validation request to the EA	ETSI TS 102 941 [3]	UC-4-1 UC-4-2 UC-4-3 UC-4-5
6.4.	The EA shall be able to validate the authorization validation request received from the AA: • Accept successful authorization validation request • Check that encrypted signature is used for AT requests from ITS-S with privacy requirements • Check the desired subject attributes in the certificate request • Check and update if necessary the validation period for the certificate	ETSI TS 102 941 [3]	UC-4-1 UC-4-2 UC-4-3 UC-4-5
6.5.	The EA shall be able to build and send an authorization validation response to the AA	ETSI TS 102 941 [3]	UC-4-1 UC-4-2 UC-4-3 UC-4-5
6.6.	The AA shall be able to build and send an authorization response to the ITS-S	ETSI TS 102 941 [3]	UC-4-1 UC-4-2 UC-4-3 UC-4-5
6.7.	The authorization response sent by AA shall follow the decision of the EA with respect to the authorization validation response	ETSI TS 102 941 [3]	UC-4-1 UC-4-2 UC-4-3 UC-4-5
6.8.	The ITS-S shall be able to build and send the authorization request	ETSI TS 102 941 [3]	UC-4-1 UC-4-2 UC-4-3 UC-4-5
6.9.	The ITS-S shall be able to build and send the authorization request containing region restriction certificate attribute	ETSI TS 102 941 [3]	UC-4-1 (optional) UC-4-2 (optional) UC-4-3 (optional) UC-4-5 (optional)
6.10.	The ITS-S shall be able to request several authorization tickets	ETSI TS 102 941 [3]	UC-4-5
6.11.	The AA shall accept authorization requests without encrypted EC signature in case of ITS-S without privacy requirements	ETSI TS 102 941 [3]	UC-4-2

5.8 PKI interoperability

NN	Requirement	References	UCs
7.1.	AA shall be able to communicate with EAs belonging to different RCAs when their corresponding Root CAs are trusted by ECTL and AA and EA both know the certificates and access points of each other.	ETSI TS 102 941 [3]	UC-4-3
7.2.	If the EA has two Access Points in the CTL, the AA shall choose the *aaAccessPoint* for its authorization validation request.	ETSI TS 102 941 [3]	UC-4-1 UC-4-2

6 Interoperability test descriptions

6.1 Overview

Interoperability test descriptions consist of three groups:

- ITS-S secured communication
- PKI communication
- CA certificate requests

These groups are described in the clauses below.

6.2 ITS-S secured communication

6.2.1 Successful basic communication

6.2.1.1 Use-case 1-1 - Both ITS-S authorized by the same AA

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC1-1		
Objective	Secure communication between ITS-S authorized by the same AA		
Description	Two ITS-S, authorized by the same AA, are sending CAMs and both accept these CAMs		
Configuration	The **CFG_SEC** configuration shall be used with additional requirements: • The ATs of all participating ITS-S are issued by the same AA		
Pre-test conditions			
REQ / PICS	**Tested Requirements**	**PICS**	
	1.1, 1.2, 1.3, 1.4, 1.8, 1.9		
Step	**Type**	**Description**	**Result**
1	Stimulus (by Sender)	The sender is triggered to send valid CAMs	
2	Verify (by Receiver)	The receiver validates received CAMs	All received CAMs are accepted by the receiving ITS-S

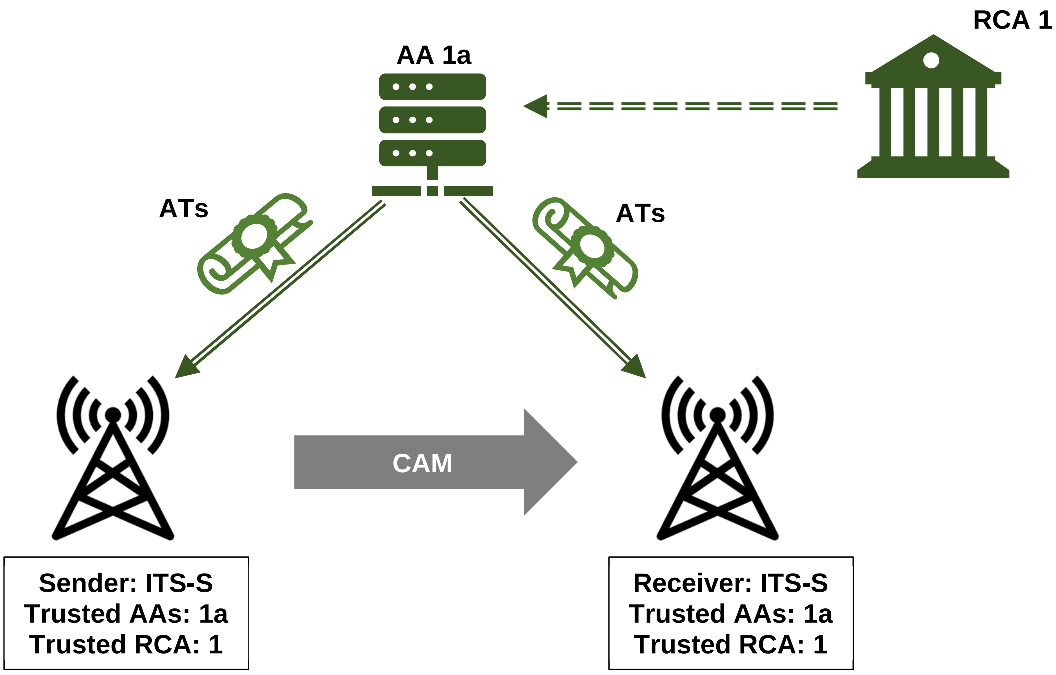


Figure 1: Secured communication when both ITS-S authorized by the same AA

6.2.1.2 Use-case 1-2 - Different AAs of the same PKI

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC1-2		
Objective	Secure communication between ITS-S authorized by different but commonly trusted AAs		
Description	Two ITS-S, authorized by different AA (belonging to the same RCA), are sending CAMs and both accept these CAMs		
Configuration	The **CFG_SEC** configuration shall be used with additional requirements: • Sender and receiver are authorized with ATs issued by different AAs belonging to the same RCA.		
Pre-test conditions			
REQ / PICS	**Tested Requirements**	**PICS**	
	1.1, 1.2, 1.3, 1.4, 1.8, 1.9		
Step	**Type**	**Description**	**Result**
1	Stimulus (by Sender)	The sender is triggered to send valid CAMs	
2	Verify (by Receiver)	The receiver validates the CAMs	All received CAMs are accepted by the receiving ITS-S

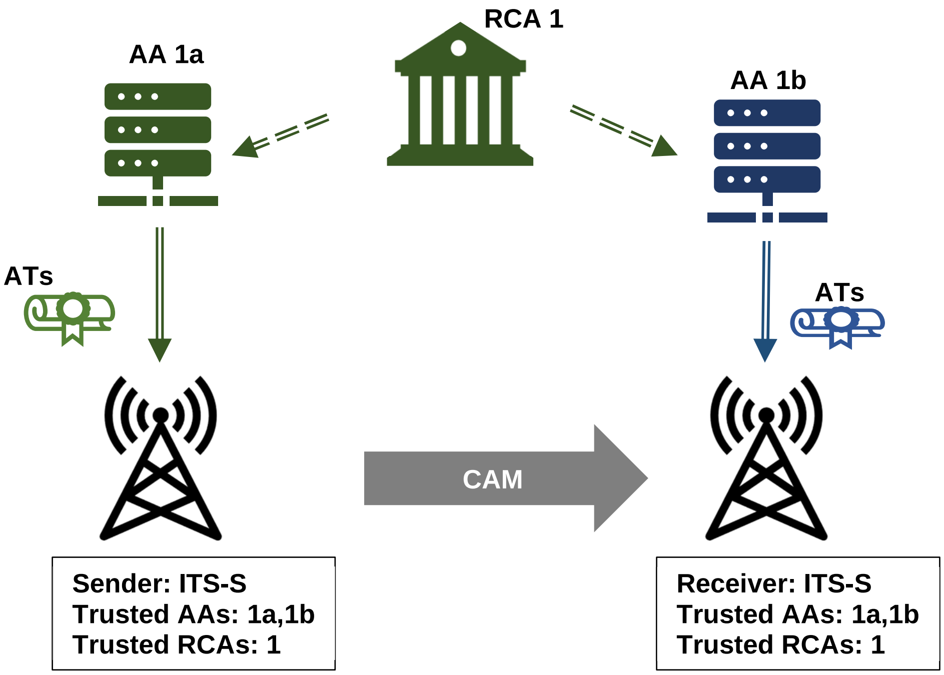


Figure 2: Secured communication when ITS-Ss was authorized by the different AAs of the same PKI

6.2.1.3 Use-case 1-3 - Peer-to-peer distribution of AA certificate

<table>
<tr><th colspan="3">Interoperability Test Description</th></tr>
<tr><td><b>Identifier</b></td><td colspan="2">TD_ITS_SEC_UC1-3</td></tr>
<tr><td><b>Objective</b></td><td colspan="2">Secure communication between ITS-S authorized by different and initially partially unknown AAs</td></tr>
<tr><td><b>Description</b></td><td colspan="2">Two ITS-S, authorized by different AA, are sending CAMs. The AA authorizing the sender is initially unknown from the receiver's perspective. The receiver therefore needs to request the AA certificate before trusting the received CAMs</td></tr>
<tr><td><b>Configuration</b></td><td colspan="2">The <b>CFG_SEC</b> configuration shall be used with the following additions:
• The ATs of the participating ITS-S are issued by different AAs.
• Both AA certificates are issued by the same commonly trusted RCA.
• The AA authorizing the sender is initially <b>unknown</b> from the receiver's perspective.
• The AA authorizing the receiver is <b>known</b> from the sender's perspective.</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Pre-test conditions</b></td><td colspan="2">• Ensure that no other ITS-S (beside the sender) in the surrounding will answered the AA certificate request (see note).</td></tr>
<tr><td><b>REQ / PICS</b></td><td><b>Tested Requirements</b></td><td><b>PICS</b></td></tr>
<tr><td></td><td>1.1, 1.2, 1.4, 1.5,
1.6 (see note),
1.8, 1.9, 1.11</td><td>Receiver: PICS_ITSS_REQUEST_AA
Sender: PICS_ITSS_RESPOND_AA</td></tr>
<tr><td colspan="3"></td></tr>
</table>

Interoperability Test Description			
Step	**Type**	**Description**	**Result**
1	Stimulus (by Sender)	• The sender is triggered to send valid CAMs.	
2	Verify (by Receiver)	The receiver validates the CAMs of the sender	• The CAM is **not** accepted by the receiving ITS-S (yet) because of the inability to verify the certificate chain of the signer due to the missing AA certificate.
3	Action (by Receiver)	• The receiver is adding a request for the missing AA certificate to its next CAM.	
4	Verify (by Sender)	The sender validates the CAMs of the receiver	• The CAM containing the request for the AA certificate is accepted by the receiving ITS-S.
5	Action (by Sender)	• The sender is appending the AA certificate to its next CAM.	
6	Verify (by Receiver)	The receiver validates the CAM of the sender containing the appended AA certificate	• The CAM is accepted by the receiving ITS-S (which is now able to verify the certificate chain).
NOTE: Depending on the circumstances of the test setup there might be multiple ITS-S listening to the channel and reacting on AA certificate requests. As the sender's devices will not append the AA certificate if another ITS-S already answered the request, the pre-condition needs to be fulfilled in order to complete the test sequence of the use case.			

