ETSITS 103 096-2 V1.1.1 (2013-07)



Intelligent Transport Systems (ITS); Testing;

Conformance test specification for TS 102 867 and TS 102 941; Part 2: Test Suite Structure and Test Purposes (TSS&TP)

Reference DTS/ITS-0050019 Keywords ITS, testing, TSS&TP

ETSI

650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C Association à but non lucratif enregistrée à la Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from: http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services: http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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

© European Telecommunications Standards Institute 2013. All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP**TM and **LTE**TM are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intelle	tual Property Rights	5
Forew	rd	5
1	cope	e
2	References	<i>6</i>
2.1	Normative references	
2.2	Informative references.	
2		
3	Definitions and abbreviations	
3.1	Definitions	
3.2	Abbreviations	
4	Prerequisites and Test Configurations	7
4.1	Test Configurations	7
4.2	PKI Hierarchy	9
4.3	Feature Restriction and Pre-Enrolment	
4.3.1	Feature Restriction	
4.3.2	Pre-Enrolment	
4.4	States in Initial Conditions	
4.4.1	ITS-S send side states	
4.4.2	ITS-S receive side states	
4.4.3	EA states	
4.4.4	AA states	
4.5	Validity of Signed Communication	
4.6 4.7	Introduction of Snippets of Data Structures	
4.7	Variants, Variables and Snippet Naming Convention	13
5	Test Suite Structure (TSS)	13
5.1	Structure for Security tests	13
5.2	Test groups	
5.2.1	Root	
5.2.2	Groups	
5.2.3	Sub groups	
5.2.4	Categories	14
6	Test Purposes (TP)	14
6.1	Introduction	14
6.1.1	TP definition conventions	14
6.1.2	TP Identifier naming conventions.	
6.1.3	Rules for the behaviour description	
6.1.4	Sources of TP definitions	
6.1.5	Mnemonics for PICS reference	
6.1.6	Message encapsulation	
6.1.7	Used constants	
6.1.8	Snippets definitions	
6.1.8.1 6.1.8.2	Regions	
6.1.8.2	Certificates	
6.1.8.2		
6.1.8.3	Messages	
6.1.8.3		
6.1.8.3		
6.1.8.3	, .	
6.2	Test purposes for SECURITY	
6.2.1	ITS Station	
6.2.1.1	Enrolment	
6.2.1.1		
6.2.1.1		

6.2.1.2	Authorization	47
6.2.1.2.1	Normal Behavior	47
6.2.1.2.2	Exceptional Behavior	54
6.2.1.3	Sending Data	66
6.2.1.4	Receiving Data	73
6.2.1.4.1	Normal Behavior	73
6.2.1.4.2	Exceptional behavior	77
6.2.2	Certificate Authority	91
6.2.2.1	Normal Behavior	91
6.2.2.1.1	Generic message verification	91
6.2.2.1.2	Key Compression	94
6.2.2.1.3	Permissions	95
6.2.2.1.4	Expiration	97
6.2.2.1.5	Regions	
6.2.2.2	Exceptional Behavior	
6.2.2.2.1	Invalid Message Fields	
6.2.2.2.2	Invalid Certificate or Certificate Chain	103
6.2.2.2.3	Invalid Certificate Fields	
6.2.2.2.4	Invalid Permissions	110
6.2.2.2.5	Invalid Regions	113
6.2.2.2.6	Expiration	
6.2.3	Enrolment Authority	
6.2.3.1	Normal Behavior	116
6.2.3.2	Exceptional Behavior	
6.2.4	Authorization Authority	
6.2.4.1	Normal Behavior	118
6.2.4.1.1	Scopes (Scope Kind and Scope Name)	118
6.2.4.1.2	Expiration	
6.2.4.2	Exceptional Behavior	
6.2.4.2.1	Invalid Certificates or Certificate Chain Fields	
6.2.4.2.2	Invalid Scopes (Subject Type and Scope Name)	
History	1 \ 3 31 1 /	
1 113tO1 y		123

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

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

The present document is part 2 of a multi-part deliverable covering Conformance test specification for ITS Security as identified below:

TS 103 096-1: "Protocol Implementation Conformance Statement (PICS)";

TS 103 096-2: "Test Suite Structure and Test Purposes (TSS&TP)";

TS 103 096-3: "Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)";

TR 103 096-4: "Validation report".

1 Scope

The present document provides the Test Suite Structure and Test Purposes (TSS&TP) for Security as defined in IEEE P 1609.2 [1], TS 102 941 [2] and TS 102 867 [3] in compliance with the relevant requirements and in accordance with the relevant guidance given in ISO/IEC 9646-7 [9].

The ISO standard for the methodology of conformance testing (ISO/IEC 9646-1 [6] and ISO/IEC 9646-2 [7]) as well as the ETSI rules for conformance testing (ETS 300 406 [10]) are used as a basis for the test methodology.

2 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 reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://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.

2.1 Normative references

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

_	
[1]	IEEE P1609.2/D12 (January 2012): "IEEE Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages.
[2]	ETSI TS 102 941: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".
[3]	ETSI TS 102 867: "Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2".
[4]	ETSI TS 103 096-1 (V1.1.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specification for TS 102 867 and TS 102 941; Part 1: Protocol Implementation Conformance Statement (PICS)".
[5]	ETSI TS 103 096-3 (V1.1.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specification for TS 102 867 and TS 102 941; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".
[6]	ISO/IEC 9646-1 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 1: General concepts".
[7]	ISO/IEC 9646-2 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 2: Abstract Test Suite specification".
[8]	ISO/IEC 9646-6 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 6: Protocol profile test specification".
[9]	ISO/IEC 9646-7 (1995): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 7: Implementation Conformance Statements".
[10]	ETSI ETS 300 406 (1995): "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

2.2 Informative references

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

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

- terms given in IEEE 1609.2 [1], TS 102 941 [2] and in TS 102 867 [3];
- terms given in ISO/IEC 9646-6 [8] and in ISO/IEC 9646-7 [9].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AA Authorization Authority
BV Normal behaviour
CA Certification Authority
CAM Cooperative Awareness I

CAM Cooperative Awareness Message
CRL Certificate Revocation List
CSR Certificate Signing Request

DENM Decentralized Environmental Notification Message

EA Enrolment Authority
EB Exceptional Behavior
ITS Intelligent Transport System

ITS-AID ITS Application ID

ITS-S ITS Station

IUT Implementation Under Test

MSEC Multicast Security
PKI Public Key Infrastructure
PSID Provider Service Identifier
SA Security Association
SSP Service Specific Permissions
TLS Transport Layer Security

TP Test Purposes
TSS Test Suite Structure

4 Prerequisites and Test Configurations

4.1 Test Configurations

The test configuration 1 as shown in figure 1 is applied for the test group of CA and EA tests.

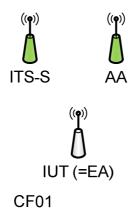


Figure 1: Test Configuration 1

The test configuration 2 as shown in figure 2 is applied for the test group of CA and AA tests.

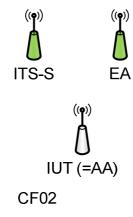


Figure 2: Test Configuration 2

The test configuration 3 as shown in figure 3 is applied for the test group of ITS-S Enrolment and Authorization tests.

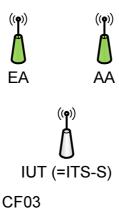


Figure 3: Test Configuration 3

The test configuration 4 as shown in figure 4 is applied for the test group of ITS-S Send and Receive Data tests.

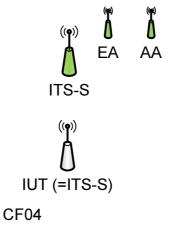


Figure 4: Test Configuration 4

4.2 PKI Hierarchy

The PKI Hierarchy is depicted below. Four different types of certificates are defined. They are listed hereafter.

- CERT_ROOT
- CERT_EA_x
- CERT_AA_x
- CERT_ENR_x
- CERT_AUTH_x

These names are used in the TP definitions, where $\underline{\ }x$ is a placeholder for numbering different certificates.

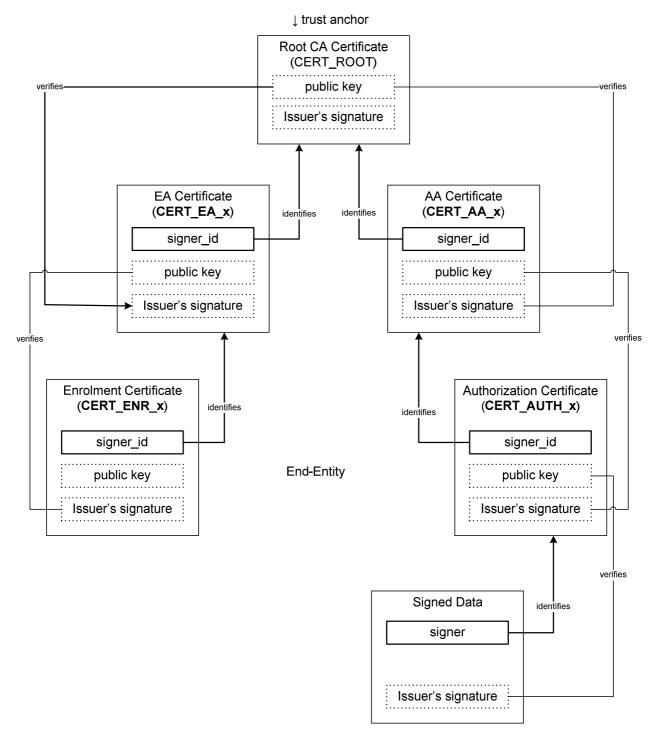


Figure 5: PKI Hierarchy

4.3 Feature Restriction and Pre-Enrolment

4.3.1 Feature Restriction

In this clause all feature restrictions are listed:

- Certificate chains where subordinate certificates make use of inherited permissions are not supported
- Only circular regions

- Only explicit certificates
- Revocation is not tested, i.e. certificate responses contain only empty revocation list
- Update Enrolment Credentials is not tested
- Remove Enrolment Credentials is not tested
- Update Authorization Tickets is not tested
- The name which identifies the CA shall be no longer that 32 bytes

4.3.2 Pre-Enrolment

Enrolment is the process by which an ITS-S obtains an enrolment certificate, which can later be used to authenticate requests for authorization certificates. An ITS-S undergoes initial enrolment by executing the Enrolment Request information flow from TS 102 941 [2].

When devices enrol with an Enrolment Authority, they should be authenticated as devices that are entitled to receive enrolment credentials of the type requested. There are two three different authentication approaches:

- Public key: Enrolment requests are authenticated by using a private key of the ITS-S. The corresponding public key is previously registered with a unique ITS-S module ID at the EA in a secure process. Every ITS-S has to be registered separately.
- Certificate: Enrolment requests are authenticated by a certificate or certificate chain.
- Self-signed: Enrolment requests are signed by the public key contained in the enrolment request. In this case the signature provides proof of possession of the corresponding private key, but does not authenticate that the private key holder is in fact authorized to receive an enrolment credential of the type requested. This authorization is provided by other mechanisms.

None of the three authentication approaches start at the device lifecycle: in all cases, there is the question of how the device is originally shown to be authenticated. The test system supports both the certificate and the self-signed forms of enrolment request.

For enrolment request:

- The test system enrolment authority shall accept the following forms of authorization, certificate and self-signed.
- The test system enrolment authority shall check that the signature on the enrolment request is cryptographically valid.
- In the case of an enrolment request signed by a certificate:
 - The test system enrolment authority shall check that the request is consistent with the permissions in the certificate.
 - The test system enrolment authority shall not carry out any other validation on the signing certificate. For example, it shall not check the signature on the signing certificate, check that the certificate chains back to a known CA, or check whether the signing certificate is revoked.

The test system enrolment authority shall issue the enrolment certificate if these validity tests pass.

From the perspective of the IUT, this has the following consequences:

- Certificate: The IUT shall be provisioned with a certificate to authenticate enrolment before testing begins (a pre-enrolment certificate).
 - The supplier shall provide instructions as to how to reset the IUT to a state where it has the preenrolment certificate but not the enrolment certificate, to allow the enrolment flow to be run multiple times.

- The supplier shall chose between two options:
 - The test system generates private key and public certificate for the device.
 - The supplier generates a private key and sends a certificate signing request to the test system.
- Self-signed: The IUT supplier shall provide instructions as to how to set the IUT into a state where it will request enrolment with a self-signed request.

4.4 States in Initial Conditions

Each TP contains an initial condition. The initial condition defines in which initial state the IUT has to be to apply the actual TP. In the corresponding Test Case, when the execution of the initial condition does not succeed, it leads to the assignment of an Inconclusive verdict. This clause defines the different initial states of the IUT.

4.4.1 ITS-S send side states

- Not enrolled state: ITS-S has all info necessary to send an EnrolmentRequest but does not have any Enrolment credentials yet
- Awaiting EnrolmentResponse state: ITS-S has sent an EnrolmentRequest and is waiting for an EnrolmentResponse
- Enrolled, but not authorized state: ITS-S has received EnrolmentResponse and is able to send AuthorizationRequest
- Awaiting AuthorizationResponse state: ITS-S has sent an AuthorizationRequest and is waiting for an AuthorizationResponse
- Authorized state: ITS-S has received a successful AuthorizationResponse

4.4.2 ITS-S receive side states

• Operational state: ITS-S has the root certificate and is ready to receive messages

4.4.3 EA states

• Operational state: EA has obtained its certificate and is ready to receive and send Enrolment messages

4.4.4 AA states

Operational state: AA has obtained its certificate and is ready to receive and send Authorization messages

4.5 Validity of Signed Communication

The check of the validity of signed communication according to clause 5.5 of IEEE P1609.2/D12 [1] (e.g. consistency check of the certificate chain, consistency check between certificate and message etc) forms an integral part of the test suite and is described in TS 103 096-3 [5], clause 6.

4.6 Introduction of Snippets of Data Structures

The data structures in IEEE P1609.2/D12 [1] can become quite complex. In order to allow to write a TP in a concise form, the usage of snippets has been introduced. A snippet is a partial extract of a data structure which is assigned with values. A snippet can be used within a TP. Please refer to clause 6.1.8 for a complete list of all defined snippets.

Within a TP, any element of the snippet can be overwritten or extended. In the example below the TP extends the snippet **MSG_ENRRSP_TS** 'signature.ecdsa_signature' to ' signature.ecdsa_signature.R.type = = uncompressed'.

```
when {
    the IUT receives a valid CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
    containing certificate_chain[last].signature.ecdsa_signature_R.type
    set to uncompressed
```

4.7 Variants, Variables and Snippet Naming Convention

The TPs use the concept of variants, variables and snippets. Their definition, how they are used and their naming conventions are defined in this clause.

Variants: In case where for a single field multiple values can be tested (e.g. different public key types), then a table is appended after the TP. This table lists all the different value which need to be tested. The TP identifier is appended with –X (e.g. **TP/SEC/ITS-S/ENR/NB-02-X**). If there are two fields for which multiple values can be tested then X and Y are appended. The field itself is written as X_FIELD_NAME (e.g. **X_PKT_SIGNATURE**).

Variables: Variables are used in TPs in order to highlight the fact that a particular part of request message needs to reappear in a response message. For example for a TP where the IUT has sent an EnrolementRequest with a permission list, and the test system needs to sent the same permission list back, then the denotation of **V_PERM_LIST** (see **TP/SEC/ITS-S/ENR/NB-11**)

Snippets: For the definition of snippets refer to the previous clause. The naming convention for snippets is defined to upper case and to have no specific prefix (e.g. **MSG_ENRREQ_IUT**). All snippets in TPs contain hyperlinks which allows to navigate from the TP directly to the snippet definition.

5 Test Suite Structure (TSS)

5.1 Structure for Security tests

Table 1 shows the Test Suite Structure (TSS) including its subgroups defined for conformance testing.

Root Group Group category SEC ENR/AUTH CA Normal behaviour Exceptional behaviour EΑ **ENR** Normal behaviour Exceptional behaviour AA **AUTH** Normal behaviour Exceptional behaviour ITS-S **ENR** Normal behaviour Exceptional behaviour AUTH Normal behaviour Exceptional behaviour S-DATA Normal behaviour Exceptional behaviour R-DATA Normal behaviour Exceptional behaviour

Table 1: TSS for SECURITY

The test suite is structured as a tree with the root defined as SEC. The tree is of rank 3 with the first rank a Group, the second rank a sub group, and the last rank a category.

5.2 Test groups

The test suite has a total of four levels. The first level is the root. The second level defines different IUTs. The third level defines various functional areas. The fourth level differentiates normal and exceptional behaviour.

5.2.1 Root

The root identifies ITS G5A as defined in IEEE 1609.2 [1], TS 102 941 [2] and TS 102 867 [3].

5.2.2 Groups

There are four functional areas identified as groups:

- Certificate Authority
- Enrolment Authority
- Authorization Authority
- ITS Station

5.2.3 Sub groups

There are four functional areas identified as sub-groups:

- Enrolment
- Authorization
- Send Data
- Receive Data

5.2.4 Categories

Test categories are limited to the normal and exceptional behaviour.

6 Test Purposes (TP)

6.1 Introduction

6.1.1 TP definition conventions

The TP definition is constructed according to EG 202 798 [i.1].

6.1.2 TP Identifier naming conventions

The identifier of the TP is constructed according to table 2.

Table 2: TP naming convention

Identifier: TP_ <root>_<gr>_<sgr>_<x>_<n< th=""><th>n></th><th></th></n<></x></sgr></gr></root>	n>	
<root> = root</root>	SEC	
<gr> = group</gr>	CA	Certificate Authorithy
	EA	Enrolment Authorithy
	AA	Authorization Authority
	ITS-S	ITS Station
<sgr> =sub-group</sgr>	ENR	Enrolment
	AUTH	Authorization
	S-DATA	Send Data
	R-DATA	Receive Data
<x> = type of testing</x>	NB	Normal Behaviour
	EB	Exceptional Behaviour
<nn> = sequential number</nn>		01 to 99
<x> = Variant for 1st permutation table</x>		A to Z
<y> = Variant for 2nd permutation tab</y>	le	A to Z

6.1.3 Rules for the behaviour description

The description of the TP is constructed according to EG 202 798 [i.1].

In the TP the following wordings are used:

- "The IUT is requested to send": An upper layer requests the security layer to apply processing to a packet.
- "The IUT receives": for packets coming from the network and given by the lower layer.
- "The IUT is configured to": the Security Layer on the IUT is requested to include a certain data element, e.g. this can be manually configured or triggered by use of a application that requires this data element.
- "The IUT accepts": the Security Layer on the IUT interprets a received message as passing all the relevant validity tests, including cryptographic validity, and passes it to a higher layer for interpretation.
- "The IUT discards": the Security Layer on the IUT interprets a received message as failing at least one validity test and does not pass it to a higher layer (drops a received message).

6.1.4 Sources of TP definitions

All TPs specified in the present document are derived from the behaviour defined in IEEE 1609.2 [1], TS 102 941 [2] and TS 102 867 [3].

6.1.5 Mnemonics for PICS reference

The following table lists mnemonic names and maps them to the PICS item number.

Table 3: Mnemonics for PICS reference

Mnemonic	PICS item
PIC_Generate_SignPayload	[4] Table A.5/1
PIC_Generate_SignExternalPayload	[4] Table A.5/2
PIC_Generate_SignPartialPayload	[4] Table A.5/3
PIC_Generate_Identified	[4] Table A.5/7
PIC Generate GenerationTime	[4] Table A.5/9
PIC_Generate_GenerationLocation	[4] Table A.5/10
PIC_Generate_ExpirationTime	[4] Table A.5/11
PIC_Generate_Certificate	[4] Table A.5/13
PIC_Generate_Ecdsa224	[4] Table A.5/15
PIC_Generate_Ecdsa256	[4] Table A.5/16
PIC_Generate_ExplicitCertificates	[4] Table A.5/17
PIC_Generate_Uncompressed	[4] Table A.5/19
PIC_Generate_Compressed	[4] Table A.5/20
PIC_Generate_CompressedFastVerification	[4] Table A.5/21
PIC_Generate_UncompressedKey	PIC_Generate_Uncompressed
PIC_Generate_CompressedKey	PIC_Generate_Compressed AND
·	PIC_Generate_CompressedFastVerification
PIC_Generate_XCoordinateOnlyKey	PIC_Generate_Compressed AND NOT
	PIC_Generate_CompressedFastVerification
PIC_Generate_SelfSigned	[4] Table A.34/2
PIC_Generate_StartValidity	[4] Table A.34/16
PIC_Generate_LifetimeIsDuration	[4] Table A.34/17
PIC_ Generate_StartValidityIsATimestamp	NOT PIC_Generate_LifetimeIsDuration
PIC_Generate_VerificationKey224	[4] Table A.34/19
PIC_Generate_VerificationKey256	[4] Table A.34/20
PIC_Generate_EncryptionKey	[4] Table A.34/21
PIC_Generate_PsidArrayWithMoreThan8Entries	[4] Table A.37/2
PIC_Verify_Uncompressed	[4] Table A.14/17
PIC_Verify_Compressed	[4] Table A.14/18
PIC_Verify_CompressedFastVerification	[4] Table A.14/19
PIC_Verify_UncompressedKey	PIC_Verify_Uncompressed
PIC_Verify_CompressedKey	PIC_Verify_Compressed AND
	PIC_Verify_CompressedFastVerification
PIC_Verify_XCoordinateOnlyKey	PIC_Verify_Compressed AND NOT
	PIC_Verify_CompressedFastVerification
PIC_Verify_SelfSigned	[4] Table A.35/1
PIC_Verify_StartValidity	[4] Table A.41/9
PIC_Verify_LifetimeIsDuration	[4] Table A.41/10
PIC_Verify_StartValidityIsATimestamp	NOT PIC_Verify_LifetimeIsDuration
PIC_Verify_VerificationKey224	[4] Table A.41/11
PIC_Verify_VerificationKey256	[4] Table A.41/12
PIC_Verify_EncryptionKey	[4] Table A.41/13
PIC_Verify_PsidArrayWithMoreThan8Entries	[4] Table A.45/2

6.1.6 Message encapsulation

```
CertificateRequest message encapsulation
Structure 1609Dot2Data {
   containing type
      indicating encrypted
   containing encrypted_data
      containing symm_algorithm set to unknown
      containing recipients
          containing cert_id
          containing enc_key
      containing ciphertext
         ---- After deciphering process -----
          containing type
             set to certificate_request
          containing request
             containing the CerticateRequest data /
NOTE:
          When a TP refers to a CertificateRequest, then it is assumed that the CertificateRequest is received in a
          1609Dot2Data as described above.
```

```
CertificateResponse message encapsulation
Structure 1609Dot2Data {
   containing type
      indicating encrypted
   containing encrypted data
      containing symm_algorithm set to unknown
      containing recipients
         containing cert_id
          containing enc key
      containing ciphertext
                 ----- After deciphering process -----
          containing type
             set to certificate_response
          containing request
             containing the CerticateResponse data
          When a TP refers to a CertificateResponse, then it is assumed that the CertificateResponse is received in a
NOTE:
          1609Dot2Data as described above.
```

```
CertificateRequestError message encapsulation
Structure 1609Dot2Data {
   containing type
      indicating encrypted
   containing encrypted_data
      containing symm_algorithm set to unknown
      containing recipients
          containing cert_id
          containing enc key
      containing ciphertext
             ------ After deciphering process ------
          containing type
             set to certificate_request_error
          containing request
             containing the CertificateRequestError data
NOTE:
          When a TP refers to a CertificateRequestError, then it is assumed that the CertificateRequestError is
          received in a 1609Dot2Data as described above.
```

6.1.7 Used constants

NAME	Value	
CLT	Current Local Time	
ANY_VALUE_OR_NONE	*	
ANY_VALUE	?	
ANY_SCOPE	anonymous_scope or id_scope or sec_data_exch_ca_scope	
ETSI_LAT		
ETSI_LON		
NICE_LAT		
NICE_LON		
PARIS_LAT		
PARIS_LON		
PSID_A		
PSID_B		
PSID_C		
PSID_D	These PSIDs shall be defined before test execution	
PSID_E	These FSIDs shall be defined before test execution	
PSID_F		
PSID_G		
PSID_H		
PSID_I		
PSID_J	These PSIDs shall be defined only when IUT supports more than 8	
PSID_K	PSID	
PSID_L		

6.1.8 Snippets definitions

6.1.8.1 Regions

Table 4: Regions definitions

```
REGION LARGE :=
GeographicRegion {
    containing region_type set to 'circle'
    containing circular region
        containing center
            containing latitude set to ETSI LAT
            containing longitude set to ETSI LON
        containing radius set to 65KM
REGION MEDIUM :=
GeographicRegion {
    containing region_type set to 'circle'
    containing circular region
        containing center
            containing latitude set to ETSI LAT
            containing longitude set to ETSI_LON
        containing radius set to 32KM
}
REGION SMALL :=
GeographicRegion {
    containing region type set to 'circle'
    containing circular_region
        containing center
            containing latitude set to ETSI LAT
            containing longitude set to ETSI LON
        containing radius set to 1KM
}
REGION OUTSIDE :=
GeographicRegion {
    containing region_type set to 'circle'
    containing circular_region
        containing center
            containing latitude set to PARIS_LAT
            containing longitude set to PARIS LON
        containing radius set to 65KM
REGION INTERSECTING :=
GeographicRegion {
    containing region_type set to 'circle'
    containing circular_region
        containing center
            containing latitude set to NICE_LAT containing longitude set to NICE_LON
        containing radius set to 65KM
```

6.1.8.2 Certificates

6.1.8.2.1 Authorities certificates

Table 5: Root certificate definition

```
CERT_ROOT :=
Certificate {
    containing version_and_type
        set to 'explicit_certificates'(2)
    containing unsigned_certificate
        containing subject_type
        set to 'root_ca'
        containing cf
        set to 'use_start_validity' and 'lifetime_is_duration'
```

```
not containing signer id
    containing scope
        containing name
            set to 'ETSI Root CA'
        containing permitted_subject_types
            set to array[1] \overline{\{}
                'sec_data_exch_ca'
        containing permissions
            containing type
               set to 'specified'
            containing permissions_list
                set to array[0]
        containing region
            containing region_type set to 'none'
    containing expiration
        set to '2020-12-31'
    containing lifetime
       set to '10Y'
    containing crl_series
       set to 0
    containing verification key
        containing algorithm
            set to 'ecdsa_nistp256_with_sha256'
        containing public_key
            containing type
                set to 'uncompresed'
            containing x/y
                set to a valid key for ECDSA-256
    not containing encryption key
containing signature
    containing ecdsa signature
        verifiable with unsigned_certificate.verification_key
        containing R
            containing type
                set to 'x_coordinate_only'
            containing x
```

