ETSI TS 103 601 V2.1.1 (2024-03)

TECHNICAL SPECIFICATION

Intelligent Transport Systems (ITS); Security; Security management messages communication requirements and distribution protocols; Release 2

Reference

RTS/ITS-005115

Keywords

ITS, protocol, security

ETSI

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

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

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

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

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

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

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

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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

1 Scope

The present document defines communication requirements and profiles to support communications from/to ITS-S stations (e.g. fixed road side ITS-S, mobile ITS-S) for the support of security management services specified in ETSI TS 102 941 [2] (i.e. certificate management, trust and revocation lists distribution).

The present document also defines the related protocol handling for the selected messages as well as the requirements for the lower layer protocol stacks and for the Security Management entity in order to support message dissemination and reception.

2 References

2.1 Normative references

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

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

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

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

[1] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2".

[2] ETSI TS 102 941: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2".

[3] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2".

[4] ETSI TS 103 248 (V2.3.1): "Intelligent Transport Systems (ITS); GeoNetworking; Port Numbers for the Basic Transport Protocol (BTP); Release 2".

[5] ETSI TS 103 836-4-1: "Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality; Release 2".

[6] ETSI TS 102 965: "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration; Release 2".

[7] Recommendation ITU-T X.696: "Information technology - ASN.1 encoding rules: Specification of Octet Encoding Rules (OER)".

[8] IEEE Std 1609.2™-2022: "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages".

2.2 Informative references

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

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

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

[i.1] IEEE 802.11™: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.2] ETSI EN 302 890-1: "Intelligent Transport Systems (ITS); Facilities layer function; Part 1: Services Announcement (SA) specification".

[i.3] ISO/IEC 9646-7 (1995): "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[i.4] ISO/IEC 8824-1:2015: "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[i.5] ETSI TS 103 836: Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols.

[i.6] C. Fragouli et al: "Network coding: an instant primer", ACM SIGCOMM Computer Communication Review, Vol. 36, No. 1, January 2006, pp 63-68.

[i.7] Pouya Ostovari, Jie Wu, and Abdallah Khreishah: "Network Coding Techniques for Wireless and Sensor Networks", 18 January 2015.

[i.8] Philip A. Chou and Yunnan Wu: "Network Coding for the Internet and Wireless Networks", Microsoft Report MSR-TR-2007-70, June 2007.

[i.9] Farhan Jamil, Anam Javaid, Tariq Umer, Mubashir Husain Rehmani: "A comprehensive survey of network coding in vehicular ad-hoc networks", Wireless Networks, May 2016.

[i.10] Robert H. Morelos-Zaragoza: The Art of Error Correcting Coding, Second Edition, John Wiley & Sons, 2006, ISBN: 0470015586.

[i.11] IETF RFC 6726: "FLUTE - File Delivery over Unidirectional Transport", November 2012.

[i.12] IETF RFC 5651, M. Luby, M. Watson, L. Vicisano: "Layered Coding Transport (LCT) Building Block", October 2009.

[i.13] IETF RFC 5052, M. Watson, M. Luby, and L. Vicisano: "Forward Error Correction (FEC) Building Block", August 2007.

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 102 940 [1], ETSI TS 102 941 [2] and the following apply:

CTL/CRL Distribution Application: software application supported by an ITS-S that enables a relay service for storing and distribution of CTL/CRL to other ITS-S

Maximum Transmission Unit (MTU): maximum packet size in octets that can be conveyed in one piece over a data link

3.2 Symbols

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

N1 number of attempts that an ITS-S is authorized to do after the sending of the EC request. Note that N1 is a non-negative integer (N1 ≥ 0)
N1 = 0 means that no EC retry is possible
N1 = 1 means that after sending the EC request and not having received the response (because of EC request loss or EC response loss), the ITS-S can use the EC retry service only one time
N2 it is the number of attempts that an ITS-S is authorized to do after the sending of the AT request. Note that N2 is a non-negative integer (N1 ≥ 0).
N2 = 0 means that no AT retry is possible
N2 = 1 means that after sending the AT request and not having received the response (because of AT request loss or AT response loss), the ITS-S can use the AT retry service only one time
T1 time interval between two successive repeated EC requests that are performed by an ITS-S
T2 life-time duration of the created EC request by the requesting ITS-S
T3 time interval between the reception/storage of the context information of the initial EC Request and the last incoming/repeated EC request received by an EA
T4 time interval between two successive repetitions of the same AT request that are performed by an ITS-S
T5 life-time duration of the created AT by the requesting ITS-S
T6 time interval between the reception/storage of the context information of the initial AT Request and the last incoming/repeated AT request received by an AA
$T_{P2pctldMax}$ maximum waiting time before a responder ITS-S which has received a request for a specific CTL or a broadcasting ITS-S starts transmitting the successive segments containing the full CTL, after listening to detect if another ITS-S has not already started to send the same CTL
d repetition duration of the CTL or CRL broadcast transmission in days or in seconds. If d=0 then the list is transmitted only once
f repetition frequency of the CTL or CRL broadcast transmission in millihertz
N_{total} total number of consecutive segments transmitted by the Sender which applies segmentation of the original message, e.g. a FullCtl