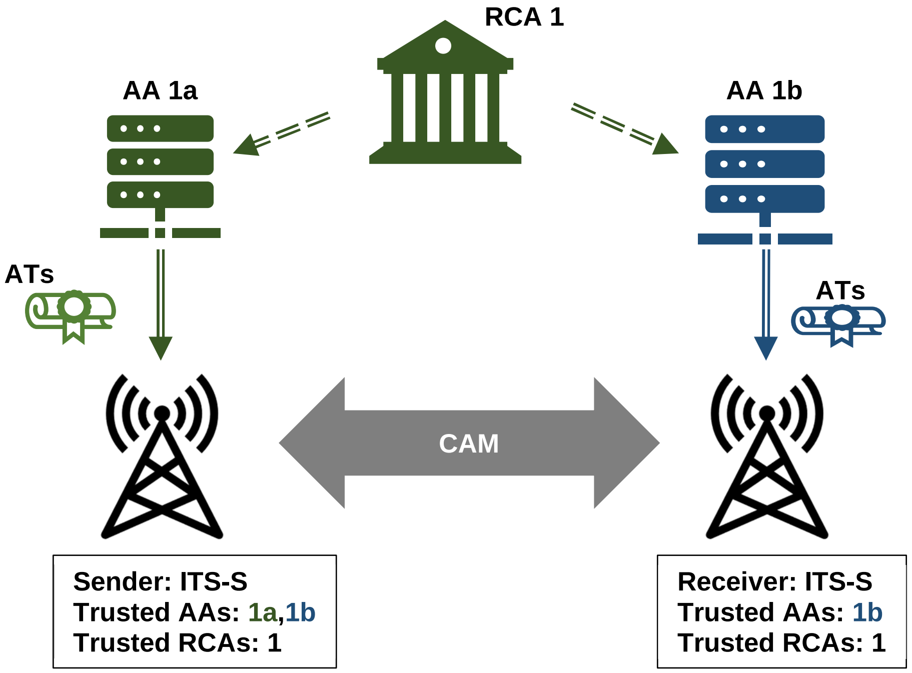


Figure 3: Peer-to-peer certificate distribution

6.2.1.4 Use-case 1-4 - Participating ITS-S are registered in different RCAs

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC1-4		
Objective	Secure communication between ITS-S authorized by AAs of different RCAs		
Description	Two ITS-S, authorized by AAs belonging to different RCAs, are sending CAMs and both accept these CAMs		
Configuration	The **CFG_SEC** configuration shall be used with the following additions: • The ATs of the participating ITS-S are issued by different AAs. • The sender AA certificate and the receiver AA certificate are issued by different, but commonly known and trusted RCAs.		
Pre-test conditions			
REQ / PICS	**Tested Requirements**	**PICS**	
	1.1, 1.2, 1.3, 1.4, 1.8, 1.9, 2.1, 2.2, 2.4, 2.5, 2.6		
Step	**Type**	**Description**	**Result**
1	Stimulus (by Sender)	• The sender is triggered to send valid CAMs.	
2	Verify (by Receiver)	The receiver validates the CAMs	• The CAM is accepted by the receiving ITS-S.

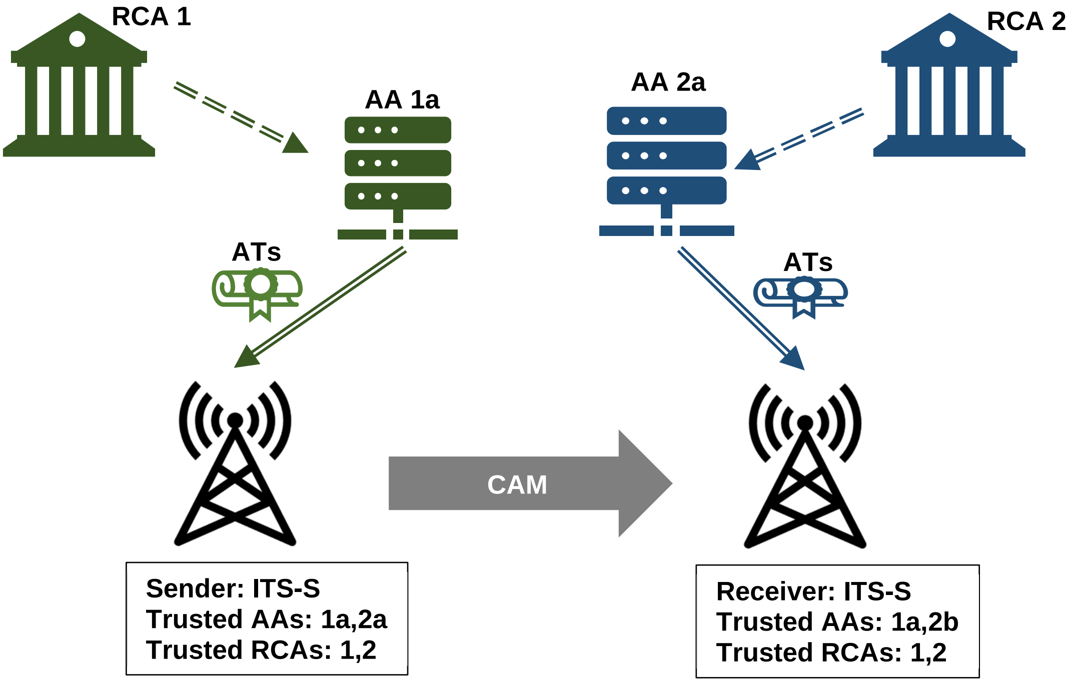


Figure 4: Secured communication using certificates from different PKIs

6.2.1.5 Use-case 1-5 - Pseudonym changing

<table>
<tr><th colspan="4">Interoperability Test Description</th></tr>
<tr><td><b>Identifier</b></td><td colspan="3">TD_ITS_SEC_UC1-5</td></tr>
<tr><td><b>Objective</b></td><td colspan="3">ITS-S are changing the ATs and related identifiers (pseudonym change) as expected</td></tr>
<tr><td><b>Description</b></td><td colspan="3">Two ITS-S, authorized by the same AA, are sending CAMs and both accept these CAMs. The two ITS-Stations are running the same GNSS simulation. The ITS-S shall perform pseudonym changes according to the EC CP/SP strategy. See ETSI TR 103 415 [i.3], Table 4</td></tr>
<tr><td><b>Configuration</b></td><td colspan="3">The <b>CFG_SEC</b> configuration shall be used with the following additions:
• The ATs of all participating ITS-S are issued by the same AA.
• The ITS-S are configured to use the GNSS simulation correspondent to selected certificate changing strategy.</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td><b>Pre-test conditions</b></td><td colspan="3">Both GNSS simulations, of sender and receiver, shall be set to the same starting point. It needs to be ensured that both ITS-Ss stay within communication range throughout the test</td></tr>
<tr><td rowspan="2"><b>REQ / PICS</b></td><td><b>Tested Requirements</b></td><td colspan="2"><b>PICS</b></td></tr>
<tr><td>1.1, 1.2, 1.3, 1.4, 1.8, 1.9, 1.11, 1.12</td><td colspan="2"></td></tr>
<tr><td colspan="4"></td></tr>
<tr><th>Step</th><th>Type</th><th>Description</th><th>Result</th></tr>
<tr><td rowspan="2">1</td><td>Stimulus
(by Sender)</td><td colspan="2">• The sender is triggered to send valid CAMs.
• The GNSS simulation is started.</td></tr>
<tr><td>Stimulus
(by Receiver)</td><td colspan="2">• The GNSS simulation is started (about the same time as the sender's simulation).</td></tr>
<tr><td rowspan="3">2</td><td>Verify
(by Receiver)</td><td>The receiver validates the CAMs throughout the whole GNSS simulation</td><td>• The CAMs are accepted by the receiving ITS-S</td></tr>
<tr><td>Action
(by Sender)</td><td colspan="2">The sender will perform pseudonym changes according to the change strategy</td></tr>
<tr><td>Verify
(by Receiver)</td><td>The receiver identifies pseudonym changes OR the receiver identifies the disappearance of the old sender and the subsequent appearance of a new sender</td><td>• Pseudonym changes of the sender are identified.
• The pseudonym changes happen according to the expected change strategy (e.g. within the expected time frame and section of the GNSS trace).</td></tr>
</table>