Table 6: Enrolment authority certificate definition

```
CERT_EA :=
Certificate {
    containing version_and_type
        set to 'explicit_certificates'(2)
    containing unsigned certificate
        containing subject type
           set to 'sec_data_exch_ca'
        containing cf
           set to 'use_start_validity' and 'lifetime_is_duration'
        containing signer id
           set to the 8-byte hash of CERT ROOT
        containing signature_alg
            set to 'ecdsa_nistp256_with_sha256'
        containing scope
            containing name
set to 'ETSI EA'
            containing permitted_subject_types
                set to array[1] {
                     'sec_data_exch_ca'
            containing permissions
                containing type
                    set to 'specified'
                containing permissions list
                    set to array[0]
            containing region
                set to REGION_LARGE
        containing expiration
           set to '2020-12-31'
        containing lifetime
            set to '10Y'
        containing crl_series
            set to 0
        containing verification_key
```

```
containing algorithm
            set to 'ecdsa_nistp256_with_sha256'
        containing public_key
            containing type
                set to 'uncompresed'
            containing x/y
                set to a valid key for ECDSA-256
    containing encryption key
        containing algorithm
           set to 'ecies nistp256'
        containing supported_symm_alg
           set to 'aes_128_ccm'
        containing public_key
            containing type
                set to 'uncompresed'
            containing x/y
                set to a valid key for ECIES-256
containing signature
    containing ecdsa signature
        verifiable with CERT ROOT. verification key
        containing R
            containing type
                set to 'x_coordinate_only'
            containing x
```

Table 7: Authorization authority certificate definition

```
CERT AA :=
Certificate {
    containing version_and_type
    set to 'explicit_certificates'(2)
    containing unsigned_certificate
        containing subject type
           set to 'sec_data_exch_ca'
        containing cf
            set to 'use_start_validity' and 'lifetime_is_duration'
        containing signer_id
            set to the 8-byte hash of CERT ROOT
        containing signature_alg
            set to 'ecdsa_nistp256_with_sha256'
        containing scope
            containing name
                set to 'ETSI AA'
            containing permitted_subject_types
                set to array[1] {
                     'sec data exch ca'
            containing permissions
                containing type
                    set to 'specified'
                containing permissions_list
                    set to array[0]
            containing region
                set to REGION_LARGE
        containing expiration
            set to '2020-12-31'
        containing lifetime
            set to '10Y'
        containing crl_series
           set to 0
        containing verification_key
            containing algorithm
                set to 'ecdsa_nistp256_with_sha256'
            containing public_key
                containing type
                    set to 'uncompresed'
                containing x/y
                    set to a valid key for ECDSA-256
        containing encryption_key
            containing algorithm
                set to 'ecies_nistp256'
            containing supported_symm_alg
                set to 'aes 128 ccm'
            containing public_key
                containing type
```

```
set to 'uncompresed'
containing x/y
set to a valid key for ECIES-256
containing signature
containing ecdsa_signature
verifiable with CERT_ROOT.verification_key
containing R
containing type
set to 'x_coordinate_only'
containing x

}
```

6.1.8.2.2 End-Entities certificates

6.1.8.2.2.1 Certificates issued by test system

Table 8: Enrolment certificate issued by test system

```
CERT ENR TS
Certificate {
    containing version_and_type
        set to 'explicit_certificates'(2)
    containing unsigned_certificate
        containing subject type
           set to 'sec_data_exch_csr'
        containing cf
            indicating 'use_start_validity' and 'lifetime_is_duration'
        containing signer_id
            set to 8-byte hash of the CERT EA
        containing signature_alg
            set to 'ecdsa_nistp256_with_sha256'
        containing scope
            containing name
                set to 'EC SCOPE DEFAULT'
            containing permitted_subject_types
                set to MSG_ENRREQ_IUT.unsigned_csr
                        .type specific data.sec data exch ca scope.permitted subject types
            containing permissions
                set to MSG_ENRREQ_IUT.unsigned csr
                         . \verb|type_specific_data.sec_data_exch_ca_scope.permissions|\\
            containing region
                set to MSG_ENRREQ_IUT.unsigned_csr.type_specific_data.sec_data_exch_ca_scope.region
        containing expiration
        containing lifetime
        containing crl_series
           set to 0
        containing verification key
            set to {\tt MSG\_ENRREQ\_IUT}. {\tt unsigned\_csr.verification\_key}
    containing signature
        containing ecdsa signature
            verifiable with CERT EA. verification key
            containing R
                containing type
                    set to 'compressed_y_0' or 'compressed_y_1'
                containing x/y
                    set to a valid key for ECDSA-256
         This certificate is a response to the EnrolmentRequest message MSG_ENRREQ_IUT.
NOTE:
```

Table 9: Authorization certificate issued by test system

```
CERT_AUTH_TS :=
Certificate {
    containing version_and_type
        set to 'explicit_certificates'(2)
    containing unsigned_certificate
        containing subject_type
        set to 'sec_data_exch_csr'
        containing cf
        indicating 'use_start_validity' and 'lifetime_is_duration'
        containing signer_id
        set to 8-byte hash of the CERT_AA
```

```
containing signature alg
            set to 'ecdsa_nistp256_with_sha256'
        containing scope
            containing name
                set to 'AC_SCOPE_DEFAUL'
            containing permitted subject types
                set to MSG_AUTHREQ_IUT.unsigned_csr
                         .type specific data.sec data exch ca scope.permitted subject types
            containing permissions
                set to MSG AUTHREQ IUT.unsigned csr
                        .type_specific_data.sec_data_exch_ca_scope.permissions
            containing region
                set to MSG AUTHREQ IUT.unsigned csr
                        .type specific data.sec data exch ca scope.region
        containing expiration
        containing lifetime
        containing crl_series
            set to 0
        containing verification key
            set to MSG AUTHREQ IUT.unsigned csr.verification key
    containing signature
        containing ecdsa_signature
            verifiable with CERT EA. verification key
            containing R
                containing type
                    set to 'compressed_y_0' or 'compressed_y_1'
                containing x/y
                    set to a valid key for ECDSA-256
         This certificate is a response to the AuthorizationRequest message MSG_AUTHREQ_IUT.
NOTE:
```

6.1.8.2.2.2

Table 10: Enrolment certificate issued by IUT

Certificates issued by implementation under test

```
CERT_ENR_IUT :=
Certificate {
    containing version_and_type
        set to explicit_certificates(2)
    containing unsigned certificate
        containing subject type
           set to MSG ENRREQ TS.unsigned csr.subject type
        containing cf
            set to MSG ENRREQ TS.unsigned csr.cf
        containing signer_id set to 8-byte hash of the CERT EA
        containing signature_alg
           set to 'ecdsa_nistp256_with_sha256'
        containing scope
            containing name
            containing permitted_subject_types
                set to MSG_ENRREQ_TS.unsigned_csr
                            .type specific data.sec data exch ca scope.permitted subject types
            containing permissions
                containing type set to 'specified'
                containing permissions_list
                    set to the intersection between
                        MSG ENRREQ_TS.unsigned_csr
                            .type_specific_data.sec_data_exch_ca_scope.permissions
                        and CERT_EA.scope.permissions.permissions_list
            containing region
                containing region type set to 'circle'
                containing circular region
                    set to the intersection between
                        MSG_ENRREQ_TS.unsigned_csr.type_specific_data.sec_data_exch_ca_scope.region
                        and CERT_EA.scope.region.circular_region
        containing expiration
            set to any timestamp > CLT
        containing lifetime if cf has use_start_validity and lifetime_is_duration flags set
            set to any value > expiration - CLT
        containing start_validity if cf indicating use_start_validity but not lifetime_is_duration
            set to any timestamp < CLT
        containing crl_series
        containing verification_key
            set to MSG_ENRREQ_TS.unsigned_csr.verification_key
```

```
containing signature
containing ecdsa_signature
verifiable with CERT_EA.verification_key

NOTE: This certificate is a response to the EnrolmentRequest message MSG_ENRREQ_TS.
```

Table 11: Authorization certificate issued by IUT

```
CERT AUTH IUT :=
Certificate {
    containing version_and_type
        set to 'explicit_certificates'(2)
    containing unsigned certificate
        containing subject_type
           set to MSG AUTHREQ TS.unsigned csr.subject type
        containing cf
            set to MSG_AUTHREQ_TS.unsigned_csr.cf
        containing signer id
           set to 8-byte hash of the CERT_AA
        containing signature_alg
            set to 'ecdsa_nistp256_with_sha256'
        containing type_specific_data
            containing anonymous scope if subject type set to 'sec data exch anonymous'
                containing permissions
                    containing type set to 'specified'
                    containing permissions_list
                        set to the intersection between MSG_AUTHREQ_TS.unsigned_csr
                                .type specific data.sec data exch ca scope.permissions
                        and CERT_AA.scope.permissions.permissions_list
                containing region
                    containing region type set to 'circle'
                    containing circular region
                        set to the intersection between MSG AUTHREQ TS.unsigned csr
                                .type_specific_data.sec_data_exch_ca_scope.region
                        and CERT_AA.scope.region.circular_region
            or containing id_scope if subject_type set to 'sec_data_exch_anonymous'
                containing name[0..32]
                containing permitted_subject_types
                    set to MSG_AUTHREQ_TS.unsigned_csr
                                .type specific data.sec data exch ca scope.permitted subject types
                containing permissions
                    containing type set to 'specified'
                    containing permissions_list
                        set to the intersection between MSG AUTHREQ TS.unsigned csr
                                .type_specific_data.sec_data_exch_ca_scope.permissions
                        and CERT_AA.scope.permissions.permissions_list
                containing region
                    containing region_type set to 'circle'
                    containing circular_region
                        set to the intersection between MSG_AUTHREQ_TS.unsigned_csr
                                .type_specific_data.sec_data_exch_ca_scope.region
                        and CERT_AA.scope.region.circular_region
        containing expiration
           set to any timestamp > CLT
        containing lifetime if cf has use_start_validity and lifetime_is_duration flags set
            set to any value > expiration - CLT
        containing start_validity if cf indicating use_start_validity but not lifetime_is_duration
            set to any timestamp < CLT
        containing crl series
        containing verification_key
            set to MSG_AUTHREQ_TS.unsigned_csr.verification_key
    containing signature
        containing ecdsa signature
            verifiable using CERT AA. verification key
NOTE:
         This certificate is a response to the AuthorizationRequest message MSG_AUTHREQ_TS.
```

6.1.8.3 Messages

6.1.8.3.1 ITS station testing

6.1.8.3.1.1 Enrolment

Table 12: EnrolmentRequest message received by the test system from the ITS-S

```
MSG ENRREQ IUT :=
CertificateRequest{
    containing signer
        containing type
            set to 'certificate' or
                     'certificate_chain' or
                     'self
        containing certificate if signer.type set to 'certificate' or
        containing certificates if signer.type set to 'certificate chain'
    containing unsigned csr
        containing version and type
            set to 'explicit_certificates'(2)
        containing request_time
            set to any timestamp <= CLT
        containing subject type
            set to 'sec_data_exch_csr'
        containing cf
            not indicating 'encryption_key' flag
        containing type specific data
            containing sec_data_exch_ca_scope containing name [0..32]
                 containing permitted_subject_types
                     set to array[1] := {
                         'sec data exch anonymous' or 'sec data exch identified localized'
                 containing permission
                     containing type
set to 'specified'
                     containing permissions_list
                 containing region
                    containing region_type
                        set to 'circle'
                    containing circular region
        containing expiration
            set to any timestamp > CLT
        containing lifetime if cf indicating 'use_start_validity' and 'lifetime_is_duration'
        containing start_validity if cf indicating 'use_start_validity'
and not indicating 'lifetime_is_duration'
            set to any timestamp < expiration
        containing verification_key
            containing algorithm set to 'ecdsa_nistp256_with_sha256'
            containing public key
        containing response_encryption_key
            containing algorithm set to 'ecies nistp256'
            containing supported symm alg set to 'aes 128 ccm'
            containing public key
    containing signature
        containing ecdsa_signature
             verifiable using {
                 signer.certificate.unsigned certificate.verification key
                         if signer.type is 'certificate'
                 or signer.certificates[last].unsigned_certificate.verification_key
                         if signer.type is 'certificate_chain'
                 or unsigned csr.verification key
                         if signer.type is 'self'
            }
```

Table 13: EnrolmentResponse message sent by the test system to the ITS-S

```
MSG_ENRRSP_TS :=
CertificateResponse {
    containing f
        set to 'NotRequested' (0)
    containing certificate_chain
        set to array[] = {
            CERT_ROOT,
            CERT_EA,
            CERT_ENR_TS
        }
    containing crl_path
        set to length 0
}
```

Table 14: EnrolmentRequestError message sent by the test system to the ITS-S

```
MSG_ENRERR_TS :=
CertificateRequestError {
    containing signer.type
        set to 'certificate'
    containing signer.certificate
        set to CERT_EA
    containing request_hash
        set to HASH (MSG_ENRREQ_IUT)
    containing reason
    containing signature
        containing ecdsa_signature
        verifiable using CERT_EA.unsigned_certificate.verification_key
}
```

6.1.8.3.1.2 Authorization

Table 15: AuthorizationRequest message received by the test system from the ITS-S

```
MSG AUTHREQ IUT :=
CertificateRequest{
    containing signer
        containing type
            set to 'certificate' or
                    'certificate_chain'
        containing certificate if signer.type set to 'certificate' or
        containing certificates if signer.type set to 'certificate chain'
    containing unsigned csr
        containing version_and_type
           set to 'explicit certificates'(2)
        containing request time
            set to any timestamp <= CLT
        containing subject_type
           set to 'sec data exch anonymous' or 'sec data exch identified localized'
        containing cf
           not indicating 'encryption_key' flag
        containing type_specific_data
            containing anonymous scope if subject type set to 'sec data exch anonymous'
                containing permissions
                    containing type
                       set to 'specified'
                    containing permissions_list
                containing region
                    containing region_type
                        set to 'circle'
                    containing circular_region
            or containing id_scope if subject_type set to 'sec_data_exch_identified_localized'
                containing name [0..32]
                containing permissions
                    containing type
                       set to 'specified'
                   containing permissions list
                containing region
                    containing region_type
                       set to 'circle'
                    containing circular_region
```

```
containing expiration
        set to any timestamp > CLT
    containing lifetime if cf indicating 'use_start_validity' and 'lifetime_is_duration'
    containing start_validity if cf indicating 'use_start_validity'
                            and not indicating 'lifetime_is_duration'
        set to any timestamp < expiration
    containing verification key
        containing algorithm set to 'ecdsa nistp256 with sha256'
        containing public_key
    containing response encryption key
       containing algorithm set to 'ecies nistp256'
        containing supported_symm_alg set to 'aes_128_ccm'
        containing public_key
containing signature
    containing ecdsa_signature
        verifiable using CERT_ENR_TS.unsigned_certificate.verification_key
```

Table 16: EnrolmentResponse message received by the test system from the EA

```
MSG_AUTHRSP_TS :=
CertificateResponse {
    containing f
        set to 'NotRequested' (0)
    containing certificate_chain
        set to array[] = {
            CERT_ROOT,
            CERT_AA,
            CERT_AUTH_TS
        }
    containing crl_path
        set to length 0
}
```

Table 17: EnrolmentRequestError message sent by the test system to the ITS-S

```
MSG_AUTHERR_TS :=
CertificateRequestError {
    containing signer.type
        set to 'certificate'
    containing signer.certificate
        set to CERT_AA
    containing request_hash
        set to HASH(MSG_AUTHREQ_IUT)
    containing reason
    containing signature
        containing signature
        containing ecdsa_signature
        verifiable using CERT_AA.unsigned_certificate.verification_key
}
```

6.1.8.3.1.3 Send and Recive Data

Table 18: 1609Dot2Data message to be sent by the test system to the ITS-S under test

```
MSG_SIGNED_TS :=
Structure 1609Dot2Data {
    containing protocol_version
        set to 2
    containing type
        set to 'signed'
    containing signed_data
        containing signer
    containing unsigned_data
        containing unsigned_data
        containing signed
        containing signed
        containing signed
        containing signed
        containing signed
        containing signature
}
```

Table 19: 1609Dot2Data message received by the test system from the ITS-S under test

```
MSG_SIGNED_IUT :=

Structure 1609Dot2Data {

   containing protocol_version
      set to 2

   containing type
      set to 'signed'
      or set to 'signed_partial_payload'
      or set to 'signed_external_payload'
      containing signed_data
      containing signer
      containing unsigned_data
            containing bysid
      containing signature
            verifiable using signer
}
```

6.1.8.3.2 Enrolment Authority testing

Table 20: EnrolmentRequest message sent by the test system to the EA

```
MSG ENRREQ TS :=
CertificateRequest {
    containing signer
        containing type
            set to 'certificate'
        containing certificate
            set to CERT ROOT
    containing unsigned csr
        containing version_and_type
            set to 'explicit_certificates'(2)
        containing request time
           set to CLT
        containing subject type
            set to 'sec data exch csr'
        containing cf
           indicating 'use start validity' and 'lifetime is duration'
        containing type_specific_data
            containing sec_data_exch_ca_scope
                containing name
                    set to 'EC SCOPE DEFAULT'
                containing permitted_subject_types
                    set to array[1]
                        containing 'sec_data_exch_identified_localized'
                containing permission
                    containing type
                        set to 'specified'
                    containing permissions_list
                        set to array[1]
                            containing PSID A
                containing region set to REGION SMALL
        containing expiration
           set to 31. Dec 2020
        containing lifetime
            set to 10Y
        containing verification key
            containing algorithm
               set to 'ecdsa nistp256 with sha256'
            containing public key
                containing type
                    set to 'x_coordinate_only'
                containing x
                    set to a valid key for ECDSA-256
        containing response_encryption_key
            containing algorithm
                set to 'ecies nistp256'
            containing supported symm alg
                set to 'aes_128_ccm'
            contains public key
                contains type
                    set to 'x_coordinate_only'
                containing x
                    set to a valid key for ECIES-256
```

```
containing signature
containing ecdsa_signature
verifiable by signer.certificate.unsigned_certificate.verification_key
}
```

Table 21: EnrolmentResponse message received by the test system from the EA

```
MSG_ENRRSP_IUT :=
CertificateResponse {
   containing f
   containing certificate_chain
      set to array[3]
      containing CERT_ROOT
      containing CERT_EA
      containing CERT_EA
      containing CERT_ENR_IUT
}
```

Table 22: EnrolmentRequestError message received by the test system from the EA

```
MSG_ENRERR_IUT :=
CertificateRequestError {
   containing signer.type
      set to 'certificate'
   containing signer.certificate
      set to CERT_EA
   containing request_hash
      set to HASH(MSG_ENRREQ_TS)
   containing reason
   containing signature
      containing signature
      containing ecdsa_signature
      verifiable using CERT_EA.unsigned_certificate.verification_key
}
```

6.1.8.3.3 Authorization Authority testing

Table 23: AuthorizationRequest message to be sent by the test system to the AA

```
MSG AUTHREQ TS :=
CertificateRequest{
    containing signer
        containing type
            set to 'certificate chain'
        containing certificates
            set to arrav[3]
                containing CERT_ROOT
                containing CERT_EA
                containing CERT ENR IUT
    containing unsigned_csr
        containing version_and_type
            set to 'explicit_certificates'(2)
        containing request_time
            set to CLT
        containing subject type
            set to 'sec data exch identified localized'
        containing cf
           indicating 'use start validity' and 'lifetime is duration'
        containing type_specific_data
            containing id_scope
                containing name
                    set to 'AC_SCOPE_DEFAULT'
                containing permissions
                    containing type
   set to 'specified'
                    containing permissions list
                        set to arrav[1]
                            containing PSID A
                 containing region
                    containing region_type
                        set to 'circle'
                    containing circular_region
                        set to REGION SMALL
```

```
containing expiration
       set to '31 Dec 2020'
    containing lifetime
       set to '10Y'
    containing verification_key
       containing algorithm
            set to 'ecdsa_nistp256_with_sha256'
        containing public key
            containing type
               set to 'x_coordinate_only'
            containing x
                set to a valid key for ECDSA-256
    containing response_encryption_key
       containing algorithm
           set to 'ecies_nistp256'
        containing supported_symm_alg
            set to 'aes_128_ccm'
        contains public_key
           contains type
                set to 'x_coordinate_only'
            containing x
               set to a valid key for ECIES-256
containing signature
    containing ecdsa signature
        verifiable by signer.certificate.unsigned_certificate.verification_key
```

Table 24: AuthorizationResponse message received by the test system from the AA

```
MSG_AUTHRSP_IUT :=
CertificateResponse {
    containing f
    containing certificate_chain
        set to array[3]
        containing CERT_ROOT
        containing CERT_AUTH_IUT
}
```

Table 25: AuthorizationRequestError message received by the test system from the AA

```
MSG_AUTHERR_IUT :=
CertificateRequestError {
    containing signer.type
        set to 'certificate'
    containing signer.certificate
        set to CERT_AA
    containing request_hash
        set to HASH(MSG_AUTHREQ_IUT)
    containing reason
    containing signature
        containing signature
        containing ecdsa_signature
        verifiable using CERT_AA.unsigned_certificate.verification_key
}
```

6.2 Test purposes for SECURITY

6.2.1 ITS Station

6.2.1.1 Enrolment

6.2.1.1.1 Normal Behaviour

6.2.1.1.1.1 Enrolment Request verification

TD Id	TDICEC/ITC C/END/ND 04			
IPIG	TP Id TP/SEC/ITS-S/ENR/NB-01			
Summary	ummary Check that ITS-S generates correctly a generic EnrolmentRequest message			
Reference	Reference IEEE P1609.2/D12 [1], 6.3.33			
	ETSI TS 102 941 [2] Table 1 : Contents of ITS-S EnrolmentRequest message			
Config Id	CF03			
PICS Selection				
	Initial conditions			
with {				
the IUT in 'NotEnr	olled' state			
}				
	Expected behaviour			
ensure that {				
when {				
the IUT is requ	the IUT is requested to send an EnrolmentRequest message			
, , , , , , , , , , , , , , , , , , , ,				
then {				
the IUT sends a valid CertificateRequest set to MSG_ENRREQ_IUT				
}	}			

	TP Id TP/SEC/ITS-S/ENR/NB-02-X			
	Summary Check that ITS-S generates enrolment request with signature of different types			
	Reference IEEE P1609.2/D12 [1], 6.2.17			
		ETSI TS 102 941 [2] Table 1 : Con	tents of ITS-S EnrolmentRequest message	
	Config Id	CF03		
F	PICS Selection			
		Initial condi	tions	
with {				
the	IUT in 'NotEnrolled'	state		
the	IUT is configured to	use signature of form X_PKT_SIGN	ATURE	
}				
		Expected beh	aviour	
ensure				
	en {			
	the IUT is requested	to send an EnrolmentRequest mess	sage	
}				
the		10 eg 15 - 1 11 1100 EN	1775 H.T.	
		CertificateRequest set to MSG_EN	IRREQ_IUT	
		ure.ecdsa_signature		
	containing R.t			
	set to X_F	PKT_SIGNATURE		
}	}			
}	}			
V		Variants		
X	DIC C	PIC	X_PKT_SIGNATURE	
Α		ate_XCoordinateOnlyKey	x_coordinate_only	
В		erate_CompressedKey	compressed_lsb_y_0/1	
С	PIC_Gene	rate_UncompressedKey	uncompressed	

```
TP Id
                      TP/SEC/ITS-S/ENR/NB-03
     Summary
                      Check that ITS-S generates enrolment request with signature calculated using compressed
                      representation of all public keys
     Reference
                      IEEE P1609.2/D12 [1], 6.2.17
                      ETSI TS 102 941 [2], Table 1: Contents of ITS-S EnrolmentRequest message
     Config Id
                      CF03
  PICS Selection
                      PIC_Generate_UncompressedKey
                                               Initial conditions
with {
   the IUT in 'NotEnrolled' state
   the IUT is configured to use uncompressed public keys for verification key
   the IUT is configured to use uncompressed public keys for response_encryption_key
                                              Expected behaviour
ensure that {
   when {
      the IUT is requested to send an EnrolmentRequest message
      the IUT sends a valid CertificateRequest set to MSG_ENRREQ_IUT
          containing unsigned_csr.verification_key.public_key.type (V_PKT_VK)
             set to 'uncompressed'
          containing unsigned_csr.response_encryption_key.public_key.type (V_PKT_REK)
             set to 'uncompressed'
          containing signature.ecdsa_signature
             calculated using compressed representation of V_PKT_VK and V_PKT_REK
   }
```

```
TP Id
                      TP/SEC/ITS-S/ENR/NB-04
     Summary
                      Check that ITS-S generates valid self-signed enrolment request.
                      IEEE P1609.2 [1], clause 6.2.17
     Reference
                      ETSI TS 102 941 [2], see table 1
     Config Id
                      CF03
  PICS Selection
                      PIC_Generate_SelfSigned
                                                Initial conditions
   the IUT in 'NotEnrolled' state
   the IUT is configured to use a self-signed enrolment request
                                               Expected behaviour
ensure that {
   when {
      the IUT is requested to send an EnrolmentRequest message
   then {
      the IUT sends a valid CertificateRequest set to MSG_ENRREQ_IUT
         containing signer.type
             set to 'self'
          containing signature
             verified using unsigned_csr.verification_key
   }
```

```
TP Id
                      TP/SEC/ITS-S/ENR/NB-05
     Summary
                      Check that ITS-S generates valid enrolment request with a different response encryption key
                      for every request.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.34
                      ETSI TS 102 941 [2], see table 1
     Config Id
                      CF03
  PICS Selection
                                                Initial conditions
with {
   the IUT in 'NotEnrolled' state
                                              Expected behaviour
ensure that {
   when {
      each time the IUT is requested to send an EnrolmentRequest message
   then {
      the IUT sends a valid CertificateRequest set to MSG_ENRREQ_IUT
         containing unsigned_csr.response_encryption_key
             set to value different from the previous ones
   }
```

```
TP Id
                      TP/SEC/ITS-S/ENR/NB-06
     Summary
                      Check that ITS-S generates valid enrolment request with a certificate containing more than 8
                      PSID entries
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.34
                      ETSI TS 102 941 [2], see table 1
     Config Id
                      CF03
  PICS Selection
                      PIC_Generate_PsidArrayWithMoreThan8Entries
                                               Initial conditions
with {
   the IUT in 'NotEnrolled' state
                                              Expected behaviour
ensure that {
   when {
      the IUT is requested to send an EnrolmentRequest message with more than 8 PSID entries
   then {
      the IUT sends a valid CertificateRequest set to MSG_ENRREQ_IUT
         containing unsigned_csr.type_specific_data.permission.permissions_list
             containing more than 8 entries
   }
```