3.3 Abbreviations

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

5G-NR	5G New Radio
AA	Authorization Authority
AES	Advanced Encryption Standard
AID	Application Identifier
ALC	Asynchronous layered coding
ASN	Abstract Syntax Notation
AT	Authorization Ticket
B2B	Business to Business

BTP	Basic Transport Protocol
CA	Certification Authority
CAM	Cooperative Awareness Message
CCMS	Cooperative-ITS Certificate Management System
CP	Certificate Policy
CPOC	C-ITS Point Of Contact
CRL	Certificate Revocation List
CTL	Certificate Trust List
CXLDA	CRL/CTL Distribution Application
DC	Distribution Centre
EA	Enrollment Authority
EC	Enrollment Credential
ECTL	European Certificate Trust List
EN	European Norm
FDT	File Delivery Table
FEC	Forward Error Correction
F-PDU	Facilities Layer Protocol Data Unit
GBC	GeoBroadCast
GN	GeoNetworking
GN_SAP	GeoNetworking_Service Access Point
GN6	GeoNetworking over IPv6
GUC	GeoUniCast
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
ITS	Intelligent Transport System
ITS-G5	5 GHz wireless communication
ITS-S	Intelligent Transport System - Station
LCT	Layer Coding Transport
MTU	Maximum Transmission Unit
NR	New Radio
OER	Octet Encoding Rules
OID	Object Identification number
P2P	Peer-to-Peer
P2PCXLD	Peer-to-peer CRL/CTL Distribution service
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
PSID	Provider Service Identifier
RA	Router Advertisement
RAN	Radio Access Network
RCA	Root Certification Authority
R-ITS-S	Roadside ITS-S
RMT	Reliable Multicast Transport
RSU	Road Side Unit
SAM	Service Advertisement Message
SCH	Service CHannel
SCRM	Segmented CTL Response Message
SHA	Secure Hash Algorithm
SHB	Single Hop Broadcast
SLAAC	StateLess Address Auto-Configuration
SM-PDU	Security Management PDU
TA	Trust Anchor
TCP	Transmission Control Protocol
TLM	Trust List Manager
TS	Technical Specification
UC	Use Case
UPER	Unaligned Packed Encoding Rule
URL	Uniform Resource Locator
V2X	Vehicle to Everything
V-ITS-S	Vehicle ITS-S
WLAN	Wireless Local Area Network

3.4 Notations

For the purposes of the present document, the notations given in ETSI TS 102 940 [1] apply.

4 Services description: use cases and requirements

4.1 Certificate provisioning service

4.1.1 Service description

4.1.1.1 Overview

The certificates reloading service consists for an ITS-S to request EC/AT to the PKI in an online and automatic manner. EC requests are not frequent as an ITS-S usually requests one EC at the beginning of its lifecycle and then renews its EC in advance before the end of its key validity period [2]. However, AT are requested much more often. Indeed when an ITS-S has only a few remaining Ats it requests new ones to the PKI.

Figure 1 depicts the service from a V-ITS-S and a R-ITS-S point of view:

1) (Green arrow) - A V-ITS-S is within the radio coverage of a RAN access point that provides Internet connectivity (e.g. cellular base station, Wi-Fi hotspot, R-ITS-S, etc.). The V-ITS-S thus sends its EC/AT request to the PKI via the RAN access point and the Gateway. The PKI processes the request and sends back immediately its response to the V-ITS-S.

2) (Orange arrows) - A R-ITS-S is connected to the Internet either wired (e.g. optical fibre, Ethernet, etc.) or wirelessly via a RAN access point (e.g. cellular base station, Wi-Fi® hotspot, etc.). The R-ITS-S thus sends its EC/AT request to the PKI directly (wire) or via the RAN access point and the Gateway. The PKI processes the request and sends back immediately its response to the R-ITS-S.

NOTE: In the present document, the RAN Access Point and the Gateway are differentiated. The RAN Access Point is hardware that provides radio access and the Gateway is the relaying software that links the local network with the Internet. However the Gateway may be integrated in the RAN Access Point.