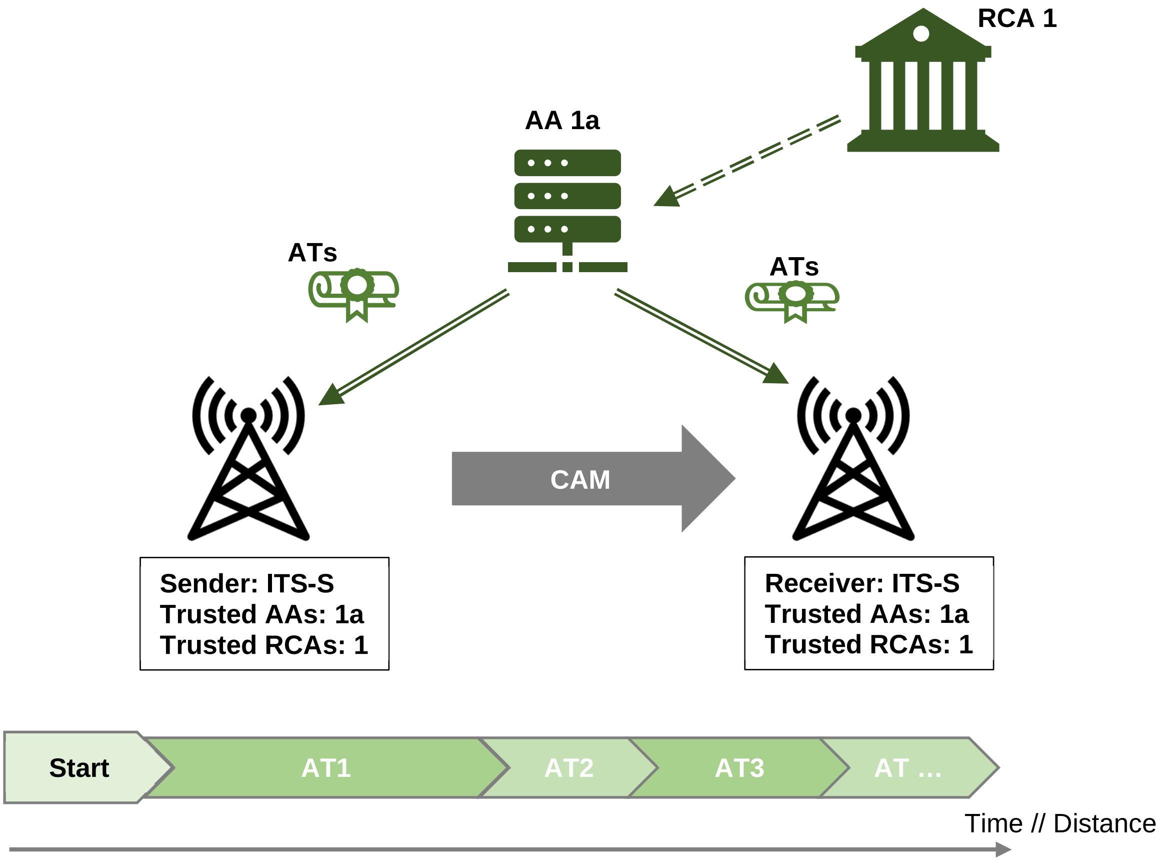


Figure 5: Pseudonym changing

6.2.2 Exceptional behaviour basic communication

6.2.2.1 Use-case 2-1 - Invalid certificate region

Interoperability Test Description		
Identifier	TD_ITS_SEC_UC2-1	
Objective	No communication between ITS-S within unauthorized regions	
Description	The sending ITS-S is triggered to send DENMs. The regional restrictions of the available ATs do not include the place of the UC execution	
Configuration	The **CFG_SEC** configuration shall be used with the following additions: • The ATs of all participating ITS-S are issued by the same AA. • All ATs available for the participating ITS-S have a regional restriction and are not authorized for the place of the UC execution. • The ITS-S are in the "authorized" state (equipped with valid ATs, besides not being authorized for the place of the UC execution).	
Pre-test conditions		
REQ / PICS	**Tested Requirements**	**PICS**
	1.7	PICS_ITSS_REGION_SUPPORT

Interoperability Test Description			
Step	**Type**	**Description**	**Result**
1	Stimulus (by Sender)	• The sender is triggered to send DENMs.	
2	Verify (by Receiver)	The receiver validates incoming DENMs	• **Either** no DENM is received (because the sender rejects sending out DENMs without proper permissions) - **preferred Result;** • **Or** a DENM of the sender is received and the DENM is **not** accepted by the receiving ITS-S (as the place of sending is not within the allowed regions of the AT used for authorizing the DENM).

6.2.2.2 Use-case 2-2 - Invalid ValidityPeriod of ATs

Interoperability Test Description		
Identifier	TD_ITS_SEC_UC2-2	
Objective	Rejected sending of CAMs if no AT with a valid ValidityPeriod is available	
Description	The sending ITS-S is triggered to send CAMs. The ValidityPeriod of all available ATs does not include the time of the UC execution (→ all ATs are either expired or not valid yet). See note	
Configuration	The **CFG_SEC** configuration shall be used with the following additions: • The ATs of all participating ITS-S are issued by the same AA. • All ATs available for the participating ITS-S are not valid at the time of the UC execution (either expired or not valid yet). • The ITS-S are in the "enrolled" state.	
Pre-test conditions	• The sending ITS-S shall not have the possibility to contact any AA to retrieve new ATs during the UC execution (→ the ITS-S shall be "offline").	
REQ / PICS	**Tested Requirements**	**PICS**
	1.4	

Step	**Type**	**Description**	**Result**
1	Stimulus (by Sender)	• The sender is triggered to send CAMs.	
2	Verify (by Receiver)	The receiver validates incoming CAMs	• **Either** no CAM is received (because the sender rejects sending out CAMs without valid ATs) - **preferred Result**; • **Or** a CAM of the sender is received and the CAM is **not** accepted by the receiving ITS-S (as the AT used for authorizing the CAM is not valid at the time of message creation).
NOTE: If all ATs are expired, the ITS-S is expected to return to the "enrolled" state.			

6.2.2.3 Use-case 2-3 - PSID exceptional behaviour

6.2.2.3.1 Use-case 2-3a - CAM PSID missing in ATs - rejected sending

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC2-3a		
Objective	Rejected sending of CAMs if ATs are missing the CAM PSID		
Description	The sending ITS-S is triggered to send CAMs. Its available ATs do not include the PSID for CAMs (36)		
Configuration	The **CFG_SEC** configuration shall be used with the following additions: • The ATs of all participating ITS-S are issued by the same AA. • All ATs available for the participating ITS-S do not include the PSID for CAMs. The ITS-S are in the "authorized" state (equipped with valid ATs, besides not being authorized for sending out CAMs).		
Pre-test conditions			
REQ / PICS	**Tested Requirements**	**PICS**	
	1.8		
Step	**Type**	**Description**	**Result**
1	Stimulus (by Sender)	• The sender is triggered to send CAMs.	
2	Verify (by Receiver)	The receiver validates incoming CAMs	• **Either** no CAM is received (because the sender rejects sending out CAMs without proper permissions) - **preferred Result**; • **Or** a CAM of the sender is received and the CAM is **not** accepted by the receiving ITS-S (as the AT used for authorizing the CAM does not have the PSID for doing so).

6.2.2.3.2 Use-case 2-3b - DENM PSID missing in ATs - rejected sending

Interoperability Test Description		
Identifier	TD_ITS_SEC_UC2-3b	
Objective	Rejected sending of DENMs if ATs are missing the DENM PSID	
Description	The sending ITS-S is triggered to send DENMs. Its available ATs do not include the PSID for DENMs (37)	
Configuration	The **CFG_SEC** configuration shall be used with the following additions: • The ATs of all participating ITS-S are issued by the same AA. • All ATs available for the participating ITS-S do not include the PSID for DENMs. • The ITS-S are in the "authorized" state (equipped with valid ATs, besides not being authorized for sending out DENMs).	
Pre-test conditions		
REQ / PICS	**Tested Requirements**	**PICS**
	1.8	

Interoperability Test Description			
Step	**Type**	**Description**	**Result**
1	Stimulus (by Sender)	• The sender is triggered to send DENMs.	
2	Verify (by Receiver)	The receiver validates incoming DENMs	• **Either** no DENM is received (because the sender rejects sending out DENMs without proper permissions) - **preferred Result**; • **Or** a DENM of the sender is received and the DENM is **not** accepted by the receiving ITS-S (as the AT used for authorizing the DENM does not have the PSID for doing so).

6.2.2.4 Use-case 2-4 - Using of AT issued by AA included in the CRL

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC2-4		
Objective	Rejection of CAMs authorized with ATs that are issued by a revoked AA		
Description	The receiving ITS-S does not know the AA that authorized the ATs of the sender. The signer identifier of the received AT refers to a revoked AA. Therefore the receiver does not request the AA certificate but ignores the received CAM		
Configuration	The **CFG_SEC** configuration shall be used with the following additions: • The ATs of the participating ITS-S are issued by different AAs. • The sender AA certificate is revoked. • The sender does not possess the current CRL (and therefore does not know that the AA is revoked). • The receiver is in possession of the current CRL (including the sender AA). • The AA authorizing the sender is **unknown** from the receiver's perspective (besides being included in the CRL). • The ITS-Ss are in the "authorized" state.		
Pre-test conditions	• Ensure that the sender is not able to retrieve the current CRL before and during the execution of the test.		
REQ / PICS	**Tested Requirements**	**PICS**	
	1.1, 1.4, 1.9, 1.10	PICS_CRL_SUPPORT_CURRENT OR PICS_CRL_SUPPORT_FOREIGN	
Step	**Type**	**Description**	**Result**
1	Stimulus (by Sender)	• The sender is triggered to send valid CAMs.	
2	Verify (by Receiver)	The receiver validates the CAMs of the sender	• The CAM is **not** accepted by the receiving ITS-S and the receiving ITS-S is **not** requesting the missing AA certificate.