6.2.1.1.1.2 Enrolment Response acceptance

TP ld	TP/SEC/ITS-S/ENR/NB-07		
Summary	Summary Check that ITS-S correctly decrypts enrolment response.		
Reference			
Config Id	CF03		
PICS Selection			
	Initial conditions		
with {			
the IUT awaiting E	nrolmentResponse		
}			
	Expected behaviour		
ensure that {			
when {			
the IUT receive	es a CertificateResponse (EnrolmentResponse)		
}			
then {			
the IUT decrypts the response			
}			
}	}		

```
TP/SEC/ITS-S/ENR/NB-08
       TP Id
                      Check that the ITS-S accepts a valid enrolment response having correct fields and values.
     Summary
                      IEEE P1609.2/D12 [1], clause 5.6.2.2
     Reference
                      ETSI TS 102 941 [2], see table 2
     Config Id
                      CF03
  PICS Selection
                                               Initial conditions
with {
   the IUT having sent an EnrolmentRequest set to MSG_ENRREQ_IUT
      containing unsigned_csr.type_specific_data.sec_data_exch_ca_scope
         containing permissions.permissions_list (V_PERM_LIST)
   the IUT awaiting EnrolmentResponse
                                             Expected behaviour
ensure that {
   when {
      the IUT receives a valid CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
          containing response.certificate_chain[last]
             containing unsigned_certificate.scope.permissions.permissions_list
                set to V_PERM_LIST
   then {
      the IUT accepts the CertificateResponse
   }
```

```
TP/SEC/ITS-S/ENR/NB-09
        TP Id
     Summary
                       Check that the ITS-S accepts a valid enrolment response even if the permissions in the issued
                       certificate are a subset of requested permissions
                       IEEE P1609.2/D12 [1], clause 5.6.2.2
     Reference
                       ETSI TS 102 941 [2], see table 2
      Config Id
                       CF03
  PICS Selection
                                                   Initial conditions
with {
   the IUT having sent an EnrolmentRequest set to MSG_ENRREQ_IUT
       containing unsigned_csr.type_specific_data.sec_data_exch_ca_scope containing permissions.permissions_list (V_PERM_LIST)
   the IUT awaiting EnrolmentResponse
                                                 Expected behaviour
ensure that {
   when {
       the IUT receives a valid CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
          containing response.certificate_chain[last].unsigned_certificate.scope.permissions.permissions_list
              set to a subset of V_PERM_LIST
   then {
       the IUT accepts the CertificateResponse
```

TP Id	TP/SEC/ITS-S/ENR/NB-10-X			
Summary	Summary Check that ITS-S accepts enrolment response with different public key types			
Reference	IEEE P1609.2/D12 [1], clause 6.2.17			
	ETSI TS 102 941 [2], see table 2			
Config Id	CF03			
PICS Selection				
	Initial conditions			
with {				
the IUT awaiting Er	nrolmentResponse			
}				
	Expected behaviour			
ensure that {				
when {				
the IUT receives	s a valid CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS			
containing c	ertificate_chain[last]			
containir	ng verification_key.public_key.type			
set to	X_PKT_VK			
containir	containing signature.ecdsa_signature.R.type			
set to X_PKT_SIGNATURE				
}				
then {				
the IUT accepts the CertificateResponse				
}				
}				

Variants				
X	X_PKT_SIGNATURE	X_PKT_VK	PIC Selection	
Α	compressed_lsb_y_0/1	compressed_lsb_y_0/1	PIC_Verify_CompressedKeyKey	
В	compressed_lsb_y_0/1	x_coordinate_only	PIC_Verify_CompressedKeyKey PIC_Verify_XCoordinateOnlyKey	
С	compressed_lsb_y_0/1	uncompressed	PIC_Verify_UncompressedKey	
D	x_coordinate_only	compressed_lsb_y_0/1	PIC_Verify_CompressedKeyKey PIC_Verify_XCoordinateOnlyKey	
Е	x_coordinate_only	x_coordinate_only	PIC_Verify_XCoordinateOnlyKey	
F	x_coordinate_only	uncompressed	PIC_Verify_UncompressedKey PIC_Verify_XCoordinateOnlyKey	
G	uncompressed	compressed_lsb_y_0/1	PIC_Verify_UncompressedKey PIC_Verify_CompressedKeyKey	
Н	uncompressed	x_coordinate_only	PIC_Verify_UncompressedKey PIC_Verify_XCoordinateOnlyKey	
I	uncompressed	uncompressed	PIC_Verify_UncompressedKey	

```
TP Id
                      TP/SEC/ITS-S/ENR/NB-11
     Summary
                      Check that the ITS-S accepts a valid enrolment response with signature calculated using
                      compressed representation of uncompressed public keys.
    Reference
                      IEEE P1609.2/D12 [1], clause 6.2.17
                      ETSI TS 102 941 [2], see table 2
     Config Id
                      CF03
  PICS Selection
                      PIC_Verify_UncompressedKey
                                               Initial conditions
with {
   the IUT awaiting EnrolmentResponse
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
         containing certificate_chain[last]
             containing unsigned_certificate.verification_key.public_key.type (V_PKT_VK)
                set to 'uncompressed'
             containing signature.ecdsa_signature
                calculated using compressed representation of V_PKT_VK
   then {
      the IUT accepts the CertificateResponse
```

```
TP Id
                      TP/SEC/ITS-S/ENR/NB-12
     Summary
                      Check that the ITS-S accepts a valid enrolment response with start_validity and lifetime.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.2
                      ETSI TS 102 941 [2], see table 2
     Config Id
                      CF03
  PICS Selection
                                                 Initial conditions
with {
   the IUT awaiting EnrolmentResponse
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
          containing certificate_chain[last].unsigned_certificate
             containing cf
                 indicating use_start_validity
                 indicating lifetime_is_duration
             containing lifetime
                 set to '10Y'
   then {
      the IUT accepts the CertificateResponse
   }
```

```
TP Id
                      TP/SEC/ITS-S/ENR/NB-13
     Summary
                      Check that the ITS-S accepts a valid enrolment response with start_validity value.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.2
                      ETSI TS 102 941 [2], see table 2
     Config Id
                      CF03
  PICS Selection
                      NOT PIC_Verify_LifetimeIsDuration
                                                 Initial conditions
   the IUT awaiting EnrolmentResponse
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a valid CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
          containing certificate_chain[last].unsigned_certificate
             containing cf
                 indicating 'use_start_validity'
                 and not indicating 'lifetime_is_duration'
             containing expiration
             containing start_validity
                 set to a timestamp < expiration
   then {
      the IUT accepts the CertificateResponse
   }
```

6.2.1.1.1.3 Enrolment Request Error acceptance

```
TP Id
                      TP/SEC/ITS-S/ENR/NB-14
     Summary
                      Check that ITS-S correctly decrypts enrolment request error.
     Reference
                      IEEE P1609.2/D12 [1], clause 5.6.2.1
     Config Id
                      CF03
  PICS Selection
                                                Initial conditions
with {
   the IUT awaiting EnrolmentResponse
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateRequestError (EnrolmentResponse)
   then {
      the IUT decrypts the response
```

```
TP/SEC/ITS-S/ENR/NB-15
       TP Id
     Summary
                      Check that the ITS-S accepts a valid enrolment request error having correct fields and values.
     Reference
                      IEEE P1609.2/D12 [1], clause 5.6.2.2
                      ETSI TS 102 941 [2], see table 3
                      CF03
     Config Id
  PICS Selection
                                               Initial conditions
with {
   the IUT having sent an EnrolmentRequest (V_REQUEST) set to MSG_ENRREQ_IUT
   the IUT awaiting EnrolmentResponse
                                             Expected behaviour
ensure that {
   when {
      the IUT receives a valid CertificateRequestError (EnrolmentResponse) set to MSG_ENRERR_TS
         containing request_hash
             set to the hash of the V_REQUEST
                calculated using compressed representation of all public keys
   then {
      the IUT accepts the CertificateRequestError
```

	TP ld	TP/SEC/ITS-S/ENR/NB-16-X		
S	Summary	Check that ITS-S accepts enro	elment request error with various types of signature public keys.	
R	eference	IEEE P1609.2/D12 [1], clause	6.2.17	
		ETSI TS 102 941 [2], see table	23	
	Config Id	CF03		
PIC	S Selection			
		Init	tial conditions	
with {				
the	IUT awaiting E	nrolmentResponse		
}				
		Ехре	ected behaviour	
ensure	that {			
wh	en {			
	the IUT receive	s a valid CertificateRequestErro	or (EnrolmentResponse) set to MSG_ENRERR_TS	
	containing s	ignature.ecdsa_signature.R.typ	e	
	set to X	_PKT_SIGNATURE		
}	}			
the	•			
	the IUT accepts	the CertificateRequestError		
}				
}				
			Variants	
X	X_F	PKT_SIGNATURE	PIC Selection	
Α	Χ_	_coordinate_only	PIC_Verify_XCoordinateOnlyKey	
В	com	pressed_lsb_y_0/1	PIC_Verify_CompressedKey	
С	·	uncompressed	PIC_Verify_UncompressedKey	

6.2.1.1.2 Exceptional Behavior

TD ! !	TRIOSCUTO O'SNR SER OA		
TP ld	TP/SEC/ITS-S/ENR/EB-01		
Summary	Check that ITS-S discards enrolment response if the subordinate certificate's validity region is		
	large than the issuing certificate's validity region.		
Reference	IEEE P1609.2/D12 [1], clause 5.5.3.3		
Config Id	CF03		
PICS Selection			
	Initial conditions		
with {			
the IUT awaiting E	nrolmentResponse		
	red to use EA certificate CERT_EA		
•	gned_certificate.scope.region		
	ON_SMALL		
1 301 to REGI	ON_OMALE		
J	Expected behaviour		
ensure that {	Expected behaviour		
•			
when {	0 (f. + D (F. + - 1D) + + M00 ENDOD TO		
	s a CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS		
	pertificate_chain[last] (CERT_ENR_TS)		
containi	containing unsigned_certificate.scope.region		
set to REGION_LARGE			
}			
then {			
the IUT discards the CertificateResponse			
·			
3			
, j			

```
TP Id
                      TP/SEC/ITS-S/ENR/EB-02
                      Check that ITS-S discards enrolment response if the subordinate certificate's validity region is
     Summary
                      outside of the issuing certificate's validity region.
                      IEEE P1609.2/D12 [1], clause 5.5.3.3
     Reference
     Config Id
                      CF03
  PICS Selection
                                                Initial conditions
with {
   the IUT awaiting EnrolmentResponse
   and the TS configured to use EA certificate CERT_EA
      containing unsigned_certificate.scope.region
          set to REGION_SMALL
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
         containing certificate_chain[last] (CERT_ENR_TS)
             containing unsigned_certificate.scope.region
                set to REGION_OUTSIDE
   then {
      the IUT discards the CertificateResponse
```

```
TP Id
                      TP/SEC/ITS-S/ENR/EB-03
     Summary
                      Check that ITS-S discards enrolment response if the subordinate certificate's validity period is
                      longer than issuing certificate's validity period.
     Reference
                      IEEE P1609.2/D12 [1], clause 5.5.3.3
     Config Id
                      CF03
  PICS Selection
                                                Initial conditions
with {
   the IUT awaiting EnrolmentResponse
   and the TS configured to use EA certificate CERT_EA
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
          containing certificate_chain[last] (CERT_ENR_TS)
             containing unsigned_certificate.expiration > CERT_EA.unsigned_certificate.expiration
   then {
      the IUT discards the CertificateResponse
   }
```

```
TP Id
                      TP/SEC/ITS-S/ENR/EB-04
     Summary
                      Check that ITS-S discards enrolment response if the subordinate certificate's permissions are
                      not included in issuing certificate.
     Reference
                      IEEE P1609.2/D12 [1], clause 5.5.3.3
     Config Id
                      CF03
  PICS Selection
                                                Initial conditions
with {
   the IUT has sent a valid EnrolmentRequest set to MSG_ENRREQ_IUT
      containing unsigned_csr.type_specific_data.sec_data_exch_ca_scope.permissions.permissions_list
          set to array [2]
             containing PSID A
             containing PSID_B
   and the IUT awaiting EnrolmentResponse
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
          containing certificate_chain[last-1] (CERT_EA)
             containing unsigned_certificate.scope.permissions.permissions_list
                 set to array[1]
                    containing PSID_A
          containing certificate_chain[last] (CERT_ENR_TS)
             containing unsigned_certificate.scope.permissions.permissions_list
                 set to array[1]
                    containing PSID_B
   then {
      the IUT discards the CertificateResponse
```

	TP ld	TP/SEC/ITS-S/ENR/EB-05-X
S	ummary	Check that ITS-S discards enrolment response if the message content type is different than
		'encrypted'.
	eference	IEEE P1609.2/D12 [1], clause 5.6.2.1
С	onfig Id	CF03
PICS	S Selection	
		Initial conditions
with {		
the	IUT awaiting Er	nrolmentResponse
}		
		Expected behaviour
ensure		
whe		4000D (0D)
1		s a 1609Dot2Data structure
	containing ty	ype
		INVALID_CONTENT_TYPE
,		encrypted_data.ciphertext ciphering process
/	containir	
		o 'certificate_response'
		ng response
		o MSG_ENRRSP_TS
/		
['] }		
ther	n {	
		s the received message
}		3
}		
		Variants
Χ		X_INVALID_CONTENT_TYPE
Α		unsecured (0),
В	signed(1)	
С		certificate_request(3)
D	certificate_response(4)	
Е	anonymous_certificate_response(5)	
F	certificate_request_error(6)	
G	crl_request(7)	
Н	crl(8)	
I		signed_partial_payload(9)
J		signed_external_payload(10)
K		signed_wsa(11)
L		certificate_response_acknowledgment (12)
М		ANY_VALUE(128)
		` ,

```
TP/SEC/ITS-S/ENR/EB-06-X
       TP Id
     Summary
                     Check that ITS-S discards enrolment response if the protocol_version is not 2.
    Reference
                     IEEE P1609.2/D12 [1], clause 6.2.1
     Config Id
                     CF03
  PICS Selection
                                              Initial conditions
with {
  the IUT awaiting EnrolmentResponse
                                             Expected behaviour
ensure that {
  when {
      the IUT receives a 1609Dot2Data structure
         containing protocol_version
            set to X_INVALID_VERSION_NUMBER
         containing type
            set to 'encrypted'
         containing encrypted_data.ciphertext
         ---- After deciphering process -----
             containing type
                set to 'certificate_response'
             containing response
                set to MSG_ENRRSP_TS
  then {
      the IUT discards the received message
  }
                                                  Variants
                                          X_INVALID_VERSION_NUMBER
 Α
                                                         0
 В
                                                          1
 С
                                                          3
 D
                                                        255
```

TP Id	TP/SEC/ITS-S/ENR/EB-07		
Summary	Check that ITS-S discards enrolment request error if the signer type is not valid.		
Reference	IEEE P1609.2/D12 [1], clause 6.2.4		
Config Id	CF03		
PICS Selection			
	Initial conditions		
with {			
the IUT awaiting Er	nrolmentResponse		
}			
Expected behaviour			
ensure that {	ensure that {		
when {			
the IUT receives	the IUT receives a 1609Dot2Data structure		
containing s	containing signed_data.signer.type		
set to 'self'			
}			
then {			
the IUT discards the received message			
}			
}			

```
TP Id
                     TP/SEC/ITS-S/ENR/EB-08-X
     Summary
                     Check that ITS-S discards enrolment respond if the certificate is not an explicit one.
     Reference
                     IEEE P1609.2/D12 [1], clause 6.3.1
     Config Id
                     CF03
  PICS Selection
                                              Initial conditions
with {
   the IUT awaiting EnrolmentResponse
                                             Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
         containing certificate_chain[last].version_and_type
             set to X_INVALID_CERT_VERSION_AND_TYPE
   then {
      the IUT discards the received message
  }
                                                   Variants
                                     X_INVALID_CERT_VERSION_AND_TYPE
 X
 Α
                                                         0
 В
                                                         1
 С
                                                         3
 D
                                                        255
```

```
TP Id
                      TP/SEC/ITS-S/ENR/EB-09
                      Check that ITS-S discards enrolment response if the hash was not calculated using
     Summary
                     compressed representation of public keys.
    Reference
                     IEEE P1609.2/D12 [1], clause 6.3.1
     Config Id
                      CF03
  PICS Selection
                     PIC_Verify_UncompressedKey
                                               Initial conditions
with {
   the IUT awaiting EnrolmentResponse
   and the TS configured to use EA certificate CERT_EA
      containing unsigned_certificate.verification_key.public_key.type (V_PKT_VK_EA)
         set to 'uncompressed'
      containing unsigned_certificate.encryption_key.public_key.type (V_PKT_EK_EA)
         set to 'uncompressed'
                                             Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
         containing certificate_chain[last]
             containing unsigned_certificate.signer_id
                calculated using uncompressed representation of V_PKT_VK_EA and V_PKT_EK_EA
   then {
      the IUT discards the received message
```

```
TP Id
                      TP/SEC/ITS-S/ENR/EB-10
     Summary
                      Check that ITS-S discards enrolment response without specified expiration time.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.2
     Config Id
                      CF03
  PICS Selection
                                                Initial conditions
with {
   the IUT awaiting EnrolmentResponse
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
         containing certificate_chain[last].unsigned_certificate.expiration
             set to 0
   then {
      the IUT discards the received message
```

```
TP/SEC/ITS-S/ENR/EB-11
       TP Id
     Summary
                      Check that ITS-S discards enrolment response which includs PSIDs that are not specified in
                       upper certificates.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.2
     Config Id
                      CF03
  PICS Selection
                                                 Initial conditions
   the IUT awaiting EnrolmentResponse
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
          containing certificate_chain
             set to array with length > 1
          containing certificate_chain[last-1].unsigned_certificate.scope.permissions.permissions_list
             set to array[1]
                 containing PSID_A
          containing certificate chain[last].unsigned certificate.scope.permissions.permissions list
             set to array[1]
                 containing PSID_B
   then {
      the IUT discards the CertificateResponse
```

```
TP/SEC/ITS-S/ENR/EB-12
       TP Id
     Summary
                     Check that ITS-S discards enrolment response if it has duplicated PSID.
     Reference
                     IEEE P1609.2/D12 [1], clause 6.3.9
     Config Id
                     CF03
  PICS Selection
                                              Initial conditions
with {
   the IUT having sent an EnrolmentRequest set to MSG_ENRREQ_IUT
      containing unsigned csr.type specific data.sec data exch_ca_scope
         containing permissions.permissions_list (V_PERM_LIST)
   the IUT awaiting EnrolmentResponse
                                             Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS
      containing unsigned_certificate.scope.permissions.permissions_list
         set to array[2]
             containing V_PERM_LIST[0]
             containing V_PERM_LIST[0]
   then {
      the IUT discards the received message
```

	TP Id	TP/SEC/ITS-S/ENR/EB-13-X	
Su	ımmary	Check that ITS-S discards enrolment response if the latitude is less than –900 000 000 or	
		greater than 900 000 000.	
Re	ference	IEEE P1609.2/D12 [1], clause 6.3.18	
Co	onfig ld	CF03	
PICS	Selection		
		Initial conditions	
with {			
the II	UT awaiting E	nrolmentResponse	
}	· ·	·	
		Expected behaviour	
ensure t	hat {		
wher	•		
		es a CertificateResponse (EnrolmentResponse) set to MSG_ENRRSP_TS	
	containing certificate_chain[last].unsigned_certificate		
		ing scope.region.circular_region.center.latitude	
	set to X_INVALID_LATITUDE		
١	Set to X_INVALID_LATITODE		
then	ſ		
	•	ds the received message	
۱ "	ie io i discare	as the received message	
}			
J		Variants	
Х		X INVALID LATITUDE	
A		90000001	
В		-90000001	

7	TP Id	TP/SEC/ITS-S/ENR/EB-14-X	
Su	mmary	Check that ITS-S discards enrolment response if the longitude is less than -1 800 000 000 or	
		greater than 1 800 000 000.	
Ref	ference	IEEE P1609.2/D12 [1], clause 6.3.18	
	nfig ld	CF03	
PICS	Selection		
		Initial conditions	
with {			
the Il	JT awaiting Er	nrolmentResponse	
}			
		Expected behaviour	
ensure th	hat {		
when	n {		
th	ne IUT receives	s a CertificateResponse set to MSG_ENRRSP_TS	
	containing c	ertificate_chain[last].unsigned_certificate	
		ng scope.region.circular_region.center.longitude	
	set to X_INVALID_LONGITUDE		
}	}		
then	then {		
th	the IUT discards the received message		
}			
}			
		Variants	
X		X_INVALID_LONGITUDE	
Α		1800000001	
В		-180000001	

6.2.1.2 Authorization

6.2.1.2.1 Normal Behavior

TP Id	TP/SEC/ITS-S/AUTH/NB-01		
Summary	Check that ITS-S generates correctly a generic AuthorizationRequest message.		
Reference	ETSI TS 102 941 [2], see table 4		
Config Id	CF03		
PICS Selection			
	Initial conditions		
with {			
the IUT in Enrolled	state		
}			
	Expected behaviour		
ensure that {			
when {	when {		
the IUT is reque	ested to send an AuthorizationRequest message		
}			
then {			
the IUT sends a valid CertificateRequest set to MSG_AUTHREQ_IUT			
}			
}]}		

```
TP Id
                      TP/SEC/ITS-S/AUTH/NB-02-X
     Summary
                      Check that ITS-S generates authorization request with various signature types.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.2.17
     Config Id
                      CF03
  PICS Selection
                                                Initial conditions
with {
   the IUT in Enrolled state
   the IUT is configured to use signature of type X_PKT_SIGNATURE
                                              Expected behaviour
ensure that {
   when {
      the IUT is requested to send an AuthorizationRequest message
   then {
      the IUT sends a valid CertificateRequest set to MSG_AUTHREQ_IUT
          containing signature.ecdsa_signature.R.type
             set to X_PKT_SIGNATURE
   }
                                                     Variants
  X
                           PIC Selection
                                                                              X_PKT_SIGNATURE
                   PIC_Generate_CompressedKey
                                                                             compressed_lsb_y_0/1
  Α
                 PIC_Generate_XCoordinateOnlyKey
PIC_Generate_UncompressedKey
  В
                                                                               x_coordinate_only
  С
                                                                                 uncompressed
```

```
TP Id
                       TP/SEC/ITS-S/AUTH/NB-03
     Summary
                      Check that ITS-S generates valid authorization request with a certificate containing lifetime field
                      when cf flag is set use_start_validity and lifetime_is_duration.
                      IEEE P1609.2/D12 [1], clause 6.3.2
     Reference
     Config Id
                       CF03
  PICS Selection
                      PIC_Generate_StartValidity AND PIC_Generate_LifetimeIsDuration
                                                 Initial conditions
with {
   the IUT in Enrolled state
   the IUT is configured to use use_start_validity and lifetime_is_duration
                                               Expected behaviour
ensure that {
   when {
      the IUT is requested to send an AuthorizationRequest message
   then {
      the IUT sends a valid CertificateRequest set to MSG AUTHREQ IUT
          containing unsigned_csr
             containing cf
                 indicating 'use_start_validity'_
                 indicating 'lifetime_is_duration'
             containing lifetime
   }
```

TP Id	TP/SEC/ITS-S/AUTH/NB-04		
Summary	Check that ITS-S generates valid authorization request with a certificate containing start_validity		
	field when cf flag is set use_start_validity.		
Reference	IEEE P1609.2/D12 [1], clause 6.3.2		
Config Id	CF03		
PICS Selection	PIC_Generate_StartValidity AND NOT PIC_Generate_LifetimeIsDuration		
	Initial conditions		
with {			
the IUT in Enrolled	state		
the IUT is configure	ed to use 'use_start_validity' but not 'lifetime_is_duration'		
}			
	Expected behaviour		
ensure that {			
when {			
the IUT is reque	ested to send an AuthorizationRequest message		
}			
`	then {		
	valid CertificateRequest set to MSG_AUTHREQ_IUT		
containing unsigned_csr			
containing cf			
indicating 'use_start_validity'			
not indicating 'lifetime_is_duration'			
containir	ng start_validity		
}			
}			

TP Id	TP/SEC/ITS-S/AUTH/NB-05		
Summary	Check that ITS-S generates valid authorization request with a CSR certificate with name of		
	length > 0 and $<= 32$.		
Reference	IEEE P1609.2/D12 [1], clause 6.3.19		
Config Id	CF03		
PICS Selection			
	Initial conditions		
with {			
the IUT in Enrolled	state		
}			
	Expected behaviour		
ensure that {			
when {			
the IUT is requ	the IUT is requested to send an AuthorizationRequest message		
}	}		
then {	then {		
	the IUT sends a valid CertificateRequest set to MSG_AUTHREQ_IUT		
containing unsigned_csr.containing type_specific_data.id_scope.name			
set to value of length > 0 and <= 32 or of length zero (see Note)			
}			
}			
NOTE: Value of ler	ngth 0 is encoded as '00'.		