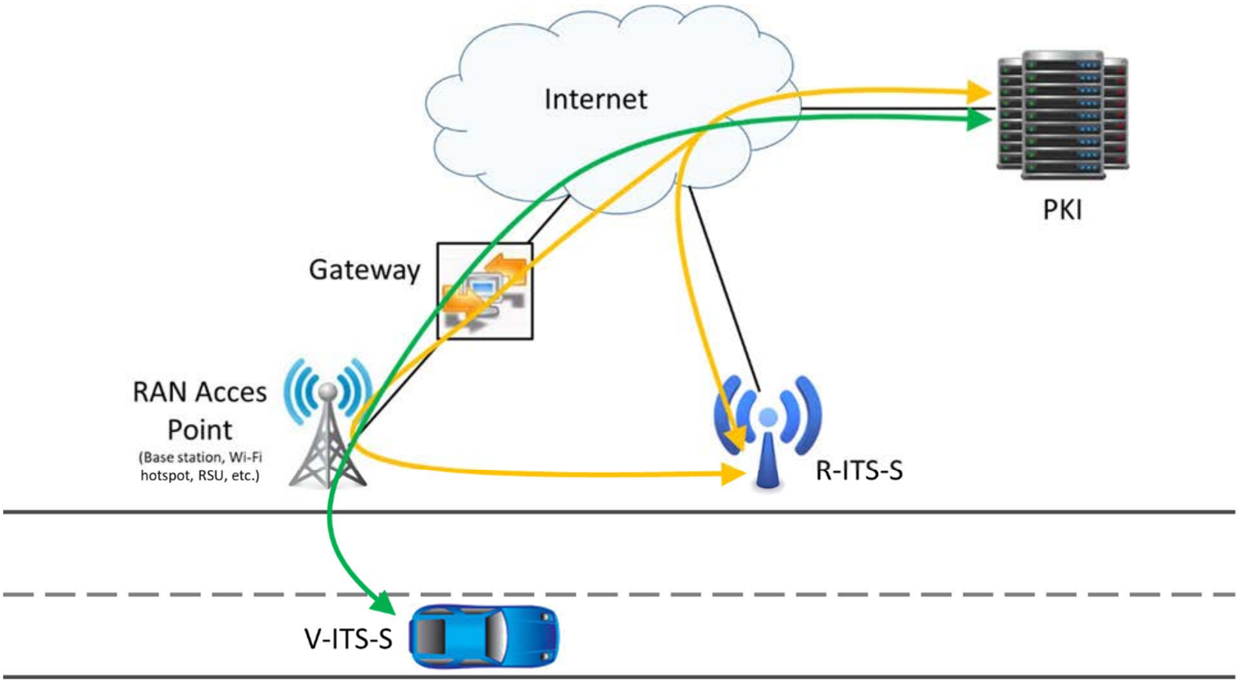


Figure 1: Example of certificates reloading service for a V-ITS-S (green) and a R-ITS-S (orange)

4.1.1.2 UC-SEC-01: EC initial request or re-keying

Use Case ID:	***UC-SEC-01***
Use Case Name:	Enrolment credential initial request or re-keying.
Priority:	Mandatory.
Related Requirement:	ITS-S is registered in the PKI. ITS-S has Ipv6 connectivity.

Primary Actor	ITS-S.		
Description	ITS-S requests an EC to the EA. After verification, the EA replies positively by sending back the requested EC to the ITS-S.		
Preconditions	ITS-S has its canonical key pair, a canonical identifier, the URL of the EA and the EA certificate. ITS-S is already registered in EA database. ITS-S has Ipv6 connectivity. If a wireless connectivity is used, the ITS-S shall be under the radio coverage of an access point that provides Ipv6 connectivity.		
Success End Condition	ITS-S receives its EC from the EA.		
Failed End Condition	ITS-S does not receive its EC.		
Involved components	Security layer.		
Main Success Scenario	1) ITS-S creates the EC request and sends it to the EA. 2) The EA verifies the EC request (as specified in ETSI TS 102 941 [2]) and sends the EC response to the ITS-S. 3) ITS-S receives its EC delivered by the EA.		
Extensions	None.		
Variations (Alternatives)	If the ITS-S does not receive a response from the EA, it may resume the same EC request to the EA until a maximum retry threshold or maximum delay is reached. Notice that the ITS-S may select another communication profile to resend its request. If the above procedure failed and the ITS-S has still not received its EC and its current EC has expired, the ITS-S notifies the user or the manufacturer/device operator about the situation.		
Includes			
Security Characteristics			
Authentication	Yes	Integrity	Yes
Confidentiality	Yes	Authorization	Yes
Anonymity privacy	No	Pseudonymity privacy	No
Availability	Yes	Plausibility	No
Auditability (Accountability)	Yes	Jurisdictional Access	-

4.1.1.3 UC-SEC-02: AT reloading

Use Case ID:	***UC-SEC-02***
Use Case Name:	Authorization ticket reloading.
Priority:	Mandatory.
Related Requirement:	ITS-S is registered in the PKI. ITS-S has a valid EC. ITS-S has Ipv6 connectivity.