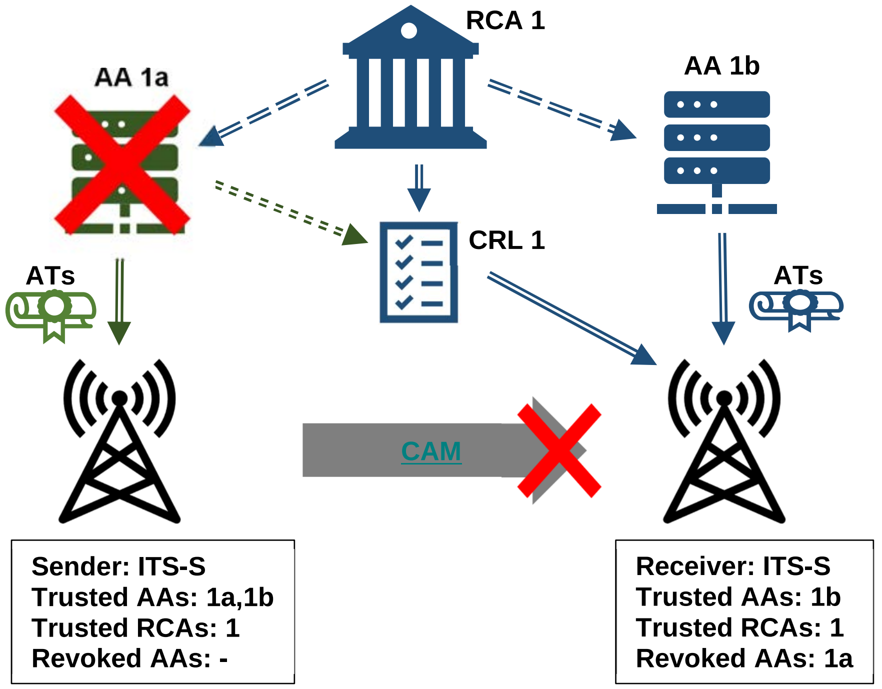


Figure 6: Secured communication using AT issued by AA included in the CRL

6.2.2.5 Use-case 2-5 - Unknown RCA

Interoperability Test Description		
Identifier	TD_ITS_SEC_UC2-5	
Objective	Rejection of messages of ITS-S belonging to an untrusted RCA	
Description	The receiving ITS-S does not know the RCA of the sender. The untrusted RCA is not part of the ECTL. The sender AA is not known, too, and needs to be requested	
Configuration	The **CFG_SEC** configuration shall be used with the following additions: • The ATs of the participating ITS-S are issued by different AAs. • The sender AA certificate is issued by an unknown RCA (not part of the ECTL). • The AA authorizing the sender is initially **unknown** from the receiver's perspective. • The AA authorizing the receiver is **known** from the sender's perspective. • The ITS-Ss are in the "authorized" state.	
Pre-test conditions	• Ensure that no other ITS-S (beside the sender) in the surrounding will answered the AA certificate request (see note).	
REQ / PICS	**Tested Requirements**	**PICS**
	1.1, 1.4, 1.5, 1.6 (see note), 1.8, 1.9, 1.11, 2.1, 2.2, 2.4, 2.5, 2.6	Receiver: PICS_ITSS_REQUEST_AA AND PICS_ECTL_SUPPORT Sender: PICS_ITSS_RESPOND_AA

Interoperability Test Description			
Step	**Type**	**Description**	**Result**
1	Stimulus (by Sender)	- The sender is triggered to send valid CAMs.	
2	Verify (by Receiver)	The receiver validates the CAMs of the sender	- The CAM is **not** accepted by the receiving ITS-S (yet) because of the inability to verify the certificate chain of the signer due to the missing AA certificate.
3	Action (by Receiver)	- The receiver is adding a request for the missing AA certificate to its next CAM.	
4	Verify (by Sender)	The sender validates the CAMs of the receiver	- The CAM containing the request for the AA certificate is accepted by the receiving ITS-S.
5	Action (by Sender)	- The sender is appending the AA certificate to its next CAM.	
6	Verify (by Receiver)	The receiver validates the CAM of the sender containing the appended AA certificate	- The CAM is **not** accepted by the receiving ITS-S (which is now able to check the certificate chain and detect the unknown RCA).
NOTE:	Depending on the circumstances of the test setup there might be multiple ITS-S listening to the channel and reacting on AA certificate requests. As the sender's devices will not append the AA certificate if another ITS-S already answered the request, the pre-condition needs to be fulfilled in order to complete the test sequence of the use case.		

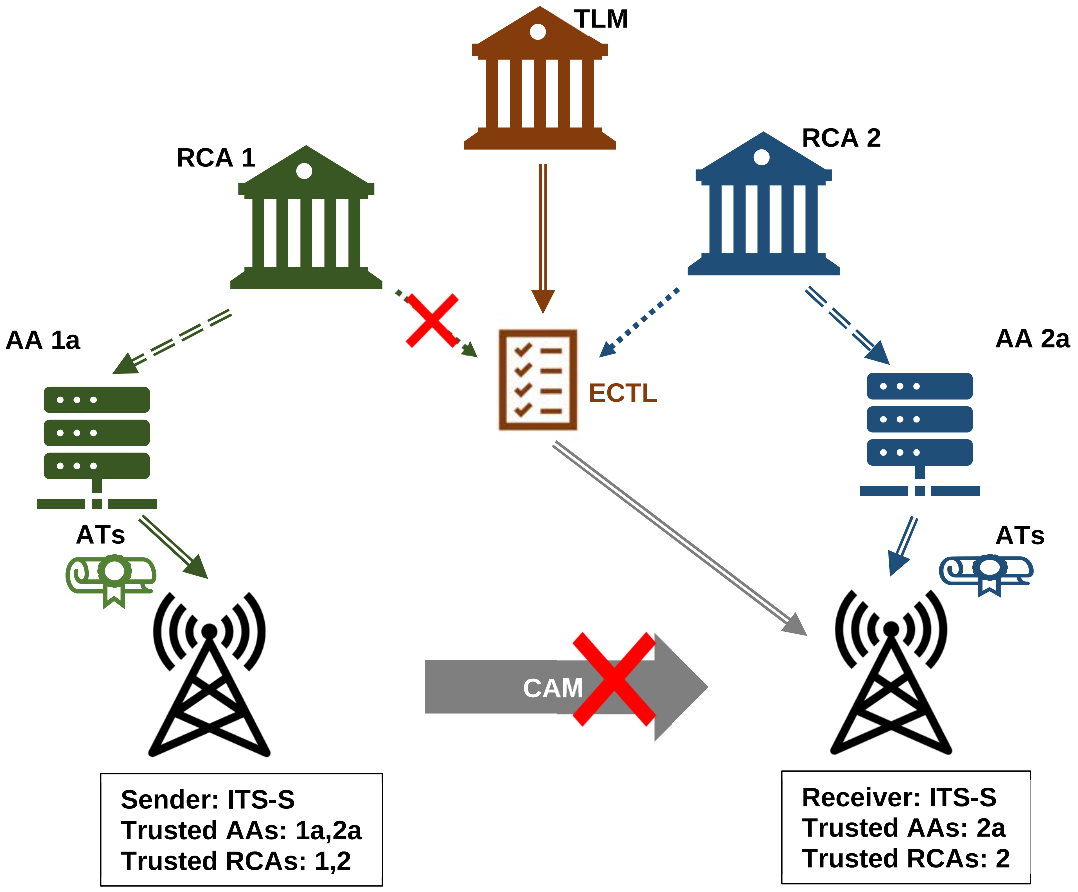


Figure 7: Secured communication when unknow RCA is not included in the ECTL

6.3 PKI communication

6.3.0 Overview

Interoperability tests for PKI communication can be accomplished through a sequence of the UCs below. Comprehensive scenarios (see clause 6.4) including a sequence of use cases shall describe the ITS-S and PKI communications as a whole, starting with enrolment, authorization by the same or different AA, and finally sending a first message (CAM or DENM).

6.3.1 Enrolment behaviour

6.3.1.1 Use-case 3-1 - Valid enrolment behaviour

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC3-1		
Objective	Valid enrolment behaviour.		
Description	ITS-S stations "senders" are registered to their PKI. Check that the EC certificate is received when the enrolment process is triggered on the ITS-S "sender". It is recommended for the PKI to issue the CTL containing EA entry with EA certificate and one or two access points URLs.		
Configuration	The **CFG_PKI_ENROLMENT** configuration shall be used with additional requirements: • The ITS-S is in the "Initialized and Unenrolled" state (registered to the EA).		
Pre-test conditions			
REQ / PICS	**Requirements**	**PICS**	
	3.1, 3.2, 5.2, 5.3, 5.5	PICS_ITSS_PKI_ENROLMENT	
Step	**Type**	**Description**	**Result**
1	Stimulus	ITS-S is triggered to send Enrolment request.	
2	Action	ITS-S sends the valid Enrolment Request message.	
3	Verify	The EA validates the enrolment request message.	The enrolment request is valid.
4	Action	EA generates and sends enrolment credential EC.	
5	Verify	ITS-S receives and validates the EC.	The EC is valid.

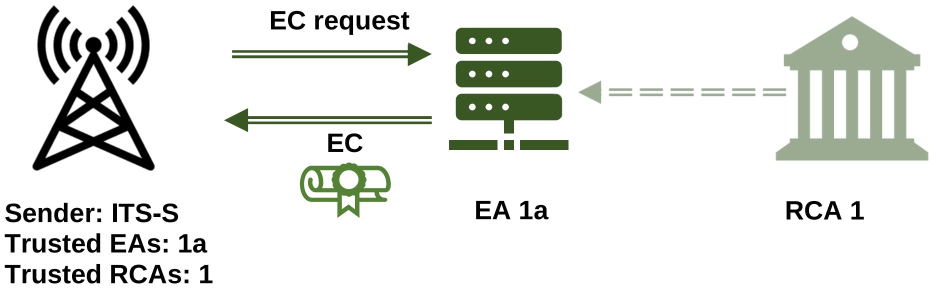


Figure 8: Valid enrolment behaviour

6.3.1.2 Use-case 3-2 - Enrolment behaviour with already enrolled station

Interoperability Test Description	
Identifier	TD_ITS_SEC_UC3-2
Objective	Valid re-enrolment behaviour.
Description	ITS-S stations "senders" are registered to their PKI and was already enrolled. Check that the new EC certificate is received when the enrolment process is triggered on the ITS-S.
Configuration	The **CFG_PKI_ENROLMENT** configuration shall be used with additional requirements: • The ITS-S is in the "Enrolled and Unauthorized" state (has a valid EC).

Interoperability Test Description			
Pre-test conditions			
REQ / PICS	**Requirements**	**PICS**	
	3.1, 3.2, 5.2, 5.3, 5.5, 5.7	PICS_ITSS_PKI_ENROLMENT PICS_ITSS_PKI_RE_ENROLMENT	
Step	**Type**	**Description**	**Result**
1	Stimulus	ITS-S is triggered to send re-Enrolment request.	
2	Action	ITS-S sends the valid re-Enrolment Request message.	
3	Verify	The EA validates the re-enrolment request message.	The re-enrolment request is valid.
4	Action	EA generates and sends new enrolment credential EC.	
5	Verify	ITS-S receives and validates the new EC.	The new EC is valid.