TP Id	TP/SEC/ITS-S/AUTH/NB-06		
Summary	Check that ITS-S generates valid authorization request with a certificate containing more than 8		
	entries in the permissions_list field.		
Reference	IEEE P1609.2/D12 [1], clause 6.3.9		
Config Id	CF03		
PICS Selection	PIC_Generate_PsidArrayWithMoreThan8Entries		
	Initial conditions		
with {			
the IUT in Enrolled	state		
}			
	Expected behaviour		
ensure that {			
when {			
the IUT is reque	ested to send an AuthorizationRequest message with more than 8 PSID entries		
}			
then {			
the IUT sends a valid CertificateRequest set to MSG_AUTHREQ_IUT			
containing unsigned_csr.type_specific_data.id_scope.permissions.permissions_list			
set to array with length > 8			
}			
}	}		

1	ΓP ld	TP/SEC/ITS-S/AUTH/NB-07-X	
Su	mmary	Check that ITS-S generates valid authorization request with a certificate containing 1 to 8	
	•	entries in the permissions_list field.	
Ref	ference	IEEE P1609.2/D12 [1], clause 6.3.23	
Co	nfig ld	CF03	
PICS	Selection		
		Initial conditions	
with {			
the IL	JT in Enrolled	state	
}			
		Expected behaviour	
ensure th	nat {	·	
when	•		
		ested to send an AuthorizationRequest message with X_N PSID items	
}	.0.0		
then	{		
		a valid CertificateRequest set to MSG_AUTHREQ_IUT	
		unsigned_csr.type_specific_data.id_scope.permissions.permissions_list	
		ray with length X_N	
ı	Set to diray with length A_N		
}			
J	Variants		
Х		X_N	
A		1	
В		4	
C		8	
		o	

```
TP Id
                      TP/SEC/ITS-S/AUTH/NB-08
     Summary
                      Check that ITS-S generates valid authorization request with a valid hash.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.1
     Config Id
  PICS Selection
                      PIC_Generate_UncompressedKey
                                                Initial conditions
with {
   the IUT in Enrolled state
   the IUT has obtained an Enrolment Certificate (CERT_ENR_TS)
      containing unsigned_certificate.verification_key.public_key.type (V_PKT_VK_ENR)
          set to 'uncompressed'
                                              Expected behaviour
ensure that {
   when {
      the IUT is requested to send an AuthorizationRequest message
      the IUT sends a valid CertificateRequest set to MSG_AUTHREQ_IUT
          containing signer
             containing certificate or certificates[last]
                 containing unsigned_certificate.signer_id
                    calculated using compressed representation of V_PKT_VK_ENR
   }
```

```
TP Id
                      TP/SEC/ITS-S/AUTH/NB-09
     Summary
                      Check that ITS-S generates valid authorization request with a valid signature.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.33
     Config Id
                      CF03
  PICS Selection
                     PIC Generate UncompressedKey
                                               Initial conditions
with {
   the IUT in Enrolled state
   the IUT is configured to send requests with uncompressed verification_key
   the IUT is configured to send requests with uncompressed response_encryption_key
                                              Expected behaviour
ensure that {
   when {
      the IUT is requested to send an AuthorizationRequest message
   then {
      the IUT sends a valid CertificateRequest set to MSG_AUTHREQ_IUT
          containing unsigned_csr.verification_key.public_key.type (V_PKT_VK)
                                           containing unsigned_csr.response_encryption_key.public_key.type
             set to 'uncompressed'
(V_PKT_REK)
             set to 'uncompressed'
          containing signature.ecdsa_signature
             calculated using compressed representation of V_PKT_VK and V_PKT_REK
   }
```

TP ld	TP/SEC/ITS-S/AUTH/NB-10		
Summary	Check that ITS-S generates valid authorization request with a different		
	response_encryption_key for every request.		
Reference	[1], clause 6.3.34		
Config Id	CF03		
PICS Selection			
	Initial conditions		
with {			
the IUT in Enrolled	d state		
}			
	Expected behaviour		
ensure that {	ensure that {		
when {			
each time the I	IUT is requested to send an AuthorizationRequest message		
}			
then {			
the IUT sends a valid CertificateRequest set to MSG_AUTHREQ_IUT			
containing unsigned_csr.response_encryption_key			
set to value <> from the previous ones			
}			
}			

TP ld	TP/SEC/ITS-S/AUTH/NB-11		
Summary	Check that the ITS-S accepts a valid authorization response having correct fields and values.		
Reference	ETSI TS 102 867 [3], clause 5.1.2.1, table 14		
Config Id	CF03		
PICS Selection			
	Initial conditions		
with {			
the IUT in Enrolled	state		
the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT			
}	·		
	Expected behaviour		
ensure that {			
when {			
the IUT receives a valid CertificateResponse (AuthorizationResponse) set to MSG_AUTHRSP_TS			
}			
then {			
the IUT accepts	the IUT accepts the CertificateResponse		
}			

```
TP/SEC/ITS-S/AUTH/NB-12
       TP Id
     Summary
                      Check that the ITS-S accepts a valid authorization response having correct fields and values.
     Reference
                      IEEE P1609.2/D12 [1], clause 5.6.2.2
     Config Id
                      CF03
  PICS Selection
                                                Initial conditions
with {
   the IUT in Enrolled state
   the IUT has sent a valid CertificateRequest set to MSG_AUTHREQ_IUT
      containing unsigned_csr.type_specific_data.permission.permissions_list
          set to array
             containing PSID_A
             containing PSID_B
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a valid CertificateResponse set to MSG_AUTHRSP_TS
          containing certificate_chain[last].unsigned_certificate.type_specific_data.ANY_SCOPE
             containing permissions.permissions_list
                 set to array
                    not containing PSID_A
   then {
      the IUT accepts the CertificateResponse
   }
```

-	TP ld	TP/SEC/ITS-S/AUTH/NB-13-X	
			animatica managas simas di kurandan simastuma with
Su	mmary	· · · · · · · · · · · · · · · · · · ·	orization response signed by ecdsa_signature with
-		different public key types.	
	ference	IEEE P1609.2/D12 [1], clause 6.2.17	
	onfig Id	CF03	
PICS	Selection		
		Initial conditi	ons
with {			
the Il	JT in Enrolled	state	
the Il	the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT		
}			
		Expected beha	viour
ensure th	hat {		
when	•		
	•	es a valid CertificateResponse (Authorization	onResponse) to MSG AUTHRSP TS
		certificate_chain[last].signature.ecdsa_sign	•
		ng type set to X_PKT_SIGNATURE	ataront
3	oomann	ng type cot to A_t ttt _oto.tt tt ott	
then	ſ		
	•	s the CertificateResponse	
1	ie io i accept	3 the Certificater(esponse	
\ \			
ſ		Variants	
Х		PIC Selection	X PKT SIGNATURE
A		PIC_Verify_CompressedKey	compressed_lsb_y_0/1
В		C_Verify_XCoordinateOnlyKey	x_coordinate_only
С	P	IC_Verify_UncompressedKey	uncompressed

```
TP/SEC/ITS-S/AUTH/NB-14
        TP Id
     Summary
                      Check that the ITS-S accepts a valid authorization response with start_validity.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.2
     Config Id
  PICS Selection
                      PIC_Verify_StartValidity AND PIC_Verify_LifetimeIsDuration
                                                 Initial conditions
with {
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a valid CertificateResponse set to MSG_AUTHRSP_TS
          containing certificate_chain[last].unsigned_certificate
             containing cf
                 indicating 'use_start_validity'
                 not indicating 'lifetime_is_duration'
             containing start_validity
             not containing lifetime
   then {
      the IUT accepts the CertificateResponse
```

6.2.1.2.2 Exceptional Behavior

٦	ΓP ld	TP/SEC/ITS-S/AUTH/EB-01-X	
Su	mmary	Check that the ITS-S discards an authorization response having a non-permitted subject_type.	
Ref	erence	ETSI TS 102 867 [3], clause 5.1.2.1, IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 5.6.1.2	
	nfig ld	CF03	
PICS	Selection		
		Initial conditions	
with {	th {		
	the IUT in Enrolled state		
the Il	JT has sent a	valid AuthorizationRequest set to MSG_AUTHREQ_IUT	
}			
		Expected behaviour	
ensure th	•		
when			
th		s a CertificateResponse (AuthorizationResponse) set to MSG_AUTHRSP_TS	
		ertificate_chain[last].unsigned_certificate.subject_type	
	set to X_	INVALID_SUBJECT_TYPE	
}	,		
then		a the Oestificate Decreases	
1 -	ie iu i discardi	s the CertificateResponse	
}	}		
}	} Variants		
Х		X INVALID SUBJECT_TYPE	
A		sec_data_exch_identified_not_localized (1)	
В			
С		sec_data_exch_csr (3)	
D		wsa (4)	
E		wsa_csr (5)	
F		sec_data_exch_ca(6)	
H		wsa_ca (7)	
		crl_signer(8)	
		root_ca (255)	
G		ANY OTHER (128)	

```
TP/SEC/ITS-S/AUTH/EB-02-X
        TP Id
     Summary
                       Check that the ITS-S discards an authorization response having a non-permitted cf.
                       ETSI TS 102 867 [3], clause 5.1.2.1, IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 5.6.1.2
     Reference
     Config Id
                       CF03
  PICS Selection
                                                  Initial conditions
with {
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT
                                                Expected behaviour
ensure that {
   when {
       the IUT receives a CertificateResponse set to MSG_AUTHRSP_TS
          containing certificate_chain[last].unsigned_certificate.cf indicating X_INVALID_CONTENT_FLAGS
   then {
       the IUT discards the CertificateResponse
                                                       Variants
                                                                                    PIC Selection
                    X_INVALID_SUBJECT_TYPE
  X
                                                                NOT PIC_Verify_StartValidity
  Α
         use_start_validity (0)
  В
        encryption_key (2)
  С
        any value (3)
```

TP Id	TP/SEC/ITS-S/AUTH/EB-03-X	
Summary	Check that the ITS-S discards an authorization response having a non-permitted	
	PsidArray.type.	
Reference	ETSI TS 102 867 [3], clause 5.1.2.1, IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 5.6.1.2	
Config Id	CF03	
PICS Selection		
	Initial conditions	
with {		
the IUT in Enrolled	state	
the IUT has sent a	valid AuthorizationRequest set to MSG_AUTHREQ_IUT	
}		
	Expected behaviour	
ensure that {		
when {		
	s a CertificateResponse (AuthorizationResponse) set to MSG_AUTHRSP_TS	
	certificate_chain[last].unsigned_certificate.type_specific_data.ANY_SCOPE.permissions.type	
set to a	X_INVALID_PERM_TYPE	
}		
then {		
the IUT discards the CertificateResponse		
}		
}		
Variants		
X	X_INVALID_PERM_TYPE	
A from_issuer (0)	
B Any value (3)		
C Any value (25	55)	

```
TP Id
                      TP/SEC/ITS-S/AUTH/EB-04
     Summary
                      Check that the ITS-S discards an authorization response requesting acknowledgement.
     Reference
                      ETSI TS 102 867 [3], clause 5.1.2.1, IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 5.6.1.2
     Config Id
                      CF03
  PICS Selection
                                               Initial conditions
with {
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse (AuthorizationResponse) set to MSG_AUTHRSP_TS
         containing f
             indicating 'Requested'
   then {
      the IUT discards the CertificateResponse
```

```
TP Id
                      TP/SEC/ITS-S/AUTH/EB-05
                      Check that the ITS-S discards an authorization response that does not comply with the
     Summary
                      authorization request.
     Reference
                      ETSI TS 102 867 [3], clause 5.1.2.1, IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 5.6.1.2
     Config Id
                      CF03
  PICS Selection
                                                Initial conditions
with {
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse (AuthorizationResponse) set to MSG_AUTHRSP_TS
          containing fields that does not comply with the authorization request
   then {
      the IUT discards the CertificateResponse
```

```
TP/SEC/ITS-S/AUTH/EB-06
        TP Id
     Summary
                      Check that the ITS-S discards an authorization response error with incorrect
                      signerIdentifier_type.
                      ETSI TS 102 867 [3], clause 5.1.2.1, IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 5.6.1.2
     Reference
  Config Id
PICS Selection
                      CF03
                                                 Initial conditions
with {
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateRequestError set to MSG_AUTHERR_TS
          containing signer.type
             set to 'self'
   then {
      the IUT discards the CertificateRequestError
```

7	ΓP Id	TP/SEC/ITS-S/AUTH/EB-07-X	
Su	mmary	Check that the ITS-S discards an authorization response error having a non-permitted	
		subject_type.	
	ference	ETSI TS 102 867 [3], clause 5.1.2.1, IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 5.6.1.2	
	nfig Id	CF03	
PICS	Selection		
		Initial conditions	
with {			
	JT in Enrolled		
the IU	JT has sent a	valid AuthorizationRequest set to MSG_AUTHREQ_IUT	
}			
		Expected behaviour	
ensure th			
when			
th		s a CertificateRequestError set to MSG_AUTHERR_TS	
		igner.certificates[last].unsigned_certificate.subject_type	
,	set to X_	INVALID_SUBJECT_TYPE	
}	•		
	then {		
, tn	the IUT discards the CertificateRequestError		
, }	,		
<i>Y</i> Variants			
X		X_INVALID_SUBJECT_TYPE	
A		sec_data_exch_identified_not_localized (1)	
В		sec_data_exch_csr (3)	
C		wsa (4)	
D		wsa_csr (5)	
E		sec_data_exch_ca(6)	
F		Wsa_ca (7)	
H		crl_signer(8)	
		root_ca (255)	
G		ANY OTHER (128)	
9		ANT OTTEN (120)	

```
TP Id
                      TP/SEC/ITS-S/AUTH/EB-08
     Summary
                      Check that the ITS-S discards an authorization response having the subordinate certificate's
                      validity region not wholly contained in the issuing certificate's validity region.
                      ETSI TS 102 867 [3], clause 5.1.2.1, IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 5.6.1.2
     Reference
     Config Id
                      CF03
  PICS Selection
                                                Initial conditions
with {
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse set to MSG_AUTHRSP_TS
          containing certificate_chain[n].scope.region
             set to REGION_SMALL
          containing certificate_chain[n+1].scope.region
             set to REGION_INTERSECTING
   then {
      the IUT discards the CertificateResponse
```

```
TP Id
                      TP/SEC/ITS-S/AUTH/EB-09
                      Check that the ITS-S discards an authorization response error having the subordinate
     Summary
                      certificate's validity region not wholly contained in the issuing certificate's validity region.
                      ETSI TS 102 867 [3], clause 5.1.2.1, IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 5.6.1.2
     Reference
     Config Id
  PICS Selection
                                                Initial conditions
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG AUTHREQ IUT
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateRequestError set to MSG_AUTHERR_TS
          containing signer
             containing certificates[n].scope.region
                 set to REGION_SMALL
             containing certificates[n+1].scope.region
                set to REGION_INTERSECTING
   then {
      the IUT discards the CertificateRequestError
```

```
TP Id
                        TP/SEC/ITS-S/AUTH/EB-10
     Summary
                        Check that the ITS-S discards an authorization response having the subordinate certificate's
                        validity region not within in the issuing certificate's validity region.
ETSI TS 102 867 [3], clause 5.1.2.1, IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 5.6.1.2
     Reference
      Config Id
                        CF03
  PICS Selection
                                                     Initial conditions
with {
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT
                                                   Expected behaviour
ensure that {
   when {
       the IUT receives a CertificateResponse set to MSG_AUTHRSP_TS
           containing certificate_chain[n].scope.region
              set to REGION_SMALL
           containing certificate_chain[n+1].scope.region
              set to REGION_OUTSIDE
   then {
       the IUT discards the CertificateResponse
```

```
TP Id
                      TP/SEC/ITS-S/AUTH/EB-11
                      Check that the ITS-S discards an authorization response error having the subordinate
     Summary
                      certificate's validity region not within in the issuing certificate's validity region.
                      ETSI TS 102 867 [3], clause 5.1.2.1, IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 5.6.1.2
     Reference
     Config Id
  PICS Selection
                                                Initial conditions
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG AUTHREQ IUT
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateRequestError set to MSG_AUTHERR_TS
          containing signer
             containing certificates[n].scope.region
                 set to REGION_SMALL
             containing certificates[n+1].scope.region
                set to REGION_OUTSIDE
   then {
      the IUT discards the CertificateRequestError
```

```
TP Id
                      TP/SEC/ITS-S/AUTH/EB-12
     Summary
                      Check that the ITS-S discards an authorization response having the subordinate certificate
                      operational permissions are not a subset ofthe issuing certificate operational permissions
                      ETSI TS 102 867 [3], clause 5.1.2.1, IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 5.6.1.2
     Reference
     Config Id
                      CF03
  PICS Selection
                                                Initial conditions
with {
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse set to MSG_AUTHRSP_TS
          containing certificate_chain[n].scope.permissions
             not indicating PSID_A
          containing certificate_chain[n+1].scope.permissions
             indicating PSID_A
   }
   then {
      the IUT discards the CertificateResponse
```

```
TP Id
                      TP/SEC/ITS-S/AUTH/EB-13
                      Check that the ITS-S discards an authorization response error having the subordinate certificate
     Summary
                      operational permissions are not a subset of the issuing certificate operational permissions.
                      ETSI TS 102 867 [3] clause 5.1.2.1, IEEE P1609.2/D12 [1], 5.5.3.3, 5.6.1.2
     Reference
     Config Id
                      CF03
  PICS Selection
                                                 Initial conditions
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG AUTHREQ IUT
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateRequestError set to MSG_AUTHERR_TS
          containing signer
             containing certificates[n].scope.permissions
                 not indicating PSID_A
             containing certificates[n+1].scope.permissions
                indicating PSID_A
   then {
      the IUT discards the CertificateRequestError
```

TP ld	TP/SEC/ITS-S/AUTH/EB-14-X
Summary	Check that the ITS-S discards an authorization response encapsulated into 1609Dot2Data with
	protocol_version not egal to 2.
Reference	IEEE P1609.2/D12 [1], clause 6.2.1
Config Id	CF03
PICS Selection	
	Initial conditions
with {	
the IUT in Enrolle	d state
the IUT has sent a	a valid AuthorizationRequest set to MSG_AUTHREQ_IUT
}	
	Expected behaviour
ensure that {	
when {	
	es a 1609Dot2Data structure
	protocol_version
	(_INVALID_VERSION_NUMBER
containing	
	encrypted'
	encrypted_data.ciphertext
	eciphering process
	ing type
	to 'certificate_response'
	ing request
set	to MSG_AUTHRSP_TS
/	
}	
then {	
the IUT discar	ds the CertificateResponse
}	
}	
	Variants
Х	X_INVALID_VERSION_NUMBER
Α	0
В	1
С	3
D	255

Check that the ITS-S discards an authorization request error encapsulated into 1609Dot2Dowith protocol_version not egal to 2. Reference		
Reference IEEE P1609.2/D12 [1], clause 6.2.1 Config Id CF03 PICS Selection Initial conditions with { the IUT in Enrolled state the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT } Expected behaviour ensure that { when { the IUT receives a 1609Dot2Data structure containing protocol_version		
Config Id CF03 PICS Selection Initial conditions with { the IUT in Enrolled state the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT } Expected behaviour ensure that { when { the IUT receives a 1609Dot2Data structure containing protocol_version		
Initial conditions with { the IUT in Enrolled state the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT } Expected behaviour ensure that { when { the IUT receives a 1609Dot2Data structure containing protocol_version set to X_INVALID_VERSION_NUMBER containing type set to 'encrypted'		
Initial conditions with { the IUT in Enrolled state the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT } Expected behaviour ensure that { when { the IUT receives a 1609Dot2Data structure containing protocol_version set to X_INVALID_VERSION_NUMBER containing type set to 'encrypted'		
with { the IUT in Enrolled state the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT } Expected behaviour ensure that { when { the IUT receives a 1609Dot2Data structure containing protocol_version set to X_INVALID_VERSION_NUMBER containing type set to 'encrypted'		
the IUT in Enrolled state the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT Expected behaviour ensure that { when { the IUT receives a 1609Dot2Data structure containing protocol_version set to X_INVALID_VERSION_NUMBER containing type set to 'encrypted'		
the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT Expected behaviour		
Expected behaviour ensure that { when { the IUT receives a 1609Dot2Data structure containing protocol_version set to X_INVALID_VERSION_NUMBER containing type set to 'encrypted'		
ensure that { when { the IUT receives a 1609Dot2Data structure containing protocol_version set to X_INVALID_VERSION_NUMBER containing type set to 'encrypted'		
ensure that { when { the IUT receives a 1609Dot2Data structure containing protocol_version set to X_INVALID_VERSION_NUMBER containing type set to 'encrypted'		
when { the IUT receives a 1609Dot2Data structure containing protocol_version set to X_INVALID_VERSION_NUMBER containing type set to 'encrypted'		
the IUT receives a 1609Dot2Data structure containing protocol_version set to X_INVALID_VERSION_NUMBER containing type set to 'encrypted'		
containing protocol_version set to X_INVALID_VERSION_NUMBER containing type set to 'encrypted'		
set to X_INVALID_VERSION_NUMBER containing type set to 'encrypted'		
containing type set to 'encrypted'		
set to 'encrypted'		
/ After deciphering process		
containing type		
set to 'certificate_request_error'		
containing request		
set to MSG_AUTHERR_TS		
/		
}		
then {		
the IUT discards the CertificateResponse		
}		
}		
Variants		
X X_INVALID_VERSION_NUMBER		
Α 0		
B 1		
C 3		
D 255		

TP ld	TP/SEC/ITS-S/AUTH/EB-16	
Summary	Check that the ITS-S discards an authorization response with zero value in all expiration fields.	
Reference	IEEE P1609.2/D12 [1], clause 6.3.2	
Config Id	CF03	
PICS Selection		
	Initial conditions	
with {		
the IUT in Enrolled		
the IUT has sent a	valid AuthorizationRequest set to MSG_AUTHREQ_IUT	
}		
	Expected behaviour	
ensure that {		
when {		
the IUT receive	s a CertificateResponse (AuthorizationResponse) set to MSG_AUTHRSP_TS	
containing certificate_chain[last].unsigned_certificate		
containing expiration		
set to	0 0	
}		
then {		
the IUT discard	s the CertificateResponse	
}		
}		

```
TP/SEC/ITS-S/AUTH/EB-17
       TP Id
     Summary
                      Check that the ITS-S discards an authorization response with duplicate PSIDs.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.9
     Config Id
                      CF03
  PICS Selection
                                               Initial conditions
with {
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse (AuthorizationResponse) set to MSG_AUTHRSP_TS
         containing certificate_chain[last].unsigned_certificate
             containing type_specific_data.ANY_SCOPE.permissions.permissions_list
                set to array[2]
                    containing PSID_A
                    containing PSID_A
   then {
      the IUT discards the CertificateResponse
```

	TP ld	TP/SEC/ITS-S/AUTH/EB-18-X	
Su	mmary	Check that the ITS-S discards an authorization response with wrongly encoded latitude field.	
Ref	ference	IEEE P1609.2/D12 [1], clause 6.3.18	
Co	nfig ld	CF03	
PICS	Selection		
		Initial conditions	
with {			
the II	JT in Enrolled	state	
the II	JT has sent a	valid AuthorizationRequest set to MSG_AUTHREQ_IUT	
}			
		Expected behaviour	
ensure th	hat {		
when	n {		
th	the IUT receives a CertificateResponse (AuthorizationResponse) set to MSG_AUTHRSP_TS		
	containing certificate_chain[last].unsigned_certificate		
	containing scope.region.circular_region.center.latitude		
	set to X_INVALID_LATITUDE		
}	}		
then	then {		
th	the IUT discards the CertificateResponse		
}	}		
}			
Variants			
Χ		X_INVALID_LATITUDE	
Α		90000001	
В		-90000001	

	ΓP ld	TP/SEC/ITS-S/AUTH/EB-19-X
Su	mmary	Check that the ITS-S discards an authorization response with wrongly encoded longitude field.
Ref	erence	IEEE P1609.2/D12 [1], clause 6.3.18
Co	nfig ld	CF03
PICS	Selection	
		Initial conditions
with { the IUT in Enrolled state the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT		
J		Expected behaviour
ensure that { when { the IUT receives a CertificateResponse set to MSG_AUTHRSP_TS		
		Variants
Х		X_INVALID_LONGITUDE
A		180000001
В		-180000001

```
TP/SEC/ITS-S/AUTH/EB-20
        TP Id
     Summary
                        Check that the ITS-S discards an authorization response with an empty PsidSspArray.
     Reference
                        IEEE P1609.2/D12 [1], clause 6.3.23
     Config Id
                        CF03
  PICS Selection
                                                   Initial conditions
with {
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT
                                                 Expected behaviour
ensure that {
   when {
       the IUT receives a CertificateResponse (AuthorizationResponse) set to MSG_AUTHRSP_TS containing certificate_chain[last].unsigned_certificate
              containing ANY_SCOPE.permissions.permissions_list
                  set to array of length 0
   then {
       the IUT discards the CertificateResponse
   }
```

```
TP Id
                      TP/SEC/ITS-S/AUTH/EB-21
     Summary
                      Check that the ITS-S discards an authorization response with a certificate having a too long
                      service_specific_permission field
                      IEEE P1609.2/D12 [1], clause 6.3.24
     Reference
     Config Id
                      CF03
  PICS Selection
                                                Initial conditions
with {
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateResponse set to MSG_AUTHRSP_TS
          containing certificate chain[last].unsigned certificate
             containing type_specific_data.ANY_SCOPE.permissions.permissions_list
                 set to array[1]
                    containing a PsidSpp (V_PSIDSSPP_A)
                       containing service_specific_permission
                           longer than 31 octets
             containing a service_specific_permission
                 having a length > 32 octets
   then {
      the IUT discards the CertificateResponse
   }
```

```
TP/SEC/ITS-S/AUTH/EB-22
       TP Id
     Summary
                      Check that the ITS-S discards an authorization request error with having a wrongly calculated
                      request_hash
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.1
     Config Id
                      CF03
  PICS Selection
                     PIC_Verify_UncompressedKey
                                               Initial conditions
with {
   the IUT in Enrolled state
   the IUT has sent a valid AuthorizationRequest set to MSG_AUTHREQ_IUT
      containing unsigned_csr.verification_key.public_key.type (V_PKT_VK)
          set to 'uncompressed'
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateRequestError set to MSG_AUTHERR_TS
          containing request_hash
             calculated using uncompressed representation of V_PKT_VK
   }
   then {
      the IUT discards the CertificateRequestError
```

6.2.1.3 Sending Data

TP Id	TP/SEC/ITS-S/S-DATA/NB-01		
Summary	Check that ITS-S sends a correctly signed message with payload.		
Reference	IEEE P1609.2/D12 [1], clause 6.2.7		
Config Id	CF04		
PICS Selection	PIC_Generate_SignPayload		
	Initial conditions		
with {			
the IUT in Authorized state			
}	}		
Expected behaviour			
ensure that {			
when {			
the IUT is requested to send a signed message			
}			
then {			
the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT			
}			

TP Id	TP/SEC/ITS-S/S-DATA/NB-02		
Summary	Check that ITS-S sends correctly signed message with partial payload.		
Reference	IEEE P1609.2/D12 [1], clause 6.2.7		
Config Id	CF04		
PICS Selection	PIC_Generate_SignPartialPayload		
	Initial conditions		
with {			
the IUT in Authorize	ed state		
}			
	Expected behaviour		
ensure that {			
when {			
the IUT is reque	ested to send a signed message with partial data		
}			
then {			
the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT			
containing type			
set to 'signed_partial_payload'			
containing signed_data.unsigned_data			
containir	containing data		
}	· }		
}			

```
TP Id
                      TP/SEC/ITS-S/S-DATA/NB-03
     Summary
                      Check that ITS-S sends correctly signed message with external payload.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.2.7
     Config Id
                      CF04
  PICS Selection
                      PIC_Generate_SignExternalPayload
                                               Initial conditions
with {
   the IUT in Authorized state
                                              Expected behaviour
ensure that {
   when {
      the IUT is requested to send a signed message with external data
   then {
      the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT
         containing type
             set to 'signed_external_payload'
          containing signed_data.unsigned_data
             not containing data
   }
```

```
TP Id
                     TP/SEC/ITS-S/S-DATA/NB-04
     Summary
                      Check that if ITS-S generates correctly a signed message containing the generation time.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.2.7
     Config Id
                     CF04
                     PIC_Generate_SignPayload AND PIC_Generate_GenerationTime
  PICS Selection
                                               Initial conditions
with {
   the IUT in Authorized state and
   the IUT is configured to include generation time when signing a message
                                             Expected behaviour
ensure that {
   when {
      the IUT is requested to send a signed message
      the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT
         containing signed_data.unsigned_data
             containing tf
                indicating 'use_generation_time'
             containing generation_time
   }
```

```
TP Id
                     TP/SEC/ITS-S/S-DATA/NB-05
     Summary
                     Check that if ITS-S generates correctly multiple signed messages containing the generation
                      IEEE P1609.2/D12 [1], clause 6.2.7
    Reference
     Config Id
                      CF04
  PICS Selection
                     PIC_Generate_SignPayload AND PIC_Generate_GenerationTime
                                               Initial conditions
with {
   the IUT in Authorized state and
   the IUT is configured to include generation time when signing a message and
   the IUT has previously sent a signed message (V_MSG_0)
                                             Expected behaviour
ensure that {
   when {
      the IUT is requested to send a new signed message
   then {
      the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT
         containing signed_data.unsigned_data
             containing tf
                indicating 'use_generation_time'
             containing generation_time
                set to a value > V_MSG_0.signed_data.unsigned_data.generation_time and < CLT
   }
```

```
TP Id
                      TP/SEC/ITS-S/S-DATA/NB-06
     Summary
                      Check that if ITS-S generates correctly a ToBeSignedData containing the expiry time.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.2.7
     Config Id
                      CF04
                      PIC_Generate_SignPayload AND PIC_Generate_ExpirationTime
  PICS Selection
                                                Initial conditions
with {
   the IUT in Authorized state and
   the IUT is configured to include expiry_time when signing a message
                                              Expected behaviour
ensure that {
   when {
      the IUT is requested to send a signed message
      the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT
         containing signed_data.unsigned_data
             containing tf
                indicating 'expires'
             containing expiry_time
   }
```

```
TP Id
                      TP/SEC/ITS-S/S-DATA/NB-07
     Summary
                      Check that if ITS-S generates correctly a ToBeSignedData containing the generation location.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.2.7
     Config Id
  PICS Selection
                      PIC_Generate_SignPayload AND PIC_Generate_GenerationLocation
                                                Initial conditions
with {
   the IUT in Authorized state and
   the IUT is configured to include generation_location when signing a message
                                              Expected behaviour
ensure that {
   when {
      the IUT is requested to send a signed message
   then {
      the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT
         containing signed_data.unsigned_data
             containing tf
                indicating 'use_location'
             containing generation_location
   }
```

```
TP Id
                      TP/SEC/ITS-S/S-DATA/NB-08
     Summary
                      Check that the ITS-S can generate valid signed data with ecdsa_nistp256_with_sha256.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.2.15
     Config Id
                      CF04
  PICS Selection
                      PIC_Generate_SignPayload AND PIC_Generate_Ecdsa256
                                               Initial conditions
with {
   the IUT in Authorized state and
   the IUT is configured to use 'ecdsa_nistp256_with_sha256' as PKAlgorithm when signing a message
                                              Expected behaviour
ensure that {
   when {
      the IUT is requested to send a signed message
   then {
      the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT
         containing signed_data
             containing signer
                containing type
                    set to 'certificate_digest_with_ecdsap256'
                containing digest
             containing signature.algorithm
                set to 'ecdsa ecdsa_nistp256_with_sha256'
   }
```

```
TP Id
                     TP/SEC/ITS-S/S-DATA/NB-09
     Summary
                      Check that the ITS-S can generate valid signed data with ecdsa_nistp224_with_sha224.
    Reference
                     IEEE P1609.2/D12 [1], clause 6.2.15
     Config Id
  PICS Selection
                     PIC_Generate_SignPayload AND PIC_Generate_Ecdsa224
                                               Initial conditions
with {
   the IUT in Authorized state and
   the IUT is configured to use ecdsa_nistp224_with_sha224 as PKAlgorithm when signing a message
                                             Expected behaviour
ensure that {
   when {
             the IUT is requested to send a signed message
   then {
      the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT
         containing signed_data
             containing signer
                containing type
                    set to 'certificate_digest_with_ecdsap224'
                containing digest
             containing signature
                containing algorithm
                    set to 'ecdsa ecdsa_nistp224_with_sha224'
   }
```

•	TP Id	TP/SEC/ITS-S/S-DATA/NB-10-X	
Su	mmary	Check that ITS-S generates signed data	with signature with different public key types.
Reference		IEEE P1609.2/D12 [1], clause 6.2.15	
Co	onfig ld	CF04	
PICS	Selection	PIC_Generate_SignPayload	
Initial conditions			
with {			
the IUT in Authorized state			
the IUT is configured to sign messages using signatures with public key type of form X_PKT_SIGNATURE			
]			
Expected behaviour			
ensure that {			
when {			
the IUT is requested to send a signed message			
}			
then {			
the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT			
containing signed_data			
containing signature.ecdsa_signature.R.type			
set to X_PKT_SIGNATURE			
}			
Narioute .			
X		Variants PIC Selection	V DVT CICNATUDE
	DIO O		X_PKT_SIGNATURE
A		nerate_CompressedKeyPublicKey	compressed_lsb_y_0 or compressed_lsb_y_1
В		nerate_XCoordinateOnlyPublicKey	x_coordinate_only
С	PIC_Ger	erate_UncompressedKeyPublicKey	uncompressed

```
TP Id
                       TP/SEC/ITS-S/S-DATA/NB-11
     Summary
                       Check that ITS-S generates valid signed data with a certificate containing lifetime field when cf
                      flag is set to lifetime_is_duration.
                       IEEE P1609.2/D12 [1], clause 6.3.2
     Reference
     Config Id
                       CF04
                       PIC_Generate_SignPayload AND PIC_Generate_StartValidity AND
  PICS Selection
                       PIC_Generate_LifetimeIsDuration
                                                 Initial conditions
with {
   the IUT in Authorized state and
   the IUT is configured to put certificate in each of the signed message
                                               Expected behaviour
ensure that {
   when {
      the IUT is requested to send a signed message
   then {
      the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT
          containing signed_data.signer
             containing type
                 set to 'certificate'
              containing certificate.unsigned_certificate
                 containing cf
                    indicating 'lifetime_is_duration'
                 containing lifetime
   }
```

```
TP Id
                      TP/SEC/ITS-S/S-DATA/NB-12
     Summary
                      Check that ITS-S generates valid signed data with a certificate containing start_validity field.
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.2
     Config Id
                      CF04
  PICS Selection
                      PIC Generate SignPayload AND PIC Generate StartValidity AND NOT
                      PIC_Generate_LifetimeIsDuration
                                                 Initial conditions
with {
   the IUT in Authorized state and
   the IUT is configured to put certificate in each of the signed message
                                               Expected behaviour
ensure that {
   when {
      the IUT is requested to send a signed message
   then {
      the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT
          containing signed_data.signer
             containing type
                 set to 'certificate'
             containing certificate.unsigned_certificate
                 containing cf
                    indicating 'use_start_validity'
                 containing start_validity
   }
```

```
TP Id
                       TP/SEC/ITS-S/S-DATA/NB-13
                       Check that ITS-S generates valid signed data with a certificate containing encryption_key field.
     Summary
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.2
     Config Id
  PICS Selection
                      PIC_Generate_SignPayload AND PIC_Generate_EncryptionKey
                                                 Initial conditions
with {
   the IUT in Authorized state and
   the IUT is configured to put certificate in each of the signed message
                                               Expected behaviour
ensure that {
   when {
      the IUT is requested to send a signed message
   then {
      the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT
          containing signed_data.signer
             containing type
                 set to 'certificate'
             containing certificate.unsigned_certificate
                 containing cf
                    indicating 'encryption_key'
                 containing encryption_key
   }
```

```
TP Id
                      TP/SEC/ITS-S/S-DATA/NB-14
     Summary
                      Check that ITS-S generates valid signed data with a certificate containing more than 8 entries in
                      the permissions_list field
     Reference
                      IEEE P1609.2/D12 [1], clause 6.3.9
     Config Id
                      CF04
  PICS Selection
                      PIC_Generate_SignPayload AND PIC_Generate_PsidArrayWithMoreThan8Entries
                                                Initial conditions
with {
   the IUT in Authorized state and
   the IUT is configured to put certificate in each of the signed message
   the CERT_AUTH_TS.scope.permissions.permissions_list contains 9 PSID items
                                               Expected behaviour
ensure that {
   when {
      the IUT is requested to send a signed message
   then {
      the IUT sends a valid 1609Dot2Data set to MSG_SIGNED_IUT
          containing signed_data.signer
             containing type
                 set to 'certificate'
             containing certificate.unsigned_certificate.scope.permissions.permissions_list
                 containing 9 entries
   }
```

6.2.1.4 Receiving Data

6.2.1.4.1 Normal Behavior

6.2.1.4.1.1 Signature verification

7	TP ld	Id TP/SEC/ITS-S/R-DATA/NB-01-X				
Su	mmary		ta from another ITS-S when the Signer Identifier is a			
	Certificate Digest and the signature contains public key with various types.					
Ref	ference	ETSI TS 102 867 [3], clause 5.1.4				
Conf	iguration	CF04				
PICS	Selection					
		Initial conditi	ons			
with {						
IUT ii	n the operation	nal state				
}						
		Expected beha	viour			
ensure th	•					
when						
th		s a valid 1609Dot2Data set to MSG_SIGN	ED_TS			
	containing s	•				
		ng signer.digest				
	set to certificate_digest_with_ecdsa_p256 of CERT_AUTH_TS					
		ng a valid signature				
		aining ecdsa_signature.R.type				
	set to X_PKT_SIGNATURE					
}						
then	•					
l th	the IUT accepts the message					
}						
}	<u>}</u>					
V .		Variants	V DIT CIONATURE			
X	DIC 1	PIC Selection	X_PKT_SIGNATURE			
A		/erify_CompressedKeyPublicKey	compressed_lsb_y_0 or compressed_lsb_y_1			
В		erify_ XCoordinateOnlyPublicKey	x_coordinate_only			
С	PIC_\	Verify_ UncompressedPublicKey	uncompressed			

```
TP Id
                     TP/SEC/ITS-S/R-DATA/NB-02-X
    Summary
                     Check that ITS-S accepts valid signed data from another ITS-S when the Signer Identifier is a
                     Certificate Chain and the signature contains public key with various types.
    Reference
                     ETSI TS 102 867 [3], clause 5.1.4
  Configuration
                     CF04
  PICS Selection
                                               Initial conditions
with {
   IUT in the operational state
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a valid 1609Dot2Data set to MSG_SIGNED_TS
         containing signed_data
             containing signer
                containing type set to 'certificate_chain'
                containing certificates
             containing a valid signature
                containing ecdsa_signature.R.type
                   set to X_PKT_SIGNATURE
   then {
      the IUT accepts the message
  }
                                                    Variants
                                                                            X_PKT_SIGNATURE
                          PIC Selection
  X
               PIC_Verify_CompressedKeyPublicKey
                                                                 compressed_lsb_y_0 or compressed_lsb_y_1
  Α
  В
               PIC_Verify_XCoordinateOnlyPublicKey
                                                                              x_coordinate_only
              PIC_Verify_UncompressedKeyPublicKey
  C
                                                                               uncompressed
```

6.2.1.4.1.2 Signer verification

```
TP/SEC/ITS-S/R-DATA/NB-03
       TP Id
     Summary
                      Check that ITS-S accepts valid signed data from another ITS-S when the Signer Identifier is a
                      Certificate with a lifetime set to duration.
    Reference
                      IEEE P1609.2/D12 [1], clause 6.3.2
  Configuration
                      CF04
  PICS Selection
                     PIC_Verify_StartValidity AND PIC_Verify_LifetimeIsDuration
                                                 Initial conditions
with {
   IUT in the operational state
                                                Expected behaviour
ensure that {
   when {
      the IUT receives a valid 1609Dot2Data set to MSG_SIGNED_TS
          containing signed data.signer
             containing type set to 'certificate'
             containing certificate.unsigned_certificate
                 containing cf
                    indicating 'use_start_validity'
                    indicating 'lifetime_is_duration'
   then {
      the IUT accepts the message
```

```
TP/SEC/ITS-S/R-DATA/NB-04
       TP Id
     Summary
                      Check that ITS-S accepts valid signed data from another ITS-S when the Signer Identifier is a
                      Certificate without a lifetime set to duration.
                      IEEE P1609.2/D12 [1], clause 6.3.2
    Reference
  Configuration PICS Selection
                      CF04
                      PIC_Verify_StartValidity AND PIC_Verify_StartValidityIsATimestamp
                                                  Initial conditions
with {
   IUT in the operational state
                                                 Expected behaviour
ensure that {
   when {
      the IUT receives a valid 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data.signer
              containing type set to 'certificate'
              containing certificate.unsigned_certificate
                 containing cf
                     indicating 'use_start_validity'
                     not indicating 'lifetime_is_duration'
   then {
      the IUT accepts the message
```

TP Id				
	d IP/SEC/IIS-	S/R-DATA/NB-05-X		
Summ		S-S accepts valid signed data from another ITS-S when the Signer Identifier is a		
	Certificate containing <i>list_size</i> PSIDs.			
Refere	nce IEEE P1609.	2/D12 [1], clause 6.3.23		
Configur				
PICS Sele	ection			
		Initial conditions		
with {				
IUT in the	e operational state			
}	•			
		Expected behaviour		
ensure that	{			
when {				
the Il	JT receives a valid 1609	9Dot2Data set to MSG_SIGNED_TS		
CC	ontaining signed_data.s	igner		
	containing type set to	'certificate'		
	containing certificate.	unsigned_certificate		
	containing a subje	ect_type		
	set to 'sec_dat	ta_exch_ca'		
		permissions.permissions_list		
	containing X_I	LIST_SIZE PSID items		
}				
then {				
the Il	JT accepts the messag	e		
}				
}				
Variants				
Х	X_LIST_SIZE	PIC Selection		
Α	0			
В	1			
С	4			
D	8			
Е	9	PIC_Verify_PsidArrayWithMoreThan8Entries		

```
TP Id
                      TP/SEC/ITS-S/R-DATA/NB-06
    Summary
                      Check that ITS-S accepts valid signed data from another ITS-S when signed with a certificate
                     containing an IdentifiedNotLocalizedScope and a zero-length subject_name field.
    Reference
                     IEEE P1609.2/D12 [1], clause 6.3.22
  Configuration
                     CF04
  PICS Selection
                                                 Initial conditions
with {
   IUT in the operational state
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a valid 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data.signer
             containing type set to 'certificate'
             containing certificate.unsigned_certificate
                containing a subject_type
                    set to 'sec_data_exch_identified_not_localized'
                containing id_not_loc_scope.subject_name
                    set to an empty string
   then {
      the IUT accepts the message
```

```
TP Id
                      TP/SEC/ITS-S/R-DATA/NB-07
                      Check that ITS-S accepts valid signed data from another ITS-S when signed with a certificate
    Summary
                     containing an IdentifiedNotLocalizedScope and a non-zero-length subject_name field.
    Reference
                     IEEE P1609.2/D12 [1], clause 6.3.22
  Configuration
                     CF04
  PICS Selection
                                                 Initial conditions
   IUT in the operational state
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a valid 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data.signer
             containing type set to 'certificate'
             containing certificate.unsigned_certificate
                containing subject_type
                    indicating 'sec_data_exch_identified_not_localized'
                containing id_not_loc_scope.subject_name
                    set to non empty string
   }
   then {
      the IUT accepts the message
```

6.2.1.4.2 Exceptional behavior

6.2.1.4.2.1 Generic message verification

TP ld	ľ	TP/SEC/ITS-S/R-DATA/EB-01-X	
Summa	mmary Check that ITS-S discards a 1609.2 secured message if the protocol version is invalid.		
Referen	Reference IEEE P1609.2/D12 [1], clause 6.2.1		
Configura	Configuration CF04		
PICS Sele	ction		
		Initial conditions	
with {			
IUT in the	operation	nal state	
}			
		Expected behaviour	
col } then {	when { the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS containing protocol_version set to X_INVALID_VERSION_NUMBER }		
	Variants		
	_INVALID	_VERSION_NUMBER	
A 0			
B 1			
C 3			
D 25	5		

```
TP Id
                     TP/SEC/ITS-S/R-DATA/EB-02-X
    Summary
                     Check that ITS-S discards a 1609.2 secured message if the content type is not supported.
    Reference
                     IEEE P1609.2/D12 [1], clause 6.2.1
  Configuration
                     CF04
  PICS Selection
                                               Initial conditions
with {
   IUT in the operational state
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
         containing type
             set to X_INVALID_CONTENT_TYPE
   then {
      the IUT discards the message
                                                   Variants
          X_INVALID_CONTENT_TYPE
          unsecured (0)
   Α
   В
          encrypted(2)
          certificate_request(3)
   С
   D
          certificate_response(4)
          anonymous_certificate_response(5)
   Ε
   F
          certificate_request_error(6)
   G
          crl_request(7)
   Н
          crl(8)
   1
          signed_wsa(11)
   J
          certificate_response_acknowledgment (12)
         ANY_VALUE(128)
   Κ
```

6.2.1.4.2.2 Data fields verification

```
TP Id
                     TP/SEC/ITS-S/R-DATA/EB-03
    Summary
                     Check that ITS-S discards valid signed data from another ITS-S when the expiry time of the
                     received data is before the current time.
    Reference
                     ETSI TS 102 867 [3], clause 5.1.11
                     CF04
  Configuration
  PICS Selection
                                                Initial conditions
with {
  IUT in the operational state
                                              Expected behaviour
ensure that {
  when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
         containing signed_data.unsigned_data
             containing tf
                indicating 'expires'
             containing expiry_time
                set to value < CLT
   then {
      the IUT discards the message
  }
```

```
TP Id
                     TP/SEC/ITS-S/R-DATA/EB-04
    Summary
                     Check that ITS-S discards valid signed data which expires before generation time.
    Reference
                     IEEE P1609.2/D12 [1], clause 5.5.3.2.1
  Configuration
                     CF04
  PICS Selection
                                               Initial conditions
with {
   IUT in the operational state
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
         containing signed_data
             containing generation_time
                set to V_GEN_TIME
             containing expiry_time
                set to V_GEN_TIME - 1min
   }
   then {
      the IUT discards the message
```

```
TP Id
                      TP/SEC/ITS-S/R-DATA/EB-05
     Summary
                      Check that ITS-S discards valid signed data generated early then the validity period of the
                      signing certificate.
                      IEEE P1609.2/D12 [1], 5.5.3.2.1
    Reference
  Configuration
                      CF04
  PICS Selection
                                                 Initial conditions
with {
   IUT in the operational state
                                                Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
          containing signed data
             containing generation_time set to V_GEN_TIME
             containing signer
                 containing type
                    set to 'certificate_chain'
                 containing certificates[last].unsigned_certificate
                    containing a start_validity
                        set to V_GEN_TIME + 1min (V_START_VALIDITY_TIME)
                    containing an expiration
                        set to V_START_VALIDITY_TIME + 1Y
   then {
      the IUT discards the message
```

```
TP Id
                      TP/SEC/ITS-S/R-DATA/EB-06
     Summary
                      Check that ITS-S discards valid signed data generated later then the validity period of the
                      signing certificate.
                      IEEE P1609.2/D12 [1], clause 5.5.3.2.1
    Reference
  Configuration
                      CF04
  PICS Selection
                                                  Initial conditions
with {
   IUT in the operational state
                                                Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data
             containing generation_time set to V_GEN_TIME
             containing signer
                 containing type
                    set to 'certificate_chain'
                 containing certificates[last].unsigned_certificate
                    containing an expiration
                        set to V_GEN_TIME - 1min
   then {
      the IUT discards the message
```

```
TP Id
                     TP/SEC/ITS-S/R-DATA/EB-07
    Summary
                     Check that ITS-S discards valid signed data which expires early then the validity period of the
                     signing certificate.
    Reference
                     IEEE P1609.2/D12 [1], clause 5.5.3.2.1
  Configuration
                     CF04
  PICS Selection
                                                Initial conditions
with {
   IUT in the operational state
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data
             containing expiry_time
                set to V_EXP_TIME
             containing signer
                containing type
                    set to 'certificate_chain'
                containing certificates[last].unsigned_certificate
                    containing a start_validity
                       set to V_EXP_TIME + 1min (V_START_VALIDITY_TIME)
                    containing an expiration
                       set to V_START_VALIDITY_TIME + 1Y
   then {
      the IUT discards the message
   }
```

```
TP Id
                      TP/SEC/ITS-S/R-DATA/EB-08
     Summary
                      Check that ITS-S discards valid signed data which expires later then the validity period of the
                      signing certificate.
                      IEEE P1609.2/D12 [1], clause 5.5.3.2.1
    Reference
  Configuration
                      CF04
  PICS Selection
                                                  Initial conditions
with {
   IUT in the operational state
                                                Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data
             containing expiry_time set to V_EXP_TIME
             containing signer
                 containing type
                    set to 'certificate_chain'
                 containing certificates[last].unsigned_certificate
                    containing an expiration
                        set to V_EXP_TIME - 1min
   then {
      the IUT discards the message
   }
```

```
TP Id
                     TP/SEC/ITS-S/R-DATA/EB-09
    Summary
                     Check that ITS-S discards valid signed data from another ITS-S when the generation location of
                     the received data is beyond the range considered valid by the IUT.
    Reference
                     ETSI TS 102 867 [3], clause 5.1.11
  Configuration
                     CF04
  PICS Selection
                                                Initial conditions
with {
   IUT in the operational state
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data.unsigned_data
             containing tf
                indicating 'use_location'
             containing generation_location
                containing latitude
                    set to PARIS_LAT
                containing longitude
                    set to PARIS_LON
   then {
      the IUT discards the message
```

```
TP Id
                      TP/SEC/ITS-S/R-DATA/EB-10
    Summary
                      Check that ITS-S discards valid signed data when the generated location is outside the validity
                     region of the signer's certificate.
                     IEEE P1609.2/D12 [1], clause 5.5.3.2.1
    Reference
  Configuration
                     CF04
  PICS Selection
                                                 Initial conditions
with {
   IUT in the operational state
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data
             containing signer
                containing type set to 'certificate'
                containing certificate.unsigned_certificate.scope.region
                set to REGION SMALL
             containing unsigned_data.generation_location
                containing latitude
                    set to PARIS_LAT
                containing longitude
                    set to PARIS_LON
   then {
      the IUT discards the message
  }
```

6.2.1.4.2.3 Signature verification

```
TP Id
                     TP/SEC/ITS-S/R-DATA/EB-11
    Summary
                     Check that ITS-S discards data with a cryptographically invalid signature.
    Reference
                     IEEE P1609.2/D12 [1], clause 6.2.3
  Configuration
                     CF04
  PICS Selection
                                                Initial conditions
with {
  IUT in the operational state
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
         containing signed_data
             containing signature.ecdsa_signature
                set to the invalid signature value
   then {
      the IUT discards the message
  }
```

6.2.1.4.2.4 Signer verification

	TP ld	TP/SEC/ITS-S/R-DATA	V/EB-12-X
Sı	mmary	Check that ITS-S disca permitted value.	rds a signed 1609.2 message if the signer type is not set to a
Re	ference	IEEE P1609.2/D12 [1],	clause 6.2.1
	iguration	CF04	
PICS	Selection		
			Initial conditions
with {			
IUT in	the operational st	ate	
}			
			xpected behaviour
when { the } then {	ensure that { when { the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS containing signed_data.signer containing type set to X_INVALID_SIGNER_TYPE } then { the IUT discards the message } }		
X	V INIVALID VE	DEION NIIMDED	Variants Comments
		RSION_NUMBER	
A B	'self' (0) 6		Self-signed certificates are not allowed Invalid value
	-		
U	255		Invalid value

TP ld	TP/SEC/ITS-S/R-DATA/EB-13	
	1110-11110 J.M. 211111-2-10	
Summary	Check that ITS-S discards received data signed with a revoked certificate.	
Reference	IEEE P1609.2/D12 [1], clause 5.5.3.2.1	
Configuration	CF04	
PICS Selection		
	Initial conditions	
with {		
IUT in the operatio	nal state	
}		
	Expected behaviour	
ensure that {		
when {		
the IUT receive	es a 1609Dot2Data set to MSG_SIGNED_TS	
containing	signed_data.signer	
containi		
	o 'certificate'	
	ng certificate	
	o revoked Certificate	
Set to revoked Certificate		
) the are (
then {	1. 11	
the IUT discard	as the message	
}		
}		

	TP Id	TP/SEC/ITS-S/R-DATA/EB-14-X
S	ummary	Check that ITS-S discards valid signed data when the signer is a certificate chain in which the
		region of validity of a subordinate certificate overlaps but is not wholly contained by the region of
		validity of its issuing certificate.
	eference	IEEE P1609.2/D12 [1], clause 5.5.3.2.3
	nfiguration	CF04
PICS	S Selection	
		Initial conditions
with {		
IUT	in the operatio	nal state
}		
		Expected behaviour
ensure		
	en {	
	the IUT receive	s a 1609Dot2Data set to MSG_SIGNED_TS
		signed_data.signer
		ng type set to 'certificate_chain'
		ng certificates[n].scope.region
		o REGION_SMALL
		ng certificates[n+1].scope.region
	set t	o X_REGION
}		
the	•	
	the IUT discard	s the message
}		
}		
		Variants
	X_REGION	
	REGION_INTE	
\vdash	REGION_OUT	
С	REGION_MED	IUM

TP ld	TP/SEC/ITS-S/R-DATA/EB-15-X		
Summary Check that ITS-S discards valid signed data when the signer is a certificate chain in which t			
,	validity period of a subordinate certificate is outside that of its issuing certificate.		
Reference			
Configuration	CF04		
PICS Selection	PIC_Verify_StartValidity AND PIC_Verify_StartValidityIsATimestamp		
	Initial conditions		
with {			
IUT in the operation	onal state		
}			
	Expected behaviour		
ensure that {			
when {			
	es a 1609Dot2Data set to MSG_SIGNED_TS		
	signed_data.signer		
containing type set to 'certificate_chain'			
	ing certificates[last-1].unsigned_certificate		
	taining cf		
	set to 'use_start_validity'		
	taining an expiration		
	set to X_TIME_EXP1		
	taining start_validity		
	set to X_TIME_START1		
	ing certificates[last].unsigned_certificate taining cf		
	set to 'use start validity'		
containing an expiration			
	set to X TIME EXP2		
	taining start validity		
	set to X TIME START2		
,			