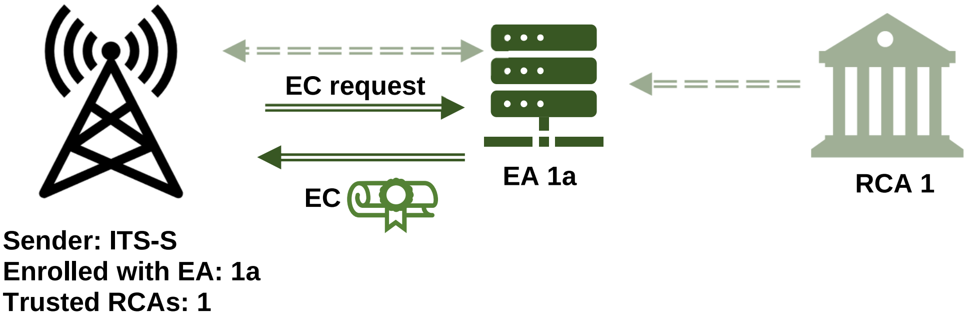


Figure 9: Enrolment behaviour with already enrolled station

6.3.1.3 Use-case 3-3 - Enrolment behaviour when ITS-S is not registered on the EA

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC3-3		
Objective	Enrolment behaviour when ITS-S is not registered on the EA.		
Description	ITS-S stations are not registered into their PKI. Check that the new EC certificate is not received when the enrolment process is triggered on the ITS-S.		
Configuration	The **CFG_PKI_ENROLMENT** configuration shall be used with additional requirements: • The ITS-S is in the "Initialized and Unenrolled" state (Not registered to the EA).		
Pre-test conditions			
REQ / PICS	**Requirements**	**PICS**	
	3.1, 3.2, 5.4	PICS_ITSS_PKI_ENROLMENT	
Step	**Type**	**Description**	**Result**
1	Stimulus	The ITS-S is triggered to send Enrolment request.	
2	Action	ITS-S sends the valid Enrolment Request message.	
3	Verify	The EA rejects the enrolment request message.	The enrolment request is not valid.
4	Action	EA returns the Enrolment Response Code *unknownits.*	
5	Verify	ITS-S receives the enrolment response code.	ITS-S remains in the "Initialized and Unenrolled" state.

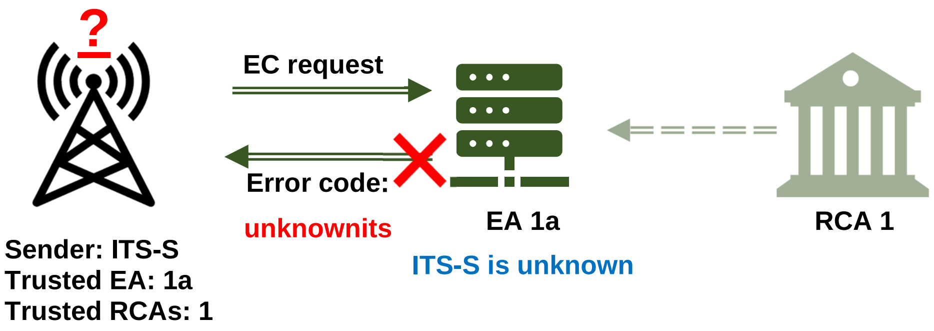


Figure 10: Enrolment behaviour when ITS-S is not registered on the EA

6.3.1.4 Use-case 3-4 - Enrolment behaviour when EA is on the CRL

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC3-4		
Objective	Enrolment behaviour when EA is on the CRL.		
Description	ITS-S stations are registered to their PKI and the corresponding EA was included into the CRL. Check that the ITS-S does not send the enrolment request when triggered or does not consider received EC certificate.		
Configuration	The **CFG_PKI_ENROLMENT** configuration shall be used with additional requirements: • The ITS-S is in the "Initialized and Unenrolled" state. The EA is on the CRL.		
Pre-test conditions			
REQ / PICS	**Requirements**	**PICS**	
	3.1, 3.2, 4.1, 4.6, 0	PICS_ITSS_PKI_ENROLMENT	
Step	**Type**	**Description**	**Result**
1	Stimulus	The ITS-S is triggered to send Enrolment request.	
2a	Verify	ITS-S checks the CRL and detects that the EA is revoked.	ITS-S does not send the Enrolment Request message.
OR			
2b	Action	ITS-S sends the valid Enrolment Request message.	
3	Verify	The revoked EA verifies the enrolment request message.	The enrolment request is valid.
4	Action	The revoked EA generates and sends enrolment credential EC.	
5	Verify	ITS-S receives the EC and verifies that the EA is revoked according to the CRL.	ITS-S rejects the received certificate.
FINALLY			
6	Verify		**ITS-S is not enrolled.**
NOTE: The main goal of the test sequence here is having the ITS-S with the "Unenrolled" state at the end of the execution, which could be done in two different ways. Depending on the circumstances of the test setup, the participants are free to run either the first sub-sequence (Steps: 1, 2a, 6) or the second one (Steps: 1, 2b, 3, 4, 5, 6).			

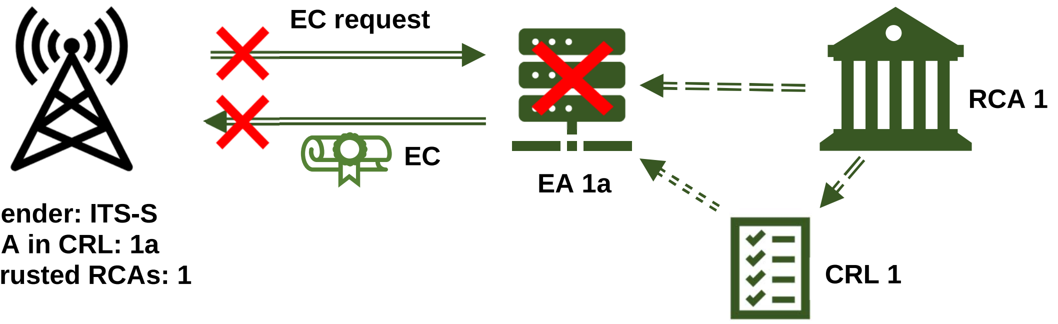


Figure 11: Enrolment behaviour when EA is on the CRL

6.3.2 Authorization behaviour

6.3.2.1 Use-case 4-1 - Valid authorization behaviour

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC4-1		
Objective	Valid authorization behaviour.		
Description	ITS-S stations are enrolled to their PKI. Check that the AT certificate is received when the authorization process is triggered on the ITS-S and ITS-S sends AT request with encrypted EC signature. It is recommended to use prove of possession for AT requests; otherwise AT requests may be rejected by PKIs. See note.		
Configuration	The **CFG_PKI_AUTHORIZATION** configuration shall be used with additional requirements: • The ITS-S is in the "Enrolled and Unauthorized" state.		
Pre-test conditions			
REQ / PICS	**Requirements**	**PICS**	
	3.2, 3.3, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (optional), 7.2		
Step	**Type**	**Description**	**Result**
1	Stimulus	The ITS-S is triggered to send Authorization Request.	
2	Action	ITS-S sends the valid Authorization Request message With PoP.	
3	Verify	The AA validates the Authorization Request message With PoP.	The Authorization Request is valid.
4	Action	The AA sends the Authorization Validation Request message to the EA using the *aaAccessPoint* available in the *EaEntry*.	
5	Verify	The EA verifies the Authorization Validation Request message.	The Authorization Validation Request is valid.
6	Action	The EA sends the Authorization Validation Response.	
7	Verify	The AA verifies the Authorization Validation Response.	The Authorization Validation Response is valid.
8	Action	The AA generates and sends the Authorization ticket AT.	
9	Verify	ITS-S receives and verifies the authorization ticket AT.	The AT is valid.
10	Stimulus	The ITS-S is triggered to send a CAM.	
11	Action	The ITS-S broadcasts a CAM signed with AT.	
NOTE: This test can be run after UC3-1 or UC3-2 as part of the sequential test scenarios PKI_SC1-1 or PKI_SC1-2 (see Table 1).			

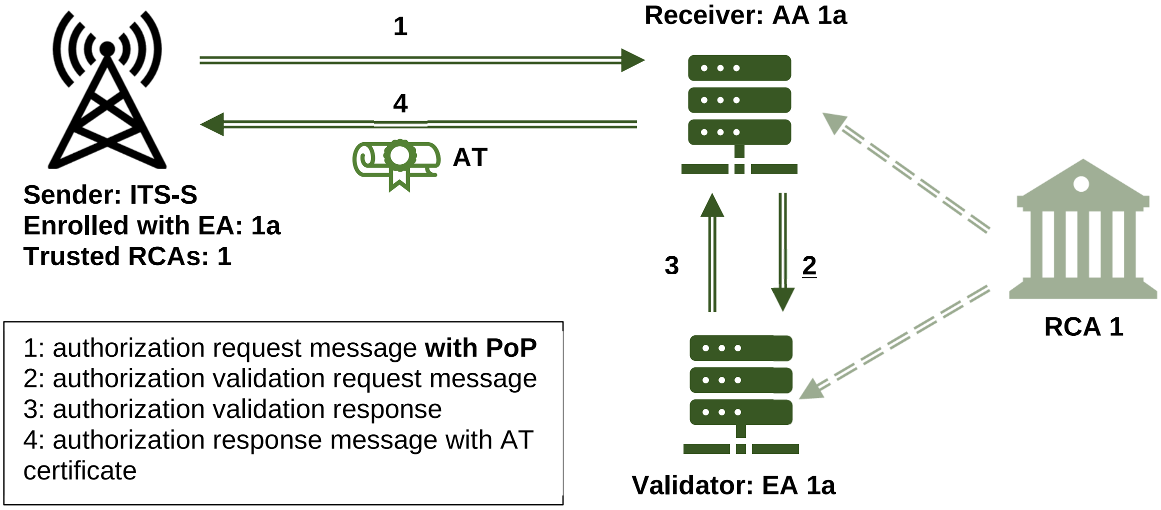

1
Receiver: AA 1a
4
AT
Sender: ITS-S
Enrolled with EA: 1a
Trusted RCAs: 1
3
2
RCA 1
1: authorization request message **with PoP**
2: authorization validation request message
3: authorization validation response
4: authorization response message with AT certificate
Validator: EA 1a