	Set to X_TIME_START2						
} *bo	n (
the	•	maaaaa					
,	the IUT discards the	message					
}							
}			Variants				
Х	X_TIME_START1	X_TIME_EXP1	X_TIME_START2	X_TIME_EXP2	Comment		
					Subordinate certificate validity		
Α	CLT+2Y	CLT+3Y	CLT-1Y	CLT+1Y	period is totaly before the issuing		
					one		
					Subordinate certificate validity		
В	CLT-1Y	CLT+2Y	CLT-2Y	CLT+1Y	period is intersecting the issuing		
					one		
					Subordinate certificate validity		
С	CLT-2Y	CLT+1Y	CLT-1Y	CLT+2Y	period is intersecting the issuing		
					one		
					Subordinate certificate validity		
D	CLT-1Y	CLT+1Y	CLT+2Y	CLT+3Y	period is totaly after the issuing		
					one		

```
TP Id
                      TP/SEC/ITS-S/R-DATA/EB-16
     Summary
                      Check that ITS-S discards valid signed data when the signer is a certificate chain in which the
                      operational permissions of a subordinate certificate are not a subset of the permissions of its
                      issuing certificate.
                      IEEE P1609.2/D12 [1], clause 5.5.3.3
    Reference
  Configuration
                      CF04
  PICS Selection
                                                  Initial conditions
with {
   IUT in the operational state
                                                Expected behaviour
ensure that {
  when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data.signer
             containing type set to 'certificate_chain'
             containing certificates[last-1].unsigned_certificate
                 containing scope.permissions.permissions_list
                    set to array[1]
                        containing PSID_A
             containing certificates[last].unsigned_certificate
                 containing scope.permissions.permissions_list
                    set to array[1]
                        containing PSID B
   then {
      the IUT discards the message
```

```
TP Id
                      TP/SEC/ITS-S/R-DATA/EB-17
     Summary
                      Check that ITS-S discards valid signed data when the signer is a certificate chain in which the
                      subordinate certificate has a valid signature which is not the signature of its issuing certificate.
                      IEEE P1609.2/D12 [1], clause 5.5.3.3
    Reference
  Configuration
                      CF04
  PICS Selection
                                                  Initial conditions
with {
   IUT in the operational state
                                                 Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data.signer
             containing type set to 'certificate_chain'
             containing certificates[last]
                 containing valid signature
                    verifiable using verification key of the certificate pointed by signer_id
                 containing signer_id
                    set to the value not equal to the 8-byte hash of the certificates[last-1]
   then {
      the IUT discards the message
```

```
TP/SEC/ITS-S/R-DATA/EB-18
        TP Id
     Summary
                       Check that ITS-S discards valid signed data when the signer is a certificate chain in which an
                       issuing certificate is not permitted to issue certificates of its subordinate certificate's type.
                       IEEE P1609.2/D12 [1], clause 5.5.3.3
     Reference
  Configuration PICS Selection
                       CF04
                                                     Initial conditions
with {
   IUT in the operational state
                                                   Expected behaviour
ensure that {
   when {
       the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
           containing signed_data.signer
              containing type set to 'certificate_chain' containing certificates[last-1].unsigned_certificate
                  containing a scope
                      containing permitted_subject_types
                          set to 'sec_data_exch_identified_localized'
              containing certificates[last].unsigned_certificate
                  containing a subject_type
                      set to 'sec_data_exch_anonymous'
   then {
       the IUT discards the message
   }
```

T	TP Id	TP/SEC/ITS-S/R-DATA/EB-19-X	
Sur	Immary Check that ITS-S discards a signed 1609.2 message if the version_and_type field is not set to		
		the value 2.	
Ref	erence	IEEE P1609.2/D12 [1], clause 6.3.2	
Confi	guration	CF04	
PICS :	Selection		
		Initial conditions	
with {			
IUT ir	n the operatio	nal state	
}			
		Expected behaviour	
ensure th	nat {		
when	١ {		
th		es a 1609Dot2Data set to MSG_SIGNED_TS	
		signed_data.signer	
	containi	ng type set to 'certificate_chain'	
		ng certificates[last].version_and_type	
	set t	o INVALID_CERT_VERSION_AND_TYPE	
}			
then	{		
th	ne IUT discard	ds the message	
}	}		
}			
	Variants		
Υ		INVALID_CERT_VERSION_AND_TYPE	
Α		0	
В		1	
С		3	
D		255	

```
TP Id
                      TP/SEC/ITS-S/R-DATA/EB-20
     Summary
                      Check that ITS-S discards a signed 1609.2 message if the signature is calculated over the hash
                     of the version_and_type and the unsigned_certificate fields if the calculation does not use the
                     compressed representation of all public keys and reconstruction values contained in the
                      certificate.
                     IEEE P1609.2/D12 [1], clause 6.3.1
    Reference
  Configuration
                     CF04
  PICS Selection
                     PIC_Verify_UncompressedKey
                                                 Initial conditions
with {
   IUT in the operational state
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data.signer
             containing type
                 set to 'certificate_chain'
             containing certificates[last].unsigned_certificate
                 containing verification_key.public_key.type (V_PKT_VK)
                    set to 'uncompressed'
                containing signature.ecdsa_signature
                    calculated using uncompressed representation of V_PKT_VK
   then {
      the IUT discards the message
   }
```

```
TP Id
                      TP/SEC/ITS-S/R-DATA/EB-21
     Summary
                      Check that ITS-S discards a signed 1609.2 message if both the crl series and the expiration
                      fields in the unsigned_certificate are empty.
    Reference
                      IEEE P1609.2/D12 [1], clause 6.3.1
  Configuration
                      CF04
  PICS Selection
                                                 Initial conditions
with {
   IUT in the operational state
                                               Expected behaviour
ensure that {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data.signer
             containing type
                 set to 'certificate_chain'
             containing certificate[last].unsigned_certificate
                 containing crl_series
                    set to 0
                 containing expiration
                    set to 0
   then {
      the IUT discards the message
```

```
TP/SEC/ITS-S/R-DATA/EB-22
       TP Id
     Summary
                      Check that ITS-S discards a signed 1609.2 message if the permissions requested in the end-
                      user certificate contains duplicate PSIDs.
                      IEEE P1609.2/D12 [1], clause 6.3.9
    Reference
  Configuration PICS Selection
                      CF04
                                                  Initial conditions
with {
   IUT in the operational state
                                                Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data.signer
             containing type
                 set to 'certificate_chain'
              containing\ certificates [last]. unsigned\_certificate. scope. permissions. permissions\_list
                 set to array[2]
                     containing PSID_A
                     containing PSID_A
   then {
      the IUT discards the message
```

T	TP Id	TP/SEC/ITS-S/R-DATA/EB-23-X		
Sur	mmary	Check that ITS-S discards a signed 1609.2 message if the latitude specified in the region		
		associated with the signers certificate scope is outside the limits of ±90°.		
Ref	erence	IEEE P1609.2/D12 [1], clause 6.3.9		
Confi	guration	CF04		
PICS	Selection			
		Initial conditions		
with { IUT ir }	n the operatio	nal state		
		Expected behaviour		
ensure th	nat {			
when	ı {			
th	e IUT receive	es a 1609Dot2Data set to MSG_SIGNED_TS		
	containing signed_data.signer			
	containing type			
	set to 'certificate_chain'			
		ng certificates[last].unsigned_certificate.scope.region		
	containing latitude			
	set to X_INVALID_LATITUDE			
}	_			
then	en {			
th	the IUT discards the message			
}				
}				
		Variants		
Χ		X_INVALID_LATITUDE		
Α		90000001		
В		-90000001		

```
TP/SEC/ITS-S/R-DATA/EB-24-X
       TP Id
                      Check that ITS-S discards a signed 1609.2 message if the longitude specified in the region
    Summary
                     associated with the signers certificate scope is outside the limits of ±180°.
                     IEEE P1609.2/D12 [1], clause 6.3.9
    Reference
  Configuration PICS Selection
                     CF04
                                                 Initial conditions
with {
   IUT in the operational state
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data.signer
             containing type
                 set to 'certificate_chain'
             containing certificates[last].unsigned_certificate.scope.region
                 containing longitude
                    set to X_INVALIT_LONGITUDE
   then {
      the IUT discards the message
                                                     Variants
  X
                                                 X_INVALID_LONGITUDE
                                                        1800000001
  Α
                                                        -1800000001
  В
```

TP ld	TP/SEC/ITS-S/R-DATA/EB-25		
Summary	Check that ITS-S discards a signed 1609.2 message if it contains a secured data exchange,		
	identified not localized scope with zero PSID SSPs in its permissions list.		
Reference	IEEE P1609.2/D12 [1], clause 6.3.23		
Configuration	CF04		
PICS Selection			
	Initial conditions		
with {			
IUT in the operatio	onal state		
}			
	Expected behaviour		
ensure that {			
when {			
the IUT receive	es a 1609Dot2Data set to MSG_SIGNED_TS		
•	signed_data.signer		
containi			
	o 'certificate_chain'		
	ng certificates[last].unsigned_certificate.scope.permissions.permissions_list		
	o array[0]		
not containing any PSID SSP			
}			
,	then {		
the IUT discard	ds the message		
}			
}			

```
TP Id
                     TP/SEC/ITS-S/R-DATA/EB-26
    Summary
                     Check that ITS-S discards a signed 1609.2 message if it contains a secured data exchange,
                     identified not localized scope with a PSID SSPs of more than 31 octets.
                     IEEE P1609.2/D12 [1], clause 6.3.23
    Reference
  Configuration
                     CF04
  PICS Selection
                                                 Initial conditions
with {
   IUT in the operational state
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data set to MSG_SIGNED_TS
          containing signed_data.signer
             containing type
                set to 'certificate_chain'
             containing certificates[last].unsigned_certificate
                containing scope.permissions.permissions_list
                    set to array[1]
                       containing V_PSIDSSPP_A
                           containing service_specific_permission
                              longer than 31 octets
   then {
      the IUT discards the message
```

6.2.2 Certificate Authority

6.2.2.1 Normal Behavior

6.2.2.1.1 Generic message verification

TP Id	TP/SEC/CA/NB-01			
Summary	Summary Check that CA correctly decrypts a Certificate Request.			
Reference	IEEE P1609.2/D12 [1], clause 5.6.2.1			
Config Id	CF01, CF02			
PICS Selection				
	Initial conditions			
with {				
the IUT in operation	nal state			
}	}			
	Expected behaviour			
ensure that {	ensure that {			
when {	when {			
the IUT receives	the IUT receives a CertificateRequest			
}				
then {				
the IUT decrypts the request				
}				
}				

TP	ld TP/SEC/CA/NB-02-X				
Sum	mary Check that CA generates certificat	Check that CA generates certificate response encoded using the key stored in			
	response_encryption_key field in t				
Refer	rence IEEE P1609.2/D12 [1], clause 6.3.	34			
Conf	fig ld CF01, CF02				
PICS Se	election				
	Initial	conditions			
with {					
the IUT	in operational state				
}					
	Expecte	d behaviour			
ensure that	t {				
when {					
the	IUT receives a CertificateRequest set to X_RE	QUEST			
	containing unsigned_csr.response_encryption_	key (V_RESPONSE_ENC_KEY)			
}	}				
then {					
	IUT sends a CertificateResponse set to X_RES	SPONSE			
	encrypted using V_RESPONSE_ENC_KEY				
}					
}	}				
	Variants				
X	X_REQUEST	X_RESPONSE			
Α	MSG_ENRREQ_TS	MSG_ENRRSP_IUT			
В	MSG_AUTHREQ_TS	MSG_AUTHRSP_IUT			

TP	Id TP/SEC/CA/NB	03-X				
Sum	mary Check that CA g	Check that CA generates certificate response.				
Refe	ence IEEE P1609.2/D	12 [1], clause 6.2.17				
Conf	ig ld CF01, CF02					
PICS S	election					
	·	Initial conditi	ions			
with {						
the IUT	in operational state					
}						
		Expected beha	aviour			
ensure tha	t {					
when {						
the	IUT receives a valid Certifica	eRequest set to X_REQ	UEST			
}						
then {						
	IUT sends a CertificateRespo		E			
	containing certificate_chain[la					
	verifiable using CERT_C	unsigned_certificate.ve	rification_key			
}	}					
}	}					
ļ	Variants					
X	X_REQUES		X_RESPONSE			
Α	MSG_ENRRE	_	MSG_ENRRSP_IUT			
В	MSG_AUTHRE	Q_TS	MSG_AUTHRSP_IUT			

```
TP/SEC/CA/NB-04-X
       TP Id
     Summary
                      Check that the CA accepts a valid certificate request having correct fields and values, signed by
                      a signer_id with type set to 'certificate'. IEEE P1609.2/D12 [1], clause 6.2.4
    Reference
     Config Id
                      CF01, CF02
  PICS Selection
                                                 Initial conditions
with {
   the IUT in operational state
                                               Expected behaviour
ensure that {
   when {
      the IUT receives a valid CertificateRequest set to X_REQUEST
          containing signer
             containing type
                 set to 'certificate'
             containing certificate
   }
   then {
      the IUT sends a CertificateResponse set to X_RESPONSE
                                                      Variants
   X
                           X_REQUEST
                                                                                X_RESPONSE
   Α
                        MSG_ENRREQ_TS
                                                                             MSG_ENRRSP_IUT
                                                                             MSG_AUTHRSP_IUT
   В
                       MSG_AUTHREQ_TS
```

TP	ld	TP/SEC/CA/NB-05-X			
Sumi	mary	Check that the CA accepts a valid certificate request having correct fields and values, signed by			
		a signer_id with type set to 'certificate_chain'.			
Refer	ence	IEEE P1609.2/D12 [1], clause 6.2.4			
Conf	ig ld	CF01, CF02			
PICS Se	election				
		Initial conditions			
with {					
the IUT	in operation	nal state			
}					
		Expected behaviour			
ensure that	t {				
when {					
the	IUT receives	s a CertificateRequest set to X_REQUEST			
	containing s	igner			
	containin	ng type			
	set to	o certificate_chain'			
	containin	ng certificates			
		o array of certificates			
}	}				
then {	then {				
	the IUT sends a CertificateResponse set to X_RESPONSE				
}	}				
}	}				
		Variants			
Y		Y REQUEST Y RESPONSE			

6.2.2.1.2 **Key Compression**

TP	ld	TP/SEC/CA/NB-06-X-Y			
Sum	nmary Check that an CA accepts a certificate request, signed by a valid certificate chain and		e request, signed by a valid certificate chain and		
	-	containing various public key types.			
Refe	ence	IEEE P1609.2/D12 [1], clause 6.2.17			
	fig Id CF01, CF02				
PICS Se	election				
		Initial co	nditions		
with {					
	in operation				
the IUT	is configure	ed to use signature of type Y_PKT_RE	S_SIGN		
}					
		Expected b	pehaviour		
ensure tha	t {				
when {					
		s a valid CertificateRequest set to X_F	REQUEST		
	containing s				
		ertificate_chain'			
		igner.certificate_chain[last]			
		ng signature.ecdsa_signature.R.type			
		Y_PKT_SIG_SIGN	v muhlin kayatan n		
		ng unsigned_certificate.verification_ke b Y_PKT_SIG_VK	y.public_key.type		
			ou tuno		
	set to Y_	nsigned_csr.verification_key.public_k _ PKT_VK			
		nsigned_csr.response_encryption_ke _PKT_REK	y.public_key.type		
		ignature.ecdsa_signature			
		ed using compressed representation o	f Y_PKT_VK and Y_PKT_REK		
	containir				
	set to	Y_PKT_REQ_SIGN			
}	}				
then {					
		valid CertificateResponse set to X_R	ESPONSE		
		ertificates[last]			
		ng unsigned_certificate.verification_ke	y.public_key.type		
		Y_PKT_VK			
		ng signature.ecdsa_signature	(
	calculated using compressed representation of Y_PK_TYPE_VK and Y_PK_TYPE_REK				
	containing R.type				
	set to Y_PKT_RES_SIGN				
}					
}		Varia	inte		
Х		X_REQUEST	X_RESPONSE		
		MSG_ENRREQ_TS	MSG_ENRRSP_IUT		
A B		MSG_ENRREQ_IS MSG_AUTHREQ_TS	MSG_ENRRSP_IUT MSG_AUTHRSP_IUT		
D		WISG_AUTHREW_15	MIOG_AUTHKOP_IUT		

Possible values:

Comp : compressed_lsb_y_0 or compressed_lsb_y_1
X_co : x_coordinate_only
Uncomp: uncompressed

Υ	Y_PKT_SIG_VK	Y_PKT_SIG_SIGN	Y_PKT_REQ_SIGN	Y_PKT_VK	Y_PKT_REK	Y_PKT_RES_SIGN
Α	Comp	X_co	X_co	Comp	Comp	Comp
В	X_co	X_co	X_co	X_co	X_co	X_co
С	Uncomp	Uncomp	Uncomp	Uncomp	Uncomp	Uncomp
D	Comp	U Uncomp	Uncomp	Comp	X_co	Uncomp
Е	X_co	Uncomp	Uncomp	X_co	X_co	X_co
F	Uncomp	Comp	Comp	Uncomp	Uncomp	Comp
G	Υ	Comp	Comp	X_co	Comp	Uncomp
Н	X_co	Comp	Comp	X_co	X_co	X_co

6.2.2.1.3 Permissions

	TP Id	TP Id TP/SEC/CA/NB-07-X-Y					
	Summary	mary Check that an CA responds to a certificate request with the list of permissions fully contained i			issions fully contained in		
			st signer certificate.				
	Reference	IEEE P1609.2/D12 [1], clauses 6.3.9 and 6.3.23,					
	Config Id CF01, CF02						
PIC	CS Selection		Indian -				
vith	(initiai c	onditions			
th th	with { the IUT in operational state the IUT is configured to provide certificates with permissions {PSID_A, PSID_B, PSID_C, PSID_D, PSID_E, PSID_F, PSID_G, PSID_H, PSID_I}						
			Expected	d behaviour			
	re that {						
W	/hen {	امانامیر میرانا	Cartificata Daguast ast to V	REQUEST			
			CertificateRequest set to X	_KEQUEST e.sec_data_exch_ca_scope.permi	ssions normissions list		
			ST_SIGNER		ออเอเเอ.คอเกแออเบเเอ_แอเ		
			_csr.type_specific_data. V_I	REQ_SCOPE			
	conta	ining permis	ssions.permissions_list	•			
		et to Y_PSIC	SSP_LIST_REQUEST				
}							
tr	nen {	la a valid Ca	wificata Dagnanaa aat ta V	DESDONSE			
			ertificateResponse set to X _ s[last].unsigned_certificate	RESPONSE			
		ining V_RE					
			rmissions.permissions_list				
			SIDSSP_LIST_RES				
}							
}							
	,	V 1		riants	ONET		
			REQUEST ENRREQ_TS	X_RESPO			
			UTHREQ_TS	MSG_AUTHI			
-	, ,	11100_F	COTTINE Q_TO	moc_AoTH	(OI _IO I		
			Va	riants			
Υ	PICS Sele	ection	Y_PSID_LIST_SIGNER	Y_PSIDSSP_LIST_REQUEST	Y_PSIDSSP_LIST_RES		
Α			{PSID_A}	{PSID_A}	{PSID_A}		
В			{PSID_A, PSID_B,	{PSID_A}	{PSID_A}		
			PSID_C, PSID_D}				
С			{PSID_A, PSID_B,	{PSID_A, PSID_B,	{PSID_A, PSID_B,		
_			PSID_C, PSID_D}	PSID_C, PSID_D}	PSID_C, PSID_D}		
D			{PSID_A, PSID_B, PSID_C, PSID_D,	{PSID_A, PSID_B, PSID_C, PSID_D,	{PSID_A, PSID_B, PSID_C, PSID_D,		
			PSID_E, PSID_F,	PSID_E, PSID_F,	PSID_E, PSID_F,		
			PSID_G, PSID_H}	PSID_G, PSID_H}	PSID_G, PSID_H}		
Е			{PSID_A, PSID_B,	{ PSID_C, PSID_D, PSID_E,	{PSID_A, PSID_B}		
			PSID_C, PSID_D}	PSID_F }			
F	PIC_Verify_Ps		{PSID_A}	{PSID_A, PSID_B,	{PSID_A}		
	thMoreThan	8Entries		PSID_C, PSID_D,			
				PSID_E, PSID_F,			
				PSID_G, PSID_H,			
	DIC Varies D	-id Λ κης: λΛ <i>l</i> :	(DCID A DCID D	PSID_I}	(DCID A)		
G	PIC_Verify_Ps thMoreThan		{PSID_A, PSID_B, PSID_C, PSID_D,	{PSID_A}	{PSID_A}		
	univioreman	ocnines	PSID_C, PSID_D, PSID_E, PSID_F,				
			PSID_G, PSID_H,				
			PSID_I}				
	I .			I	l .		

```
TP Id
                  TP/SEC/CA/NB-08-X-Y
   Summary
                  Check that an CA responds to a certificate request with the list of permissions set to the
                  intersection between requested permissions and CA certificate permissions.
   Reference
                  IEEE P1609.2/D12 [1], clauses 6.3.9 and 6.3.23
    Config Id
                  CF01, CF02
 PICS Selection
                                             Initial conditions
with {
   the IUT in operational state
   the IUT is configured with an CA certificate
      containing certificate.unsigned_certificate.sec_data_exch_ca_scope.permissions.permissions_list
         set to Y_PSID_LIST_CA_CERT
                                           Expected behaviour
ensure that {
   when {
      the IUT receives a valid CertificateRequest set to X_REQUEST
         containing unsigned_csr.type_specific_data.REQ_SCOPE
            containing permissions.permissions_list
                set to Y_PSIDSSP_LIST_REQUEST
   then {
      the IUT sends a valid CertificateResponse set to X_RESPONSE
         containing certificates[last].unsigned_certificate
            containing REQ_SCOPE
                containing permissions.permissions_list
                   set to Y_PSIDSSP_LIST_RES
   }
Note: Request signing certificate fully covers Y_PSIDSSP_LIST_REQUEST
                                                 Variants
                         X REQUEST
                                                                          X RESPONSE
                      MSG ENRREQ TS
                                                                       MSG ENRRSP IUT
   Α
   В
                     MSG_AUTHREQ_TS
                                                                      MSG_AUTHRSP_IUT
                                                 Variants
                            Y PSID LIST CA CERT
                                                      Y PSIDSSP LIST REQUEST
                                                                                     Y PSIDSSP LIST RES
        PICS Selection
                                   {PSID_A}
 Α
                                                                {PSID_A}
                                                                                            {PSID A}
 В
                               {PSID_A, PSID_B
                                                                {PSID_A}
                                                                                           {PSID A}
                                PSID_C, PSID_D}
                                                            (PSID A. PSID B.
                                                                                       (PSID A. PSID B.
 С
                               (PSID A. PSID B.
                                PSID C. PSID D
                                                            PSID C, PSID D
                                                                                       PSID C, PSID D
                                                            {PSID_A, PSID_B,
                               {PSID_A, PSID_B,
                                                                                       {PSID_A, PSID_B,
 D
                                                             PSID_C, PSID_D,
                                                                                       PSID C, PSID D,
                                PSID_C, PSID_D,
                                PSID_E, PSID_F,
                                                             PSID_E, PSID_F,
                                                                                       PSID_E, PSID_F,
                                                            PSID_G, PSID_H}
                                                                                       PSID_G, PSID_H}
                               PSID_G, PSID_H}
                               {PSID_A, PSID_B,
                                                       { PSID_C, PSID_D, PSID_E,
                                                                                       {PSID_A, PSID_B}
 Ε
                               PSID_C, PSID_D}
                                                                PSID_F }
 F
     PIC Verify PsidArray
                                                            {PSID A, PSID B,
                                                                                           {PSID A}
                                   {PSID_A}
      WithMoreThan8Entrie
                                                            PSID_C, PSID_D,
                                                             PSID_E, PSID_F,
               s
                                                             PSID_G, PSID_H,
                                                                 PSID_I}
                               {PSID_A, PSID_B,
 G
     PIC_Verify_PsidArray
                                                                {PSID_A}
                                                                                           {PSID_A}
      WithMoreThan8Entrie
                               PSID_C, PSID_D,
                                PSID_E, PSID_F,
                               PSID_G, PSID_H,
                                    PSID I
```

6.2.2.1.4 Expiration

TP ld	TP/SEC/CA/NB-09-X	TP/SEC/CA/NB-09-X			
Summary	Check that the CA accepts a valid ce	Check that the CA accepts a valid certificate request having specified start_validity time.			
Reference	IEEE P1609.2/D12 [1], clause 6.2.17				
Config Id	CF01, CF02				
PICS Selection	on				
	Initial co	nditions			
with {					
the IUT in ope	erational state				
}					
	Expected	behaviour			
ensure that {					
when {					
	eceives a CertificateRequest set to X_REQL	JEST			
	ning unsigned_csr				
CO	ntaining cf				
	indicating use_start_validity				
	and not indicating lifetime_is_duration				
CO	ntaining start_validity				
	set to 1 Jan 2010				
}					
then {					
	ends a CertificateResponse set to X_RESP	ONSE			
	ning certificates[last].unsigned_certificate				
val	valid from 1 Jan 2010				
}	}				
}					
	Varia				
Х	X_REQUEST	X_RESPONSE			
Α	MSG_ENRREQ_TS	MSG_ENRRSP_IUT			
В	MSG_AUTHREQ_TS	MSG_AUTHRSP_IUT			

TP	Pld TP/SEC/CA/NB-10-X				
Sum	mary Check that the CA accepts a valid	Check that the CA accepts a valid certificate request with lifetime set to 0.			
Refe	rence IEEE P1609.2/D12 [1], clause 6.3	IEEE P1609.2/D12 [1], clause 6.3.34			
	ETSI TS 102 941 [2] Table 1 : Co	ntents of ITS-S EnrolmentRequest message			
	ETSI TS 102 941 [2] Table 2 : Co	ntents of ITS-S AuthorizationRequest message			
Con	ig ld CF01,CF02				
PICS S	election				
	Initial	conditions			
with {					
the IUT	in operational state				
}					
	Expecte	ed behaviour			
ensure tha	t {				
when {					
the	IUT receives a CertificateRequest set to X_RE	QUEST			
	containing unsigned_csr				
	containing cf				
	indicating use_start_validity and lifetime	e_is_duration			
	containing lifetime				
	set to 0				
}					
then {					
the	IUT sends a valid CertificateResponse set to)	C_RESPONSE			
}					
}					
		ariants			
Х	X_REQUEST	X_RESPONSE			
Α	MSG_ENRREQ_TS	MSG_ENRRSP_IUT			
В	MSG AUTHREQ TS	MSG AUTHRSP IUT			

```
TP Id
                     TP/SEC/CA/NB-11-X
     Summary
                     Check that the CA accepts a valid certificate request with start_validity set to 0.
    Reference
                     IEEE P1609.2/D12 [1], clause 6.3.34
                     ETSI TS 102 941 [2] Table 1 : Contents of ITS-S EnrolmentRequest message
                     ETSI TS 102 941 [2] Table 2: Contents of ITS-S Authorization Request message
     Config Id
                     CF01, CF02
  PICS Selection
                                               Initial conditions
with {
  the IUT in operational state
                                             Expected behaviour
ensure that {
  when {
      the IUT receives a CertificateRequest set to X_REQUEST
         containing unsigned_csr
             containing cf
                indicating use_start_validity
                and not indicating lifetime_is_duration
             containing start_validity
                set to 0
   then {
      the IUT sends a valid CertificateResponse set to X_RESPONSE
  }
                                                   Variants
                         X_REQUEST
                                                                            X_RESPONSE
   Χ
                      MSG_ENRREQ_TS
                                                                          MSG_ENRRSP_IUT
   Α
                                                                         MSG_AUTHRSP_IUT
   В
                      MSG_AUTHREQ_TS
```

TP	Id TP/SEC/CA/NB-12-X					
Sum	mary Check that CA generates valid cer	Check that CA generates valid certificate response with a certificate containing the field				
	start_validity.					
Refer	rence IEEE P1609.2/D12 [1], clause 6.3.	2				
Conf	ig ld CF01, CF02					
PICS Se						
	Initial	conditions				
with {						
	in operational state					
	is configured to use start_validity flag					
the IUT	is configured not to use a lifetime_is_duration	flag				
}						
	Expecte	d behaviour				
ensure tha	t {					
when {						
the	IUT receives a valid CertificateRequest set to >	C_REQUEST				
}						
then {						
	IUT sends a CertificateResponse set to X_RES					
	containing certificate_chain[last].unsigned_cert	ficate				
	containing cf					
	indicating use_start_validity					
	and not indicating lifetime_is_duration					
	containing start_validity					
set to the timestamp < certificate_chain[last].unsigned_certificate.expiration						
}	}					
}]					
		riants				
X	X_REQUEST	X_RESPONSE				
Α	MSG_ENRREQ_TS	MSG_ENRRSP_IUT				

MSG_AUTHRSP_IUT

MSG_AUTHREQ_TS

В

6.2.2.1.5 Regions

	ld ld	TP/SEC/CA/NB-13-X-Y				
Sum	mary				gion which is fully containing in	
		the request region and in the signer region.				
Refe	rence	IEEE P1609.2/D12 [1], clauses 6.3.13, 6.3.15 and 5.5.3.3				
Con	fig ld	CF01, CF02				
PICS S	election					
			Initial co	nditions		
with {						
the IUT	in operation	nal state				
}						
			Expected I	oehaviour		
ensure tha	•					
when {		11-1 O 15 1 - D		SEQUEST		
		s a valid CertificateReq				
		er.certificate.unsigned_c	certificate.ANY	_SCOPE.region		
		GION_SIGNER	data ANIV CC	ODE series		
		ned_csr.type_specific_ GION_REQUEST	_data.ANY_SC	OPE.region		
	Selio I_KE	GION_REQUES I				
} then {						
	II IT conde a	valid CertificateRespon	nco cot to V B	ESDONSE		
		icates[last].unsigned_c				
	containing re		erillicate.Aivi_	_SCOPE.region		
	set to 'cii					
		ircular_region inside Y _	REGION RES	3		
}	oornaming o	irodiai_rogion iriolao i_				
3						
,			Varia	nts		
Х		X REQUEST			RESPONSE	
Α		MSG_ENRREQ_TS MSG_ENRRSP_IUT			ENRRSP_IUT	
В		MSG_AUTHREQ_TS MSG_AUTHRSP_IUT			AUTHRSP_IUT	
			Varia	ints		
Υ	Y_RE			ION_REQUEST	Y_REGION_RES	
Α		- SION_LARGE		ION_MEDIUM	REGION MEDIUM	
В		GION_LARGE			REGION LARGE	
C		ION_MEDIUM		GION_SMALL	REGION_SMALL	
		NEGION_OWNER NEGION_OWNER				

6.2.2.2 Exceptional Behavior

6.2.2.2.1 Invalid Message Fields

тг	Id TP/SEC/CA/EB-01-X			
Sum	Check that CA discards certificate requests if the message content type is different than			
Dofo	"encrypted".			
	ence IEEE P1609.2/D12 [1], clause 6.2.1			
	ig Id CF01, CF02			
PICS S	election			
111 6	Initial conditions			
with {	in an evaluated			
the IU	in operational state			
}	Expected behaviour			
anaura tha	•			
ensure that when {	·1			
	IUT receives a 1609Dot2Data structure			
lile	containing type			
	set to X_INVALID_CONTENT_TYPE			
}	Set to A_INVALID_GONTENT_TITLE			
then {				
	IUT discards the received message			
}	To Fidebalde the 1999/99 Incomes			
}				
,	Variants			
Х	X_INVALID_CONTENT_TYPE			
Α	unsecured (0)			
В	signed(1)			
C	certificate_request(3)			
D	certificate_response(4)			
E	anonymous_certificate_response(5)			
F	certificate_request_error(6)			
G	crl_request(7)			
H	crl(8)			
i	signed_partial_payload(9)			
J	signed_partial_payload(10)			
K	signed_wsa(11)			
L	certificate_response_acknowledgment (12)			
M	ANY_VALUE(128)			
	///41_///FOE(120)			

```
TP Id
                     TP/SEC/CA/EB-02-X
     Summary
                     Check that CA discards certificate requests if the protocol_version is not 2.
     Reference
                     IEEE P1609.2/D12 [1], clause 6.2.1.1
     Config Id
                     CF01, CF02
  PICS Selection
                                              Initial conditions
with {
   the IUT in operational state
                                            Expected behaviour
ensure that {
   when {
      the IUT receives a 1609Dot2Data structure
         containing protocol_version
            set to X_INVALID_VERSION_NUMBER
   then {
      the IUT discards the received message
   }
                                                  Variants
                                           X_INVALID_VERSION_NUMBER
   #
   Α
                                                           0
   В
                                                           1
   С
                                                           3
   D
                                                          255
```

TP	Id TP/SEC/CA/EB-03-X				
Sum	mary Check that CA discards messages others than certificate request.				
Refer	rence	L 3'			
Conf		CF01, CF02			
PICS Se	election				
		Initial conditions			
with {					
the IUT	in operation	nal state			
}					
		Expected behaviour			
ensure tha	t {				
when {		(000D (0D)			
		s a 1609Dot2Data structure			
1		ncrypted_data			
		ng encrypted_data (ToBeEncrypted data structure)			
		aining type et to X INVALID_CONTENT_TYPE			
1	30	EN TO A_INVALID_CONTENT_TITE			
then {					
•	ILIT discards	s the received message			
}	10 T diocard	s the reserved mesodage			
}	}				
		Variants			
Х		X_INVALID_CONTENT_TYPE			
Α		unsecured (0)			
В		signed(1)			
С		encrypted(2)			
D	certificate_response(4)				
E	anonymous_certificate_response(5)				
F	certificate_request_error(6)				
G	crl_request(7)				
Н	crl(8)				
I	signed_partial_payload(9)				
J	signed_external_payload(10)				
K		signed_wsa(11)			
L		certificate_response_acknowledgment (12)			
M		ANY_VALUE(128)			

TP	' ld	d TP/SEC/CA/EB-04-X-Y			
Sum	mary	Check that CA discards certificate request if the certificate is not an explicit one.			
Refe	rence	IEEE P1609.2/D12 [1], clause 6.3.1			
	fig ld	CF01, CF02			
PICS S	election				
		Initial condition	ns		
with {					
the IUT	in operation	nal state			
}					
		Expected behave	iour		
ensure tha	•				
when {					
		s a CertificateRequest set to X_REQUEST			
		nsigned_csr.version_and_type			
	set to Y_	INVALID_CERT_VERSION_AND_TYPE			
}					
then {		0 45 4 D 45 44 V DEODO			
		CertificateRequestError set to X_RESPON	ISE		
	containing re				
,	set to 've	erification_failure'			
}					
}		Varianta			
V		Variants	V DECDONOE		
X		X_REQUEST	X_RESPONSE		
A		MSG_ENRREQ_TS	MSG_ENRERR_IUT		
В	MSG_AUTHREQ_TS MSG_AUTHERR_IUT				
Varianta					
	Variants VARIABLE CERT VERSION AND TYPE				
Y	Y_INVALID_CERT_VERSION_AND_TYPE				
A	0				
В	1				
С	3				
D	255				

	TD/050/04/5D 05 V				
TP					
Sum	Imary Check that CA generates a certificate request error with valid fields when it receives the request				
	with cryptographically invalid signature.				
Refe	ence IEEE P1609.2/D12 [1]	, clause 6.2.17			
Conf	ig ld CF01, CF02				
PICS S	election				
	·	Initial conditions			
with {					
the IUT	in operational state				
}					
		Expected behaviour			
ensure tha	: {				
when {					
the	IUT receives a CertificateRequest s	set to X_REQUEST			
	containing a criptogtaphicaly invalid				
}		·			
then {					
the	IUT sends a CertificateRequestErro	or set to X_RESPONSE			
	containing reason				
	set to 'verification failure'				
}	}				
}	,				
•	Variants				
Х	X_REQUEST	X_RESPONSE			
Α	MSG_ENRREQ_T	TS MSG_ENRERR_IUT			
В	MSG_AUTHREQ_	TS MSG_AUTHERR_IUT			

6.2.2.2.2 Invalid Certificate or Certificate Chain

	1			
TP ld	TP/SEC/CA/EB-06-X			
Summary				
	certificate.			
Reference	IEEE P1609.2/D12 [1], clause 5.5.3.3			
Config Id	CF01, CF02			
PICS Selection				
	Initial conditio	ns		
with {				
the IUT in operation	onal state			
}				
	Expected behave	iour		
ensure that {				
when {				
	es a CertificateRequest set to X_REQUEST			
containing sig				
containing				
	certificate_chain'			
•	certificates[last]			
contair	ing cryptographically invalid signature			
}				
then {				
	a valid CertificateRequestError set to X_RES	SPONSE		
	containing reason			
set to '	set to 'verification_failure'			
}	}			
}				
	Variants			
Х	X_REQUEST	X_RESPONSE		
Α	MSG_ENRREQ_TS	MSG_ENRERR_IUT		
В	MSG_AUTHREQ_TS	MSG_AUTHERR_IUT		

TP	Id TP/SEC/C	A/EB-07-X			
Sum	nmary Check that an CA discards an certificate request containing a signer containing an invalid				
		(unknown root certificate).			
Refer	ference IEEE P1609.2/D12 [1], clauses 5.6.1.2 and 6.3.37				
Conf	ig Id CF01, CF0	2			
PICS Se	election				
		Initial condi	tions		
with {					
the IUT	in operational state				
}					
		Expected beh	aviour		
ensure that	t {				
when {					
		teRequest set to X_REQUES	ST		
	taining signer				
	containing type				
	set to 'certificate_ch				
	containing certificates[0				
	set to an unknown r	oot certificate			
}	}				
then {					
		ficateRequestError set to X_F	ESPONSE		
	containing reason				
	set to 'verification_failure'				
}	}				
}					
L		Variants			
X		REQUEST	X_RESPONSE		
A		ENRREQ_TS	MSG_ENRERR_IUT		
В	MSG_A	UTHREQ_TS	MSG_AUTHERR_IUT		

TP	ld	ld TP/SEC/CA/EB-08-X			
Sum	mary				
		certificate chain (expired root certificate).			
Refe	ence	IEEE P1609.2/D12 [1], clauses 5.5.3.3 and	1 6.3.37		
Con	ig ld	CF01, CF02			
PICS S	election				
		Initial condition	ns		
with {					
the IUT	in operation	nal state			
}					
		Expected behave	riour		
ensure tha	t {				
when {					
		s a CertificateRequest set to X_REQUEST			
	taining signe				
	containing ty				
		ertificate_chain'			
		ertificates[0] (root certificate)			
	containir	ng unsigned_certificate.expiration < CLT			
}					
then {					
		valid CertificateRequestError set to X_RE	SPONSE		
	containing reason				
	set to 'verification_failure'				
}	}				
}					
Х		X REQUEST	X RESPONSE		
A		MSG ENRREQ TS	MSG ENRERR IUT		
В		MSG AUTHREQ TS	MSG AUTHERR IUT		

TP/SEC/CA/EB-09-X				
Immary Check that an CA discards an certificate request containing a signer containing an invalid				
certificate chain (cryptographically invalid root certificate).				
CF01, CF02				
Initial condition	ons			
nal state				
Expected behave	riour			
<u> </u>				
s a CertificateRequest set to X_REQUEST				
ng invalid signature				
ELO CE LO DE LA VIDE	DDONOE			
•	SPUNSE			
containing reason				
Set to Verification_failure				
) }				
Variants				
X_REQUEST	X_RESPONSE			
X_REQUEST MSG_ENRREQ_TS	X_RESPONSE MSG_ENRERR_IUT			
	Check that an CA discards an certificate recertificate chain (cryptographically invalid recertificate chain (cryptographically invalid recertificate chain (cryptographically invalid received by the condition of the condition of the condition of the cryptographic condition of the cryptographic cryptographic condition of the cryptographic cryptographic condition of the cryptographic cryptograp			

TP Id	TP/SEC/CA/EB-10-X				
Summa					
	certificate chain (missing root certificate).				
Referen	ce IEEE P1609.2/D12 [1], clauses 5.6.1.2 a	nd 6.3.37			
Config	ld CF01, CF02				
PICS Selec	ction				
	Initial condit	ions			
with {					
the IUT in	operational state				
}					
	Expected beh	aviour			
ensure that {					
when {		_			
	Γreceives a CertificateRequest set to X_REQUES	Т			
	ning signer				
cor	ntaining type				
	set to 'certificate_chain'				
COI	ntaining certificates not containing a root certificate (CERT_ROOT)				
1	not containing a root certificate (CERT_ROOT)				
then {					
	Γ sends a valid CertificateRequestError set to X_R	ESPONSE			
	ntaining reason	201 01102			
	set to 'verification_failure'				
}	}				
}	}				
	Variants				
Х	X_REQUEST	X_RESPONSE			
Α	MSG_ENRREQ_TS	MSG_ENRERR_IUT			
В	MSG_AUTHREQ_TS	MSG_AUTHERR_IUT			

TF	P Id TP/SEC/CA/EB-11-X			
Sum	mary Check that an CA discards an certificate request containing an unknown signer.			
Refe	rence IEEE P1609.2/D12 [1], clause 5.5.3.3			
Con	fig ld CF02			
PICS S	election			
	Initial con	ditions		
with {				
the IU	T in operational state			
}				
	Expected b	ehaviour		
ensure tha				
when {	L			
	IUT receives a CertificateRequest set to X_REQU	EST		
cor	ntaining signer			
	containing type set to 'certificate'			
	containing certificate			
	set to unknown certificate (see note)			
}				
then {				
the	IUT sends a valid CertificateRequestError set to X	_RESPONSE		
	containing reason			
,	set to 'csr_cert_revoked'			
}				
) NOTE:	A contition to the state of a contition to a little state of	ada ta a linaum turat aradi ar		
NOTE:	A certificate that does not belong to a chain that le			
V	Varia			
X	X_REQUEST	X_RESPONSE		
A	MSG_ENRREQ_TS	MSG_ENRERR_IUT		
В	MSG_AUTHREQ_TS	MSG AUTHERR IUT		

TP I	d TP/SEC/CA/EB-12-X				
Summ	ary Check that an CA discards an certificate	Check that an CA discards an certificate request containing a revoked signer certificate.			
Refere	nce IEEE P1609.2/D12 [1], clause 6.3.37				
Config	g ld CF01, CF02				
PICS Sele	ection				
	Initial condit	ions			
with {					
the IUT i	n operational state				
}					
	Expected beh	aviour			
ensure that	[
when {					
	JT receives a CertificateRequest set to X_REQUES	T			
conta	iining signer				
CC	ontaining type				
	set to 'certificate'				
CC	ontaining certificate				
	set to revoked certificate				
}					
then {					
	the IUT sends a valid CertificateRequestError set to X_RESPONSE				
CC	containing reason				
_	set to 'csr_cert_revoked'				
}	}				
}	<u>}</u>				
	Variants				
X	X_REQUEST	X_RESPONSE			
A	MSG_ENRREQ_TS	MSG_ENRERR_IUT			
В	MSG_AUTHREQ_TS	MSG_AUTHERR_IUT			

6.2.2.2.3 Invalid Certificate Fields

TF	ld	d TP/SEC/CA/EB-13-X-Y			
Sum	mary	Check that an CA discards an certificate request with certificate content flags other than			
		'use_start_validity' or 'lifetime_is_duration'.			
	rence	ETSI TS 102 867 [3], cla	ause 5.1.2.2, IEEE P1609.2/D12	[1], clauses 6.3.2 and 6.3.34	
	fig ld	CF01, CF02			
PICS S	election				
			Initial conditions		
with {					
the IUT	in operation	nal state			
}					
			Expected behaviour		
ensure tha	t {				
when {	U.T	- O	-t-t- V DECUEOT		
		s a CertificateRequest se	et to X_REQUEST		
		nsigned_csr.cf INVALID_FLAGS			
1	sel to 1_	INVALID_FLAGS			
} then {					
	II IT sands a	valid CartificateReques	tError set to X_RESPONSE		
	containing re		LITO Set to A_NEST ONSE		
		quest_denied'			
}	0011010	quoot_uoriiou			
}					
1			Variants		
Х		X_REQUEST		X RESPONSE	
Α		MSG ENRREQ TS	3	MSG ENRERR IUT	
В		MSG AUTHREQ T	S	MSG_AUTHERR_IUT	
			Variants		
Y_INVALID_FLAGS					
Υ	use_s	start_validity (0)	lifetime_is_duration(1)	encryption_key (2)	
Α		Yes Yes		Yes	
В		No	Yes	Yes	
С		Yes No		Yes	
D		No No Yes			

TP	ld	TP/SEC/CA/EB-14-X			
Sumr	mary	Check that an CA discards an certificate request signed with expired credentials.			
Refer	ence	IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 6.3.37			
Conf	ig ld	CF01, CF02			
PICS Se	election				
		Initial conditio	ns		
with {					
the IUT	in operation	nal state			
}					
		Expected behave	iour		
ensure that	t {				
when {		O CE I D I I V DECUECT			
		s a CertificateRequest set to X_REQUEST			
	taining signe				
	containing ty				
		ertificate_chain'			
		ertificates[last]			
,	containin	g unsigned_certificate.expiration < CLT			
} +h(
then {	II IT condo o	valid CertificateRequestError set to X_RES	PROMPE		
			SPONSE		
	containing reason set to 'verification failure'				
ı	Set to verification_tailure				
}					
Variants					
Х		X_REQUEST	X_RESPONSE		
Α		MSG_ENRREQ_TS	MSG_ENRERR_IUT		
В					

```
TP Id
                     TP/SEC/CA/EB-15-X
     Summary
                     Check that CA generates certificate request error with valid fields and with signature of various
                     public key types.
                     Check that CA calculate request hash using compressed representation of all public keys.
    Reference
                     IEEE P1609.2/D12 [1], clause 6.2.17
     Config Id
                     CF01, CF02
  PICS Selection
                                              Initial conditions
with {
  the IUT in operational state
  the IUT is configured to use signature of type Y_PK_TYPE_SIGNATURE
                                            Expected behaviour
ensure that {
  when {
      the IUT receives a CertificateRequest set to X_REQUEST
         containing a criptogtaphicaly invalid signature
         containing unsigned_csr.verification_key.public_key.type (V_PK_REQ_VK)
            set to 'uncompressed'
         containing unsigned_csr.response_encryption_key.public_key.type (V_PK_REQ_REK)
            set to 'uncompressed'
  then {
      the IUT sends a CertificateRequestError set to X_RESPONSE
         containing reason
            set to 'verification_failure'
         containing request_hash
            set to the hash calculated using compressed representation of the V PK REQ VK and
                V_PK_REQ_REK
         containing signature.ecdsa_signature
            containing R.type
                set to Y PK TYPE SIGNATURE
  }
                                                  Variants
                            X REQUEST
                                                                              X RESPONSE
                         MSG_ENRREQ_TS
                                                                           MSG_ENRERR_IUT
   Α
                                                                           MSG_AUTHERR_IUT
   В
                        MSG_AUTHREQ_TS
                                                  Variants
 Υ
                                             Y_PK_TYPE_SIGNATURE
 Α
                                               compressed_lsb_y_0/1
 В
                                                 x_coordinate_only
 С
                                                   uncompressed
```

6.2.2.2.4 Invalid Permissions

TE	P ld	TP/SEC/CA/EB-16-X-Y	1	
	Immary Check that an CA discards an certificate request with an invalid PsidArray.type.			
	erence ETSI TS 102 867 [3], clause 5.1.2.2, IEEE P1609.2/D12 [1], clause 6.3.7			
	fig ld	CF01, CF02	1 1000.E/B 12 [1], olddod 0.0.11	
	election			
		Initial conditio	ns	
with {				
the IU7	Γ in operatio	nal state		
}				
		Expected behave	iour	
ensure tha	•			
when {		a a Cartificata Paguast set to V PEQUEST		
		s a CertificateRequest set to X_REQUEST gned_csr.type_specific_data.ANY_SCOPE		
		permissions.type		
		INVALID_ARRAY_TYPE		
}	30110 1	_INVALID_AIXIA1_111 E		
then {				
the	IUT sends a	a valid CertificateRequestError set to X_RES	SPONSE	
	containing r			
	set to 're	equest_denied'		
}				
}				
		Variants		
Х		X_REQUEST	X_RESPONSE	
A		MSG_ENRREQ_TS	MSG_ENRERR_IUT	
В		MSG_AUTHREQ_TS	MSG_AUTHERR_IUT	
		VI		
Υ		Variants Y_INVALID_ARI	DAY TYPE	
A		from_issu		
В		ANY OTHER		
		ANI OTTILI	(120)	

	TP ld	TP/SEC/CA/EB-17-X			
;	Summary	Check that an CA discare	ds an certificate request signed by	the certificate with the	
	permissions list which is not a superset of requested permissions list.				
	Reference	IEEE P1609.2/D12 [1], c	lause 5.5.3.3		
	Config Id	CF01, CF02			
PIC	S Selection				
ا مادند،		Initia	l conditions		
with {	T in operational:	state			
	i iii operationar.	State			
		Expec	ted behaviour		
ensure tha	at {	•			
when {	{				
the	IUT receives a	CertificateRequest set to X_R			
COI			.ANY_SCOPE.permissions.permis	ssions_list	
	set to X_PSID_				
COI	ntaining unsigne	d_csr.type_specific_data.AN	<pre>/_SCOPE.permissions.permission</pre>	s_list	
,	set to X_PS	ID_LIST_REQ			
}					
then {	. II IT aanda a wa	lid Contitionto Dominate unos an	tte V DESDONSE		
tne		lid CertificateRequestError se	T TO X_RESPONSE		
	containing reas				
1	set to 'reque	est_denied			
}					
		,	Variants		
Х		X_REQUEST	X_R	ESPONSE	
Α		MSG_ENRREQ_TS		ENRERR_IUT	
В		MSG_AUTHREQ_TS	MSG_A	UTHERR_IUT	
			Variants	V 2012 1107 250	
Υ	PI	CS Selection	X_PSID_LIST_SIGNER	X_PSID_LIST_REQ	
Α			{PSID_B}	{PSID_A}	
_			{ PSID_B, PSID_C, PSID_D,	(0015 4)	
В			PSID_E, PSID_F, PSID_G,	{PSID_A}	
			PSID_H, PSID_I}		
	{ PSID_B, PSID_C, PSID_D ,				
				(DOID A)	
	PIC_Verify_Psid/	ArrayWithMoreThan8Entries	PSID_E, PSID_F, PSID_G,	{PSID_A}	
	PIC_Verify_Psid/	ArrayWithMoreThan8Entries		, ,	
			PSID_E, PSID_F, PSID_G, PSID_H, PSID_I, PSID_J}	{PSID_B, PSID_C, PSID_D	
		ArrayWithMoreThan8Entries ArrayWithMoreThan8Entries	PSID_E, PSID_F, PSID_G,	{PSID_B, PSID_C, PSID_D, PSID_E, PSID_F, PSID_G,	
			PSID_E, PSID_F, PSID_G, PSID_H, PSID_I, PSID_J}	{PSID_B, PSID_C, PSID_D, PSID_E, PSID_F, PSID_G, PSID_H, PSID_I}	
D F			PSID_E, PSID_F, PSID_G, PSID_H, PSID_I, PSID_J} {PSID_A}	{PSID_B, PSID_C, PSID_D, PSID_E, PSID_F, PSID_G, PSID_H, PSID_I} {PSID_B, PSID_C, PSID_D	
			PSID_E, PSID_F, PSID_G, PSID_H, PSID_I, PSID_J}	{PSID_B, PSID_C, PSID_D, PSID_E, PSID_F, PSID_G, PSID_H, PSID_I} {PSID_B, PSID_C, PSID_D, PSID_E, PSID_F, PSID_G,	
D F			PSID_E, PSID_F, PSID_G, PSID_H, PSID_I, PSID_J} {PSID_A} {PSID_A}	{PSID_B, PSID_C, PSID_D, PSID_E, PSID_F, PSID_G, PSID_H, PSID_I} {PSID_B, PSID_C, PSID_D, PSID_E, PSID_F, PSID_G, PSID_H, PSID_I, PSID_J}	
D F			PSID_E, PSID_F, PSID_G, PSID_H, PSID_I, PSID_J} {PSID_A}	{PSID_B, PSID_C, PSID_D, PSID_E, PSID_F, PSID_G, PSID_H, PSID_I} {PSID_B, PSID_C, PSID_D, PSID_E, PSID_F, PSID_G,	

```
TP/SEC/CA/EB-18-X
           TP Id
        Summary
                             Check that an CA discards an certificate request if it has duplicated PSIDs.
        Reference
                             IEEE P1609.2/D12 [1], clause 6.3.9
         Config Id
                             CF01, CF02
      PICS Selection
                                               Initial conditions
with {
   the IUT in operational state
   the IUT containing CA_CERT
      containing unsigned_certificate.scope.permissions.permissions_list(V_PERM_LIST)
                                             Expected behaviour
ensure that {
   when {
      the IUT receives a CertificateRequest set to X_REQUEST
         containing unsigned_csr.type_specific_data.scope
             containing permissions.permissions_list
                set to array[2]{
    containing V_PERM_LIST[0]
                    containing V_PERM_LIST[0]
                }
   }
   then {
      the IUT sends a valid CertificateRequestError set to X_RESPONSE
         containing reason
             set to 'verification_failure'
   }
                                                   Variants
                            X REQUEST
                                                                               X_RESPONSE
                                                                             MSG_ENRERR_IUT
                         MSG_ENRREQ_TS
                        MSG_AUTHREQ_TS
                                                                            MSG_AUTHERR_IUT
   В
```