Figure 12: Valid authorization behaviour

6.3.2.2 Use-case 4-2 - Authorization behaviour with optional privacy requirements

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC4-2		
Objective	Authorization behaviour with optional privacy requirements.		
Description	ITS-S stations are registered at the PKI with optional privacy requirement. Check that the AT certificate is received when the authorization process is triggered on the ITS-S and ITS-S sends AT request with unencrypted EC signature. See note.		
Configuration	The **CFG_PKI_AUTHORIZATION** configuration shall be used with additional requirements: • The ITS-S is in the "Enrolled and Unauthorized" state. • The ITS-S is configured to send valid authorization request message with unencrypted EC signature.		
Pre-test conditions			
REQ / PICS	**Requirements**	**PICS**	
	3.2, 3.3, 6.1, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (optional), 6.11, 7.2	PICS_PKI_ITSS_NO_PRIVACY_REQ	
Step	**Type**	**Description**	**Result**
1	Stimulus	The ITS-S is triggered to send Authorization Request.	
2	Action	ITS-S sends the valid Authorization Request message with unencrypted EC signature.	
3	Verify	The AA validates the Authorization Request message with unencrypted EC signature.	The Authorization Request is valid.
4	Action	The AA sends the Authorization Validation Request message to the EA using the *aaAccessPoint* available in the *EaEntry*.	
5	Verify	The EA verifies the Authorization Validation Request message.	The Authorization Validation Request is valid.
6	Action	The EA sends the Authorization Validation Response.	
7	Verify	The AA verifies the Authorization Validation Response.	The Authorization Validation Response is valid.
8	Action	The AA generates and sends the Authorization ticket AT.	
9	Verify	ITS-S receives and verifies the authorization ticket AT.	The AT is valid.
10	Stimulus	The ITS-S is triggered to send a CAM.	
11	Action	The ITS-S broadcasts a CAM signed with AT.	
NOTE: This Use Case might only apply to a specific type of participating ITS-S (those without privacy requirements). For the other ITS-S, this Use Case is to be skipped.			

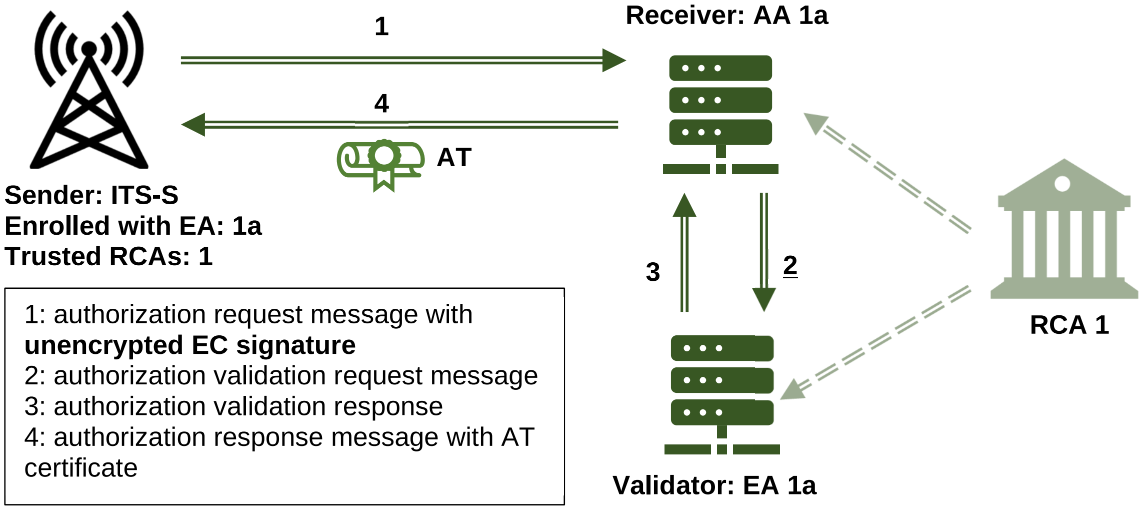
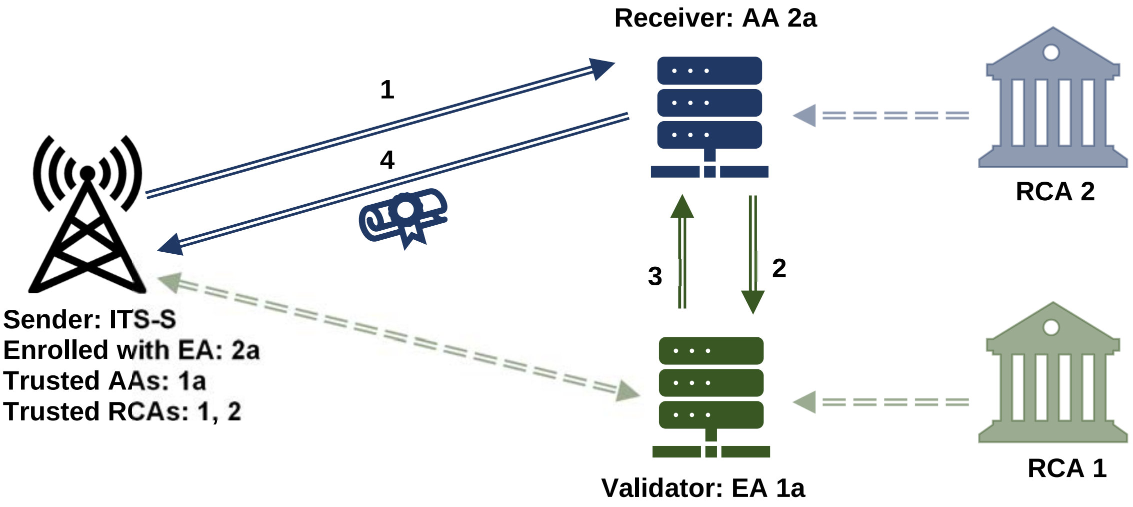

1
4
AT
Receiver: AA 1a
Sender: ITS-S
Enrolled with EA: 1a
Trusted RCAs: 1
3
2
RCA 1
1: authorization request message with **unencrypted EC signature**
2: authorization validation request message
3: authorization validation response
4: authorization response message with AT certificate
Validator: EA 1a

Figure 13: Authorization behaviour with optional privacy requirements

6.3.2.3 Use-case 4-3 - Authorization behaviour when AA and EA are from different PKI

Interoperability Test Description		
Identifier	TD_ITS_SEC_UC4-3	
Objective	Authorization behaviour when AA and EA are from different PKI.	
Description	ITS-S station is registered at one PKI and sends AT request to AA of another PKI. The AA shall send AT validation request to the EA of the first PKI and answer with AT certificate. CAs may belong to different cryptographic domains (NIST, Brainpool).	
Configuration	The **CFG_PKI_AUTHORIZATION** configuration shall be used with additional requirements: • The ITS-S is in the "Enrolled and Unauthorized" state by the first PKI. • The ITS-S has a valid enrolment credential EC issued by the EA from the first PKI. • The AA has a valid certificate issued by the RCA of the second PKI. • CTL-1 from first PKI is available and contains *EaEntry.* CTL-2 from second PKI is available and contains *AaEntry*.	
Pre-test conditions		
REQ / PICS	**Requirements**	**PICS**
	3.2, 3.3, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (optional), 7.1, 2.1, 2.2, 2.4, 2.5, 2.6	PICS_ECTL_SUPPORT

Interoperability Test Description			
Step	**Type**	**Description**	**Result**
1	Stimulus	The ITS-S is triggered to send Authorization Request to AA form second PKI.	
2	Action	ITS-S send the valid Authorization Request message With PoP to A from second PKI.	
3	Verify	The AA from second PKI verifies the Authorization Request message With PoP.	The Authorization Request is valid.
4	Action	The AA from second PKI sends the Authorization Validation Request message to the EA from first PKI using the *aaAccessPoint* available in the *EaEntry* from CTL-1.	
5	Verify	The EA from first PKI verifies the Authorization Validation Request message.	The Authorization Validation Request is valid.
6	Action	The EA from first PKI sends the Authorization Validation Response.	
7	Verify	The AA from second PKI verifies the Authorization Validation Response.	The Authorization Validation Response is valid.
8	Action	The AA from second PKI generates and sends the Authorization ticket AT.	
9	Verify	ITS-S receives and verifies the authorization ticket AT.	The AT is valid.
10	Stimulus	The ITS-S is triggered to send a CAM.	
11	Action	The ITS-S broadcasts a CAM signed with AT.	



1: authorization request message with **PoP**
2: authorization validation request message
3: authorization validation response
4: authorization response message with AT certificate

Figure 14: Authorization behaviour when AA and EA are from different PKI

6.3.2.4 Use-case 4-4 - Authorization behaviour when AA is on the CRL

Interoperability Test Description	
Identifier	TD_ITS_SEC_UC4-4
Objective	Authorization behaviour when AA is on the CRL.
Description	ITS-S stations are registered to their PKI and the corresponding AA was included into the CRL. Check that the ITS-S does not send the authorization request to this AA when triggered or does not consider received AT certificate received from this AA.
Configuration	The **CFG_PKI_AUTHORIZATION** configuration shall be used with additional requirements: • The ITS-S is in the "Enrolled and Unauthorized" state. The AA is on the CRL.

Interoperability Test Description			
Pre-test conditions			
REQ / PICS	**Requirements**		**PICS**
	3.2, 3.3, 4.1, 4.3		
Step	**Type**	**Description**	**Result**
1	Stimulus	The ITS-S is triggered to send Authorization Request.	
2a	Verify	ITS-S checks the CRL and detects that the AA is revoked.	ITS-S does not send the Authorization Request message.
OR			
2b	Action	ITS-S sends the valid Authorization Request message With PoP.	
3	Verify	The AA validates the Authorization Request message With PoP.	The Authorization Request is valid.
4	Action	The AA sends the Authorization Validation Request message to the EA using the *aaAccessPoint* available in the *EaEntry*.	
5	Verify	The EA verifies that the AA is revoked.	The EA rejects the Authorization Validation Request.
6	Action	The AA returns an error code.	
OR			
2c	Action	ITS-S sends the valid Authorization Request message With PoP.	
3	Verify	The AA validates the Authorization Request message With PoP.	The Authorization Request is valid.
4	Action	The AA sends the Authorization Validation Request message to the EA using the *aaAccessPoint* available in the *EaEntry*.	
5	Verify	The EA verifies the Authorization Validation Request message.	The Authorization Validation Request is valid.
6	Action	The EA sends the Authorization Validation Response.	
7	Verify	The AA verifies the Authorization Validation Response.	The Authorization Validation Response is valid.
8	Action	The AA generates and sends the Authorization ticket AT.	
9	Verify	ITS-S receives the AT and verifies that the AA is revoked according to the CRL.	ITS-S rejects the received certificate.
FINALLY			
10	Verify		**ITS-S is not authorized.**
NOTE: The main goal of the test sequence here is having the ITS-S with the "Unauthorized" state at the end of the execution, which could be done in three different ways. Depending on the circumstances of the test setup, the participants are free to run either the first sub-sequence (Steps: 1, 2a, 10), the second sub-sequence (Steps: 1, 2b, 3, 4, 5, 6, 10) or the third one (Steps: 1, 2c, 3, 4, 5, 6, 7, 8, 9, 10).			

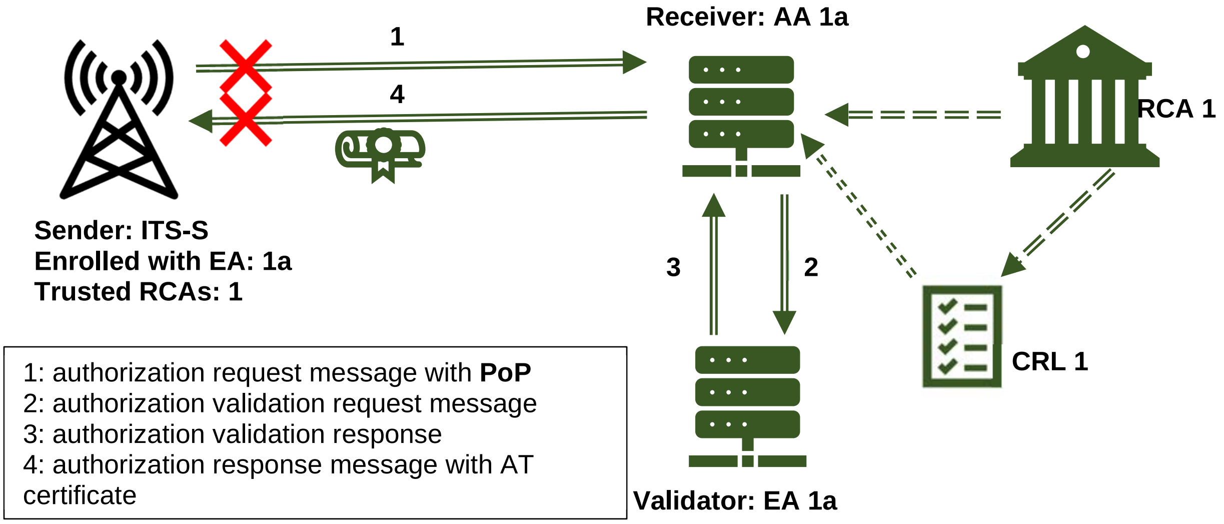

Receiver: AA 1a
1
4
RCA 1
Sender: ITS-S
Enrolled with EA: 1a
Trusted RCAs: 1
3
2
CRL 1
1: authorization request message with **PoP**
2: authorization validation request message
3: authorization validation response
4: authorization response message with AT certificate
Validator: EA 1a

Figure 15: Authorization behaviour when AA is on the CRL

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC4-4a		
Objective	Authorization behaviour with AA from another PKI when AA is on the CRL.		
Description	ITS-S stations are registered to their PKI and configured to use the revoked AA of another PKI for authorization. Check that the ITS-S does not send the authorization request to this AA when triggered or does not consider received AT certificate received from this AA. See note 1.		
Configuration	The **CFG_PKI_AUTHORIZATION** configuration shall be used with additional requirements: • The ITS-S is in the "Enrolled and Unauthorized" state. • The ITS-S is configured to use the AA from another PKI for authorization. The AA from another PKI is on the CRL.		
Pre-test conditions			
REQ / PICS	**Requirements**	**PICS**	
	3.2, 3.3, 4.1, 4.3		
Step	**Type**	**Description**	**Result**
1	Stimulus	The ITS-S is triggered to send Authorization Request.	
2a	Verify	ITS-S checks the CRL and detects that the AA is revoked.	ITS-S does not send the Authorization Request message.
OR			
2b	Action	ITS-S sends the valid Authorization Request message With PoP.	
3	Verify	The AA validates the Authorization Request message With PoP.	The Authorization Request is valid.
4	Action	The AA sends the Authorization Validation Request message to the EA using the *aaAccessPoint* available in the *EaEntry* of the CTL of the PKI where ITS-S is enrolled.	
5	Verify	The EA verifies that the AA is revoked.	The EA rejects the Authorization Validation Request.
6	Action	The AA returns an error code.	
OR			
2c	Action	ITS-S sends the valid Authorization Request message With PoP.	
3	Verify	The AA validates the Authorization Request message With PoP.	The Authorization Request is valid.
4	Action	The AA sends the Authorization Validation Request message to the EA using the *aaAccessPoint* available in the *EaEntry*.of the CTL of the PKI where ITS-S is enrolled.	
5	Verify	The EA verifies the Authorization Validation Request message.	The Authorization Validation Request is valid.
6	Action	The EA sends the Authorization Validation Response.	
7	Verify	The AA verifies the Authorization Validation Response.	The Authorization Validation Response is valid.
8	Action	The AA generates and sends the Authorization ticket AT.	
9	Verify	ITS-S receives the AT and verifies that the AA is revoked according to the CRL.	ITS-S rejects the received certificate.
FINALLY			
10	Verify		**ITS-S is not authorized.**
NOTE 1: The main goal of the test sequence here is having the ITS-S with the "Unauthorized" state at the end of the execution, which could be done in three different ways. Depending on the circumstances of the test setup, the participants are free to run either the first sub-sequence (Steps: 1, 2a, 10), the second sub-sequence (Steps: 1, 2b, 3, 4, 5, 6, 10) or the third one (Steps: 1, 2c, 3, 4, 5, 6, 7, 8, 9, 10). NOTE 2: The behaviour of the present use-case is identical to the behaviour of the use-case 4-4.			

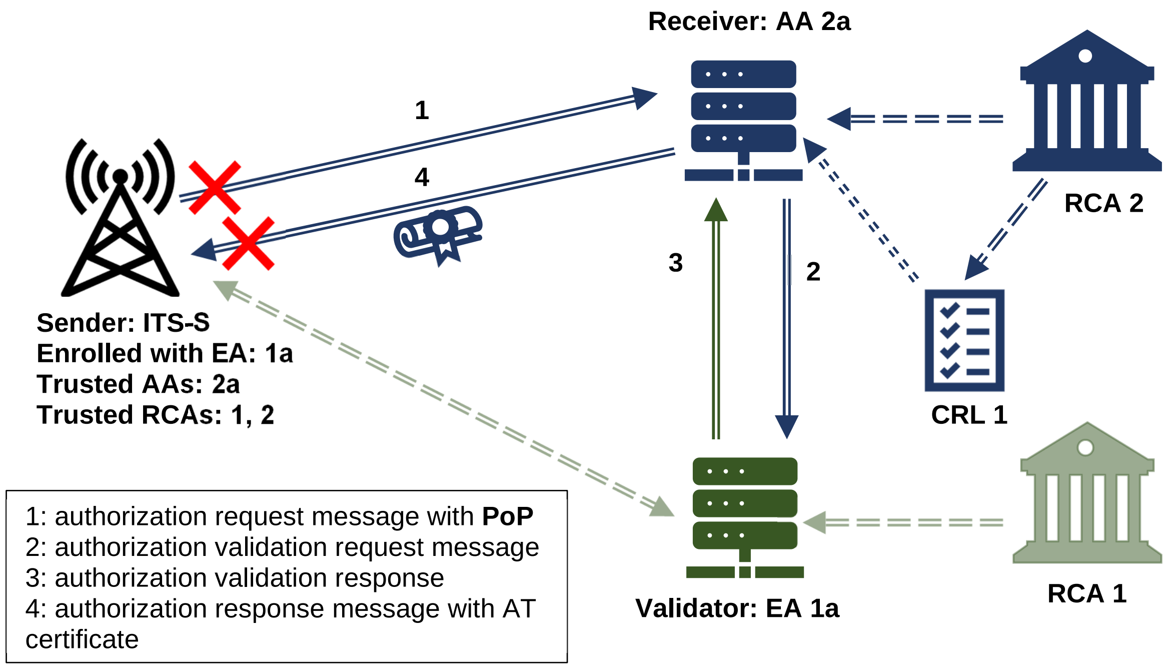

Receiver: AA 2a
1
4
3
2
RCA 2
CRL 1
Sender: ITS-S
Enrolled with EA: 1a
Trusted AAs: 2a
Trusted RCAs: 1, 2
Validator: EA 1a
RCA 1
1: authorization request message with PoP
2: authorization validation request message
3: authorization validation response
4: authorization response message with AT certificate

Figure 16: Authorization behaviour with AA from another PKI when AA is on the CRL

6.3.2.5 Use-case 4-5 - Check renewal of expired AT certificates

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC4-5		
Objective	Check renewal of expired AT certificates.		
Description	Check that ITS-S requests for new AT when all ATs in the pool are expired or about to be expired. See note.		
Configuration	The **CFG_PKI_AUTHORIZATION** configuration shall be used with additional requirements: The ITS-S is in the "Authorized" state already.		
Pre-test conditions			
REQ / PICS	**Requirements**	**PICS**	
	3.2, 3.3, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (optional), 6.10	PICS_PKI_ITSS_RENEW_AT	
Step	**Type**	**Description**	**Result**
1	Stimulus	The ITS-S is triggered to send Authorization Request when their ATs are expired or to be expired.	
2	Action	ITS-S sends the valid Authorization Request message With PoP.	
3	Verify	The AA validates the Authorization Request message With PoP.	The Authorization Request is valid.
4	Action	The AA sends the Authorization Validation Request message to the EA using the *aaAccessPoint* available in the *EaEntry*.	
5	Verify	The EA verifies the Authorization Validation Request message.	The Authorization Validation Request is valid.
6	Action	The EA sends the Authorization Validation Response.	
7	Verify	The AA verifies the Authorization Validation Response.	The Authorization Validation Response is valid.
8	Action	The AA generates and sends the Authorization ticket AT.	
9	Verify	ITS-S receives and verifies the authorization ticket AT.	The AT is valid.
10	Stimulus	The ITS-S is triggered to send a CAM.	
11	Action	The ITS-S broadcasts a CAM signed with AT.	
NOTE: This test can be run after UC3-1 or UC3-2 and UC4-1 as part of the sequential test scenarios PKI_SC1-3 (see Table 1).			