6.2.2.2.5 Invalid Regions

Check that an CA discards a certificate request signed by the certificate containing a scope with a circular region (REGION_SIGNER) and an unsigned csr with a circular region (REGION_REQUEST) that is not fully contained in the signer region. Reference	TP	⁾ Id	Id TP/SEC/CA/EB-19-X-Y				
Reference IEEE P1609.2/D12[1], clause 5.5.3.3	Sum	mary					
Reference IEEE P1609.2/D12 [1], clause 5.5.3.3 Config Id CF01, CF02 Initial conditions			a circular region (REGION_SIGNER) and an unsigned csr with a circular region				
Config Id CF01, CF02 PICS Selection Initial conditions with { the IUT in operational state } } Expected behaviour ensure that { when { the IUT receives a CertificateRequest set to X_REQUEST containing signer containing type set to 'certificate' containing certificate.unsigned_certificate.ANY_SCOPE containing region set to Y_REGION_SIGNER containing region set to Y_REGION_REQUEST } } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing region set to Y_REGION_REQUEST } } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } } Variants X							
## PICS Selection Initial conditions with {	Refei	rence	IEEE P1609.2/D12 [1], clause 5.5.3.3				
with {	Conf	fig ld	CF01, CF02				
with { the IUT in operational state } Expected behaviour ensure that { when { the IUT receives a CertificateRequest set to X_REQUEST containing signer containing signer containing certificate unsigned_certificate.ANY_SCOPE containing region set to Y_REGION_SIGNER containing unsigned_csr.type_specific_data.ANY_SCOPE containing region set to Y_REGION_REQUEST } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } } X	PICS S	election					
the IUT in operational state Expected behaviour			Initial condition	ons			
Expected behaviour ensure that { when { the IUT receives a CertificateRequest set to X_REQUEST containing signer containing signer containing type set to 'certificate' containing region set to Y_REGION_SIGNER containing unsigned_cert.type_specific_data.ANY_SCOPE containing unsigned_cert.type_specific_data.ANY_SCOPE containing region set to Y_REGION_REQUEST } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } X							
ensure that { when { the IUT receives a CertificateRequest set to X_REQUEST containing signer containing type set to 'certificate' containing certificate.unsigned_certificate.ANY_SCOPE containing region set to Y_REGION_SIGNER containing unsigned_csr.type_specific_data.ANY_SCOPE containing region set to Y_REGION_REQUEST } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } } Variants X	the IUT	in operation	nal state				
ensure that { when { the IUT receives a CertificateRequest set to X_REQUEST containing signer containing type set to 'certificate' containing certificate.unsigned_certificate.ANY_SCOPE containing region set to Y_REGION_SIGNER containing unsigned_csr.type_specific_data.ANY_SCOPE containing region set to Y_REGION_REQUEST } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } } Variants X	}						
when { the IUT receives a CertificateRequest set to X_REQUEST containing signer containing type set to 'certificate' containing certificate.unsigned_certificate.ANY_SCOPE containing region set to Y_REGION_SIGNER containing unsigned_csr.type_specific_data.ANY_SCOPE containing region set to Y_REGION_REQUEST } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } } Variants X			Expected behave	viour			
the IUT receives a CertificateRequest set to X_REQUEST containing signer containing type set to 'certificate' containing certificate.unsigned_certificate.ANY_SCOPE containing region set to Y_REGION_SIGNER containing unsigned_csr.type_specific_data.ANY_SCOPE containing region set to Y_REGION_REQUEST } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } Variants X							
containing signer containing type set to 'certificate' containing certificate unsigned_certificate.ANY_SCOPE containing region set to Y_REGION_SIGNER containing unsigned_csr.type_specific_data.ANY_SCOPE containing region set to Y_REGION_REQUEST } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } } Variants X			0 - 111 - 1 D - 1 - 1 - 1 - 1 - 1 - 1 - 1				
containing type set to 'certificate' containing certificate.unsigned_certificate.ANY_SCOPE containing region set to Y_REGION_SIGNER containing unsigned_csr.type_specific_data.ANY_SCOPE containing region set to Y_REGION_REQUEST } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } } Variants X							
set to containing certificate unsigned_certificate.ANY_SCOPE containing region set to Y_REGION_SIGNER containing unsigned_csr.type_specific_data.ANY_SCOPE containing region set to Y_REGION_REQUEST } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } } Variants X							
containing certificate.unsigned_certificate.ANY_SCOPE							
containing region set to Y_REGION_SIGNER containing unsigned_csr.type_specific_data.ANY_SCOPE containing region set to Y_REGION_REQUEST } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } } Variants X				=			
set to Y_REGION_SIGNER containing unsigned_csr.type_specific_data.ANY_SCOPE containing region set to Y_REGION_REQUEST } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } } Variants X				=			
containing unsigned_csr.type_specific_data.ANY_SCOPE							
containing region set to Y_REGION_REQUEST } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } } Variants X	con						
set to Y_REGION_REQUEST } then { the IUT sends a valid CertificateRequestError set to X_RESPONSE							
then { the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } Variants X							
then { the IUT sends a valid CertificateRequestError set to X_RESPONSE	}	001101_					
the IUT sends a valid CertificateRequestError set to X_RESPONSE containing reason set to 'request_denied' } Variants X	then {						
containing reason set to 'request_denied' } Variants X		IUT sends a	a valid CertificateRequestError set to X_RE	SPONSE			
Set to Trequest_denied Set to Trequest_denied							
Variants X X_REQUEST X_RESPONSE							
Variants X X_REQUEST X_RESPONSE	}		·				
X X_REQUEST X_RESPONSE A MSG_ENRREQ_TS MSG_ENRERR_IUT B MSG_AUTHREQ_TS MSG_AUTHERR_IUT Variants Y Y_REGION_SIGNER Y_REGION_REQUEST A REGION_SMALL REGION_OUTSIDE B REGION_SMALL REGION_LARGE	}						
A MSG_ENRREQ_TS MSG_ENRERR_IUT B MSG_AUTHREQ_TS MSG_AUTHERR_IUT Variants Y Y_REGION_SIGNER Y_REGION_REQUEST A REGION_SMALL REGION_OUTSIDE B REGION_SMALL REGION_LARGE							
B MSG_AUTHREQ_TS MSG_AUTHERR_IUT Variants Y Y_REGION_SIGNER Y_REGION_REQUEST A REGION_SMALL REGION_OUTSIDE B REGION_SMALL REGION_LARGE	Х						
Variants Y Y_REGION_SIGNER Y_REGION_REQUEST A REGION_SMALL REGION_OUTSIDE B REGION_SMALL REGION_LARGE	Α						
Y Y_REGION_SIGNER Y_REGION_REQUEST A REGION_SMALL REGION_OUTSIDE B REGION_SMALL REGION_LARGE	В		MSG_AUTHREQ_TS	MSG_AUTHERR_IUT			
Y Y_REGION_SIGNER Y_REGION_REQUEST A REGION_SMALL REGION_OUTSIDE B REGION_SMALL REGION_LARGE							
A REGION_SMALL REGION_OUTSIDE B REGION_SMALL REGION_LARGE		Variants					
B REGION_SMALL REGION_LARGE	Υ						
	A						
C REGION SMALL REGION INTERSECTING							
	С		REGION_SMALL	REGION_INTERSECTING			

6.2.2.2.6 Expiration

TP ld	TP/SEC/CA/EB-20-X					
Summary	mary Check that an CA discards a certificate request containing an expired signer certificate.					
Reference						
Config Id	CF01, CF02					
PICS Selection						
	Initial conditions					
with {						
the IUT in op	perational state					
}						
	Expected bel	naviour				
ensure that {						
when {	and the Continue to Descript out to V. DEOLIE					
	eceives a CertificateRequest set to X_REQUES	ol .				
containin						
	ining type					
	et to 'certificate'					
	ining certificate.unsigned_certificate					
CO	ontaining expiration					
	set to CLT – '1Y'					
CO	ontaining lifetime					
	set to '1Y'					
}						
then {						
the IUT s	ends a CertificateRequestError set to X_RESP	ONSE				
	ining reason					
se	set to 'csr_cert_expired'					
}	}					
}						
	Variant	-				
Χ	X_REQUEST	X_RESPONSE				
Α	MSG_ENRREQ_TS	MSG_ENRERR_IUT				
В	MSG_AUTHREQ_TS	MSG_AUTHERR_IUT				

TP	TP Id TP/SEC/CA/EB-21-X-Y					
		Check that an CA discards a certificate request with invalid expiration time.				
		09.2/D12 [1], clauses 6.3.2, 6.3				
	fig ld CF01, CF			[-],		
	election	-				
	,	Initial conditi	ons			
with {						
the IUT	in operational state					
}						
		Expected beha	viour			
ensure tha						
when {						
		ateRequest set to X_REQUEST				
	taining signer.certificat	e.unsigned_certificate				
	containing expiration set to Y_EXP_SIGN	JED				
	containing lifetime	VER.				
	set to Y_LT_SIGNE	R				
con	taining unsigned_csr					
	containing expiration					
	set to Y_EXP_REQ	UEST				
	containing lifetime					
	set to Y_LT_REQU	EST				
}						
then{						
		ficateRequestError set to X_RE	SPONSE			
	containing reason					
,	set to 'request_den	ied'				
}						
}		Variants				
Χ	Х	REQUEST	X RESP	ONSE		
Α		ENRREQ TS	MSG ENRI			
В		AUTHREQ TS	MSG AUTH			
	<u></u>	-		_		
		Variants				
Υ	Y_EXP_SIGNER	Y_LT_SIGNER	Y_EXP_REQUEST	Y_EXP_REQUEST		
Α	CLT+1Y	1Y	CLT+2Y	1M		
В	CLT+1Y	1Y	CLT+2Y	1Y		
С	CLT+1Y	1Y	CLT+2Y	2Y		
D	CLT+2Y	1M	CLT+1Y	1M		
E	CLT+2Y 1Y CLT+1Y 1M					
F	CLT+3Y	2Y	CLT+2Y	2Y		

6.2.3 Enrolment Authority

6.2.3.1 Normal Behavior

TP Id	TP/SEC/EA/ENR/NB-01					
Summary	Check that the EA accepts a valid self-signed enrolment request having correct fields and					
	values.					
Reference	Reference IEEE P1609.2/D12 [1], clause 6.2.4					
Config Id	Config Id CF01					
PICS Selection	PIC_Generate_SelfSigned					
	Initial conditions					
with {						
the IUT in operation	nal state					
}						
	Expected behaviour					
ensure that {						
when {						
	s a valid CertificateRequest set to MSG_ENRREQ_TS					
containing s						
containir	0 71					
set to	set to 'self'					
}	}					
then {	- W					
the IUT sends a	a CertificateResponse set to MSG_ENRRSP_IUT					
}						
}						

6.2.3.2 Exceptional Behavior

	TP ld	TP/SEC/EA/ENR/EB-02-X				
	Summary	Check that an EA discards a enrolment request signed by a signer_id with type set to an				
		other value than 'self', 'certificate' or ' certificate_chain'.				
	Reference ETSI TS 102 941 [2], clause 6.2.2.3					
	Config Id	CF01, CF02				
P	ICS Selection					
		Initial conditions				
with {						
the	IUT in operational stat	te				
}						
		Expected behaviour				
ensure	that {					
whe						
1	the IUT receives a Ce	rtificateRequest set to MSG_ENRREQ_TS				
	containing signer					
	containing type	;				
	set to X_IN	VALID_SUBJECT_TYPE				
}						
ther						
1	the IUT sends a valid	CertificateRequestError set to X_RESPONSE				
	containing reason					
	set to 'request_	_denied'				
}						
}						
	Variants					
X	PICS	X_INVALID_SUBJECT_TYPE				
Α	Not PIC_Verify_					
В		certificate_digest_with_ecdsap224(1)				
С		certificate_digest_with_ecdsap256(2)				
D		certificate_digest_with_other_algorithm(5)				
Е	ANY OTHER (128)					

Т	TP Id TP/SEC/EA/ENR/EB-03-X					
Sui	mmary	nmary Check that an EA discards an enrolment request with a subject type other than				
	'sec_data_exch_csr'.					
Ref	erence	rence IEEE P1609.2/D12 [1], 5.5.3.3, ETSI TS 102 867 [3], clause 5.1.2.1, IEEE P1609.2/D12 [1],				
		clause 6.3.7				
	nfig ld	CF01				
PICS	Selection					
		Initial con	ditions			
with { the IU }	JT in operation	onal state				
,		Expected be	ehaviour en la companyation de l			
ensure th	nat {	•				
when	{					
th		es a CertificateRequest set to MSG_ENF	RREQ_TS			
		unsigned_csr				
		ing subject_type				
		to X_INVALID_SUBJECT_TYPE				
		ing type_specific_data				
,	con	taining X_INVALID_SCOPE				
} then {	r					
		a valid CertificateRequestError set to X	RESPONSE			
"'	containing		NEOF ONCE			
		request_denied'				
}	551.15					
}						
		Variar				
#		INVALID_SUBJECT_TYPE	X_INVALID_SCOPE			
Α		_data_exch_anonymous (0)	AnonymousScope			
В		_exch_identified_not_localized (1)	IdentifiedNotLocalizedScope			
С	sec_dat	ta_exch_identified _localized (2)	IdentifiedLocalizedScope			
D	wsa (4) WsaCaScope					
E	wsa_csr (5) WsaCaScope					
F		sec_data_exch_ca(6)	SecDataExchCaScope			
G		wsa_ca (7)	WsaCaScope			
Н		crl_signer(8)	CRLSeries			
		root_ca (255)	RootCaScope			
J		ANY OTHER (128)	omit			

6.2.4 Authorization Authority

6.2.4.1 Normal Behavior

6.2.4.1.1 Scopes (Scope Kind and Scope Name)

```
TP Id
                      TP/SEC/AA/AUTH/NB-01
     Summary
                      Check that an AA responds to an authorization request with
                      an anonymous scope
                      with a valid authorization certificate.
                      IEEE P1609.2/D12 [1], clauses 6.2.22, 6.3.6, 6.3.7 and 6.3.19
     Reference
     Config Id
                      CF02
  PICS Selection
                                                Initial conditions
   the IUT in operational state
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a valid CertificateRequest (AuthorisationRequest) set to MSG_AUTHREQ_TS
         containing unsigned_csr
             containing subject_type
                set to 'sec_data_exch_anonymous'
             containing type_specific_data
                containing anonymous_scope
                containing additional_data
                    set to 0x00 (length 0)
   then {
      the IUT sends a valid CertificateResponse (AuthorisationResponse) set to MSG_AUTHRSP_IUT
          containing certificates[last].unsigned_certificate
             containing subject_type
                set to 'sec_data_exch_anonymous'
             containing type_specific_data
                containing anonymous_scope
                containing additional_data
                    set to 0x00 (length 0)
```

```
TP Id
                      TP/SEC/AA/AUTH/NB-02
     Summary
                      Check that an AA responds to an authorization request with
                      a localized scope with a name of different size
                      with a valid authorization certificate.
     Reference
                      IEEE P1609.2/D12 [1], clauses 6.2.22, 6.3.6, 6.3.7 and 6.3.19
     Config Id
                      CF02
  PICS Selection
                                                Initial conditions
with {
   the IUT in operational state
                                              Expected behaviour
ensure that {
   when {
      the IUT receives a valid CertificateRequest (AuthorisationRequest) set to MSG_AUTHREQ_TS
         containing unsigned_csr
             containing subject_type
                set to 'sec_data_exch_identified_localized'
             containing type_specific_data.id_scope.name
                set to SCOPE_NAME
   then {
      the IUT sends a valid CertificateResponse (AuthorisationResponse) set to MSG_AUTHRSP_IUT
         containing certificates[last].unsigned_certificate
             containing subject_type
                set to 'sec_data_exch_identified_localized'
             containing id_scope.name
                set to ANY_VALUE_OR_NONE
   }
                                                    Variants
   X
                                                      SCOPE NAME
                                                   of length > 0 and < 32
   Α
   В
                                                        of length 0
   С
                                                        of length 1
   D
                                                        of length 32
```

6.2.4.1.2 Expiration

	d ITP/SFC/	AA/AUTH/NB-03-X					
Summ	TP Id TP/SEC/AA/AUTH/NB-03-X Summary Check that AA responds to an authorization request with the validity period conformed to the						
•		request and to the enrolment certificate.					
Refere	Reference IEEE P1609.2/D12 [1], clauses 6.3.2 and 6.3.34						
Confi		<u> </u>					
PICS Sel							
	4	Initial cond	tions				
/ith {							
the IUT i	n operational state						
		Expected bel	naviour				
nsure that	{						
when {							
		CertificateRequest (Authorisation	nRequest) set to MSG_AU	THREQ_TS			
		ate.unsigned_certificate					
C	ontaining expiration	Cont					
•	set to EXP_ENR_	Cert					
C	ontaining lifetime set to LT_ENR_C	ort					
contr	set to LT_ENK_C aining unsigned_csr	GIL					
COLLE	ontaining expiration						
O.	set to EXP_AR						
C	ontaining lifetime						
•	set to LT_AR						
}							
then {							
uicii (
•	JT sends a valid Aut	thorizationResponse					
the II	nining certificates[las	thorizationResponse st].unsigned_certificate					
the II	aining certificates[last containing expiration	t].unsigned_certificate					
the II conta co	aining certificates[las ontaining expiration set to EXP_ARRe	t].unsigned_certificate					
the II conta co	aining certificates[last containing expiration set to EXP_ARRe containing lifetime	t].unsigned_certificate					
the II conta	aining certificates[las ontaining expiration set to EXP_ARRe	t].unsigned_certificate					
the II conta	aining certificates[last containing expiration set to EXP_ARRe containing lifetime	t].unsigned_certificate					
the II conta	aining certificates[last containing expiration set to EXP_ARRe containing lifetime	st].unsigned_certificate					
the II conta	nining certificates[last containing expiration set to EXP_ARRe containing lifetime set to LT_AResp	st].unsigned_certificate esp Variant		IT AR			
the II conta	aining certificates[last containing expiration set to EXP_ARRe containing lifetime set to LT_AResp	est].unsigned_certificate esp Variant t LT_ENR_Cert	EXP_AR	LT_AR			
the II contact of the II conta	eining certificates[last containing expiration set to EXP_ARRe containing lifetime set to LT_AResp EXP_ENR_Cer CLT+2Y	variant t LT_ENR_Cert 1M	EXP_AR CLT+2Y	1M			
the II contact of the II conta	eining certificates[last portaining expiration set to EXP_ARRe portaining lifetime set to LT_AResp EXP_ENR_Cer CLT+2Y CLT+2Y	variant t LT_ENR_Cert 1M 1Y	EXP_AR CLT+2Y CLT+2Y	1M 1M			
the II conta	eining certificates[last portaining expiration set to EXP_ARRe portaining lifetime set to LT_AResp EXP_ENR_Cer CLT+2Y CLT+2Y CLT+2Y	Variant t LT_ENR_Cert 1M 1Y 1Y	EXP_AR CLT+2Y CLT+2Y CLT+1Y + 1M	1M 1M 1M			
the II conta	eining certificates[last portaining expiration set to EXP_ARRest portaining lifetime set to LT_AResp EXP_ENR_Cer CLT+2Y CLT+2Y CLT+2Y CLT+2Y	Variant t LT_ENR_Cert 1M 1Y 1Y 2Y	EXP_AR CLT+2Y CLT+2Y CLT+1Y + 1M CLT+2Y	1M 1M 1M 2Y			
the II contact of the II conta	eining certificates[last portaining expiration set to EXP_ARRest portaining lifetime set to LT_AResp EXP_ENR_Cer CLT+2Y CLT+2Y CLT+2Y CLT+2Y CLT+2Y CLT+2Y	Variant t LT_ENR_Cert 1M 1Y 1Y 2Y 2Y	EXP_AR CLT+2Y CLT+2Y CLT+1Y + 1M CLT+2Y CLT + 1M	1M 1M 1M 2Y 1M			
the II contact of the II conta	eining certificates[last portaining expiration set to EXP_ARRe portaining lifetime set to LT_AResp EXP_ENR_Cer CLT+2Y CLT+2Y CLT+2Y CLT+2Y CLT+2Y CLT+2Y CLT+2Y CLT+2Y	Variant t LT_ENR_Cert 1M 1Y 1Y 2Y 2Y 4Y	EXP_AR CLT+2Y CLT+2Y CLT+1Y + 1M CLT+2Y CLT + 1M CLT+2Y	1M 1M 1M 2Y 1M 2Y			
the II contact of Cont	eining certificates[last portaining expiration set to EXP_ARRest portaining lifetime set to LT_AResp EXP_ENR_Cer CLT+2Y CLT+2Y CLT+2Y CLT+2Y CLT+2Y CLT+2Y	Variant t LT_ENR_Cert 1M 1Y 1Y 2Y 2Y	EXP_AR CLT+2Y CLT+2Y CLT+1Y + 1M CLT+2Y CLT + 1M	1M 1M 1M 2Y 1M			
the II contact of the II conta	eining certificates[last portaining expiration set to EXP_ARRest portaining lifetime set to LT_AResp expiration set to LT_ARESp e	Variant t LT_ENR_Cert 1M 1Y 1Y 2Y 2Y 4Y 4Y	EXP_AR CLT+2Y CLT+2Y CLT+1Y + 1M CLT+2Y CLT + 1M CLT+2Y CLT + 1M	1M 1M 1M 2Y 1M 2Y 1M 2Y 1M			
the II contact of the II conta	eining certificates[last portaining expiration set to EXP_ARRe portaining lifetime set to LT_AResp EXP_ENR_Cer CLT+2Y CLT+2Y CLT+2Y CLT+2Y CLT+2Y CLT+2Y CLT+2Y CLT+2Y	Variant t LT_ENR_Cert 1M 1Y 1Y 2Y 2Y 4Y 4Y	EXP_AR CLT+2Y CLT+2Y CLT+1Y + 1M CLT+2Y CLT + 1M CLT+2Y CLT + 1M	1M 1M 1M 2Y 1M 2Y 1M 2Y 1M			
the II contact of the II conta	EXP_ENR_Cer CLT+2Y	Variant t LT_ENR_Cert 1M 1Y 2Y 2Y 4Y 4Y with I	EXP_AR CLT+2Y CLT+2Y CLT+1Y + 1M CLT+2Y CLT + 1M CLT+2Y CLT + 1M EXP_AResp =< EXP_ENR_EXP_AResp <= EXP_A	1M 1M 1M 2Y 1M 2Y 1M 2Y 1M			
the II contact of the II conta	eining certificates[last portaining expiration set to EXP_ARRest portaining lifetime set to LT_AResp expiration set to LT_ARESp e	Variant t LT_ENR_Cert 1M 1Y 2Y 2Y 4Y 4Y with I	EXP_AR CLT+2Y CLT+2Y CLT+1Y + 1M CLT+2Y CLT + 1M CLT+2Y CLT + 1M	1M 1M 1M 2Y 1M 2Y 1M 2Y 1M Cert AND R			

6.2.4.2 Exceptional Behavior

6.2.4.2.1 Invalid Certificates or Certificate Chain Fields

TP	ld	TP/SEC/AA/AUTH/EB-01-X		
Sum	mary	Check that an AA discards an authorization request signed		
	•	by a signer_id with type set to an other value than 'certificate' or ' certificate_chain'.		
Refer	Reference ETSI TS 102 941 [2] (V1.1.1), clause 6.2.2.3			
Conf	Config ld CF02			
PICS Se	election			
		Initial conditions		
with {				
the IUT	in operation	nal state		
}				
		Expected behaviour		
ensure tha	t {			
when {				
		s a CertificateRequest set to MSG_AUTHREQ_TS		
1	containing s			
	containir			
	set to	X_INVALID_SIGNER_TYPE		
}				
then {				
		a valid CertificateRequestError set to MSG_AUTHERR_IUT		
	containing r			
	set to 're	equest_denied'		
}				
}		N. L. d		
<u> </u>		Variants TVP5		
X		X_INVALID_SIGNER_TYPE		
A		self(0)		
В		certificate_digest_with_ecdsap224(1)		
С		certificate_digest_with_ecdsap256(2)		
D		certificate_digest_with_other_algorithm(5)		
E		ANY OTHER (128)		

6.2.4.2.2 Invalid Scopes (Subject Type and Scope Name)

TP ld	TP/SEC/AA/AUTH/EB-02-X			
Summary	Check that an AA discards an authorization request with a subject type other than			
	sec_data_exch_anonymous or sec_data_exch_identified_localized.			
Reference	IEEE P1609.2/D12 [1], clauses 5.5.3.3 and 6.3.7, ETSI TS 102 867 [3], clause 5.1.2.1			
Config Id	CF02			
PICS Selection				
	Initial conditions			
with {				
the IUT in opera	ational state			
}				
	Expected behaviour			
ensure that {				
when {				
	sives a CertificateRequest set to MSG_AUTHREQ_TS			
	ng signer.certificate.unsigned_certificate.sec_data_exch_ca_scope.permitted_subject_types			
set to	X_PERMITTED_SUBJECT_TYPES			
	ng unsigned_csr			
	aining subject_type			
	et to X_INVALID_SUBJECT_TYPE			
	aining type_specific_data			
Co	ontaining X_INVALID_SCOPE			
}				
then {				
	the IUT sends a valid CertificateRequestError set to MSG_AUTHERR_IUT			
	containing reason			
set to	request_denied'			
}				
}				
	Variants			

	Variants					
Х	X_PERMITTED_SUBJECT_TYPES	X_INVALID_SUBJECT_TYPE	X_INVALID_SCOPE			
Α	sec_data_exch_identified_localized	sec_data_exch_identified_not_localize	IdentifiedNotLocalizedScop			
	and sec_data_exch_anonymous	d (1)	е			
В	sec_data_exch_identified_localized	sec_data_exch_csr (3)	SecDataExchCaScope			
	and sec_data_exch_anonymous					
С	sec_data_exch_identified_localized	wsa (4)	WsaCaScope			
	and sec_data_exch_anonymous					
D	sec_data_exch_identified_localized	wsa_csr (5)	WsaCaScope			
	and sec_data_exch_anonymous					
E	sec_data_exch_identified_localized	sec_data_exch_ca(6)	SecDataExchCaScope			
	and sec_data_exch_anonymous					
F	sec_data_exch_identified_localized	wsa_ca (7)	WsaCaScope			
	and sec_data_exch_anonymous					
G	sec_data_exch_identified_localized	crl_signer(8)	CRLSeries			
	and sec_data_exch_anonymous					
Н	sec_data_exch_identified_localized	root_ca (255)	RootCaScope			
	and sec_data_exch_anonymous					
I	sec_data_exch_identified_localized	ANY OTHER (128)	omit			
	and sec_data_exch_anonymous					
J	sec_data_exch_identified_localized	sec_data_exch_anonymous (0)	AnonymousScope			
K	sec_data_exch_anonymous	sec_data_exch_identified _localized	IdentifiedLocalizedScope			
		(2)				

History

Document history		
V1.1.1	July 2013	Publication