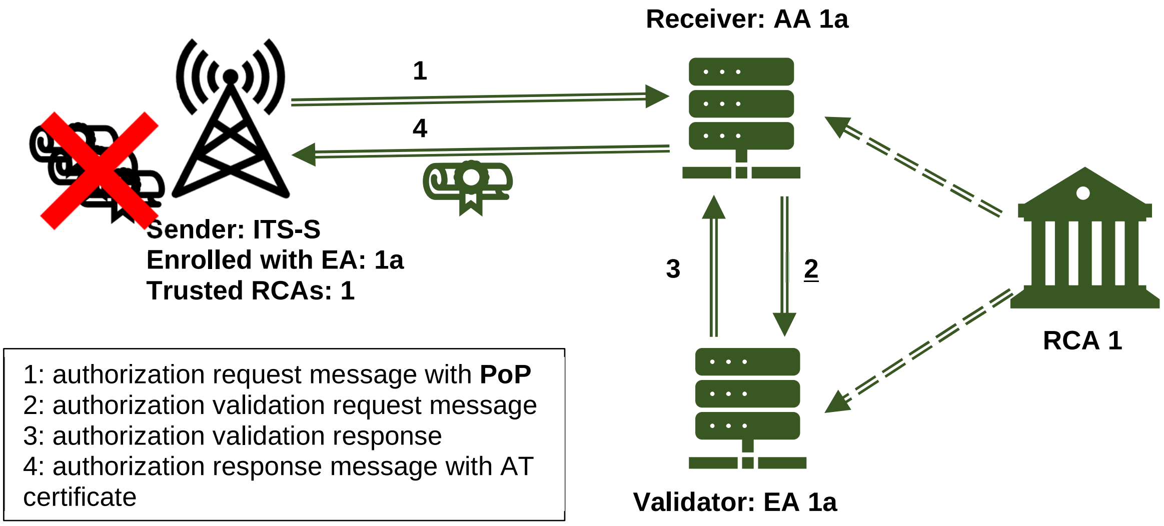
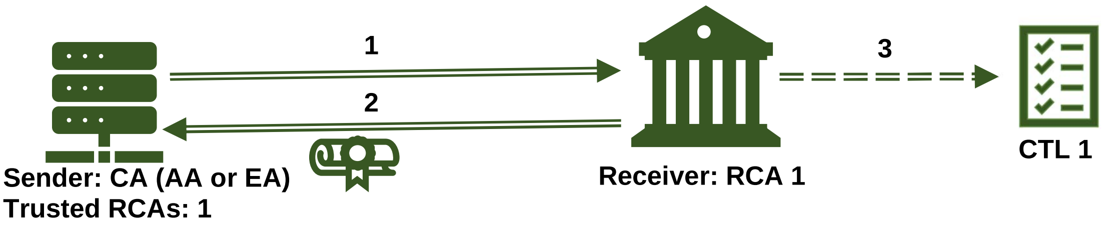

Receiver: AA 1a
1
4
Sender: ITS-S
Enrolled with EA: 1a
Trusted RCAs: 1
3
2
RCA 1
Validator: EA 1a
1: authorization request message with **PoP**
2: authorization validation request message
3: authorization validation response
4: authorization response message with AT certificate

Figure 17: Renewal of expired AT certificates

6.3.3 CA certificate request and distribution

6.3.3.1 Use-case 5-1 - Initial CA certificate request

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC5-1		
Objective	Initial CA certificate request.		
Description	CA generates the valid CaCertificateRequestMessage and provides it to RCA. RCA generates a new CA certificate, provides it to the CA, updates and publishes the CTL accordingly. See note.		
Configuration	The **CFG_PKI_CAs** configuration shall be used with additional requirements: • The RCA has a valid self-signed certificate.		
Pre-test conditions			
REQ / PICS	**Requirements**	**PICS**	
		PICS_PKI_CA_MANAGEMENT	
Step	**Type**	**Description**	**Result**
1	Stimulus	The CA (EA or AA) is triggered to request its certificate from the RCA.	
2	Action	The CA (EA or AA) sends the *CaCertificateRequestMessage to the RCA.*	
3	Verify	The RCA verifies CA certificate request.	The CA certificate request is valid.
4	Action	• The RCA generates certificate to the CA (EA or AA). • The RCA update CTL with the certificate of the CA (EA or AA).	
5	Verify	The CA (EA or AA) receives its certificate.	• The certificate is valid. • The CTL is updated an available.
NOTE: This test can be run as part of the sequential test scenarios PKI_SC3-1 (see Table 3).			

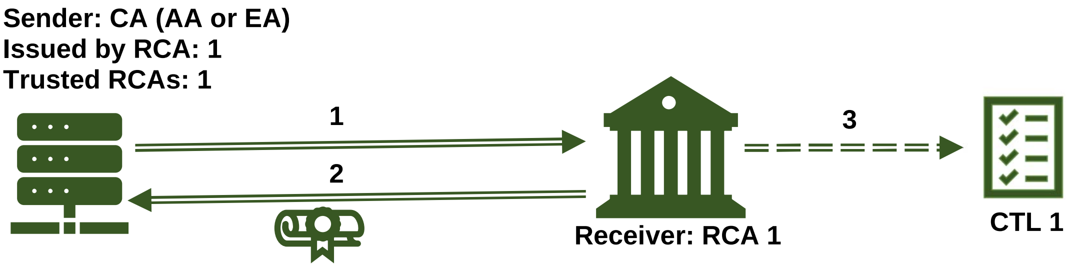


1: CAs (EA, AA) prepares CaCertificateRequestMessage and transmit it to RCA
2: RCA generates CAs certificates
3: RCA updates CTL with new certificates

Figure 18: Initial CA certificate request

6.3.3.2 Use-case 5-2 - Re-keying of CA certificate

Interoperability Test Description			
Identifier	TD_ITS_SEC_UC5-2		
Objective	Re-keying of CA certificate.		
Description	CA generates the valid CaCertificateRekeyingMessage and provides it to RCA. RCA generates a new CA certificate, provides it to the CA, updates and publishes the CTL accordingly. See note.		
Configuration	The **CFG_PKI_CAs** configuration shall be used with additional requirements: • The RCA has a valid self-signed certificate.		
Pre-test conditions			
REQ / PICS	**Requirements**	**PICS**	
		PICS_PKI_CA_MANAGEMENT	
Step	**Type**	**Description**	**Result**
1	Stimulus	The CA (EA or AA) is triggered to update its certificate with new public key.	
2	Action	The CA (EA or AA) sends the *CaCertificateRekeyingMessage to the RCA.*	
3	Verify	The RCA verifies CA Rekeying request.	The CA Rekeying request is valid.
4	Action	• The RCA generates certificate to the CA (EA or AA). • The RCA update CTL with the new certificate of the CA (EA or AA).	
5	Verify	The CA (EA or AA) receives its certificate with the new key.	• The certificate is valid. • The CTL is updated an available.
NOTE: This test can be run as part of the sequential test scenarios PKI_SC3-1 (see Table 3).			



1: CAs (EA, AA) prepares CaCertificateRequestMessage and transmit it to RCA
2: RCA generates CAs certificates
3: RCA updates CTL with new certificates

Figure 19: Re-keying of CA certificate

6.4 Comprehensive scenarios

Comprehensive scenarios may include a group of ITS-S and their PKI, a group of ITS-S and different PKIs or only PKI certification authorities. When an ITS-S is involved, the test scenario shall start by the enrolment, then the authorization and finish with broadcasting a message (CAM, DENM) to the neighbouring using the issued ATs.

ITS-S shall request CTLs and CRLs if necessary and missing AA certificates. New CRL containing one AA can be issued during the test.

The following tables provide the sequence of some of the aforementioned use cases describing comprehensive scenarios.

Table 1: ITS-S secured communication scenarios for CFG_SEC configuration

Scenario	Description	UCs sequence
PKI_SC1-1	Communication using valid AT from the same PKI (can be executed multiple times with certificates from different PKI) Communication using valid AT from different AA from the same PKI Communication using valid AT from AA from two different PKIs	UC1-1 UC1-2 UC1-4
PKI_SC1-2	Peer-2-Peer distribution of AA certificate from the same PKI	UC1-3
PKI_SC1-3	Pseudonym changing	UC1-5
PKI_SC1-4	Exceptional scenarios: Invalid AT certificate region Invalid AT validity period Missing of application PSID in AT	UC2-1 UC2-2 UC2-3a UC2-3b
PKI_SC1-5	Using of AT issued by revoked AA Using of AT issued by AA signed by untrusted RCA	UC2-4 UC2-5

Table 2: PKI communication scenarios for CFG_PKI_ENROLMENT and CFG_PKI_AUTHORIZATION configurations

Scenario	Description	UCs sequence
PKI_SC2-1	Enrolment procedure Re-enrolment with the same EA Authorization with the same PKI Authorization with the same PKI with optional privacy Renewal of AT certificates after expiration of validity period Authorization with the same PKI when AA is revoked	UC3-1 UC3-2 UC4-1 UC4-2 UC4-5 UC4-4
PKI_SC2-2	Enrolment procedure Authorization with AA from another PKI Authorization with AA from another PKI when AA is revoked	UC3-1 UC4-3 UC4-4
PKI_SC2-3	Enrolment when ITS-S is not registered in the EA	UC3-3
PKI_SC2-4	Enrolment when EA is in CRL	UC3-4

Table 3: PKI CA management scenarios for CFG_CAs configuration

Scenario	Description	UCs sequence
PKI_SC3-1	Initial CAs certificate request Re-keying of CAs certificate	UC5-1 UC5-2

Annex A (informative): Bibliography

- ETSI EG 202 798 (V1.1.1): "Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing".

History

Document history		
V1.1.1	May 2019	Publication
V1.2.1	February 2022	Publication