Primary Actor	ITS-S.
Description	ITS-S requests an AT to the AA. After verifications, the AA replies positively by sending back the requested AT to the ITS-S.
Preconditions	ITS-S has its canonical key pair, a canonical identifier, its EC certificate and associated private key, the URL of the AA and the AA certificate. ITS-S is already registered in EA database. ITS-S has Ipv6 connectivity. If wireless connectivity is used, the ITS-S shall be under the radio coverage of an access point that provides Ipv6 connectivity.
Success End Condition	ITS-S receives its AT from the AA.
Failed End Condition	ITS-S does not receive its AT.
Involved components	Security layer.

Main Success Scenario	1) ITS-S creates the AT request and sends it to the AA. 2) The AA verifies the AT request (as specified in ETSI TS 102 941 [2]) and sends the AT reply to the ITS-S. 3) ITS-S receives its AT delivered by the AA.		
Extensions	None.		
Variations (Alternatives)	If the ITS-S does not receive a response from the AA, it may resume the same AT request to the AA until a maximum retry threshold or maximum delay is reached. Notice that the ITS-S may select another communication profile to resend its request. If the above procedure failed and the ITS-S has still not received its AT, the ITS-S may create a new AT request and sends it to another AA.		
Includes			
Security Characteristics			
Authentication	Yes	Integrity	Yes
Confidentiality	Yes	Authorization	Yes
Anonymity privacy	No	Pseudonymity privacy	Yes
Availability	Yes	Plausibility	No
Auditability (Accountability)	Yes	Jurisdictional Access	-

4.1.1.4 Use cases and communication profiles mapping

Table 1 summarizes the communication profiles that can be used for each use case. Details of the communication profiles are provided in clause 6 of the present document.

Table 1: Mapping between use cases and communication profiles

		CPS_001	CPS_002	CPS_003	CPS_004
UC-SEC-01	**R-ITS-S**		X		
	V-ITS-S	X (see note)	X		
UC-SEC-02	**R-ITS-S**		X		
	V-ITS-S	X	X		
NOTE: CPS_001 cannot be used to request the first EC as the ITS-S has no AT yet to sign the GN packet.					

4.1.2 Requirements

4.1.2.1 Security requirements

The PKI management protocols shall satisfy the following basic set of security objectives:

- **Authentication/authorization control:** authentication consists to be sure of the identity which sends data. Authorization control is the verification of an access policy, based on a trusted authentication. Authenticate all entities participating in the protocol is required to prevent illegitimate persons to enter in the system, or to access some unauthorized resources or services.

- **Integrity:** the integrity of all transmitted data is important to ensure that the contents of the received data are not altered.

- **Confidentiality/Privacy:** the enrolment/authorization request data and the delivered certificates in responses shall only be accessed by authorized entities. The real identity of ITS Station has to be protected, by cryptographic mechanisms and depending on the type of data sent.

- **Non-repudiation/Traceability:** non-repudiation is necessary to prevent ITS Station or others entities from denying the transmission or the content of their messages. Traceability, which is the warranty that an entity cannot refute the emission or reception of information, is also extremely important.

- **Unlinkability:** ability of a user to make multiple uses of resources or services without others being able to link these uses together.

- **Anonymity:** ability of a user to use a resource or service without disclosing the user's identity.

4.2 CTL distribution service

4.2.1 Service description

4.2.1.1 Overview

Within the CCMS framework, the CTL or ECTL is generated and issued by the Root CA or the TLM and published by a DC or CPOC to be made available to all the participants of the trusted C-ITS system, as specified in ETSI TS 102 940 [1]. The issuance of a new CTL (or ECTL) should be done periodically as well as on specific conditions triggered by a security management event or a security incident such as the revocation of an entity of the CCMS.

For each new update of the CTL issued by a Root CA, the Root CA shall provide the base CTL information (fullCTL) and the corresponding Delta CTL (deltaCTL) following the data structures' format specified in ETSI TS 102 941 [2].

For each new update of the ECTL issued by the TLM, the TLM shall provide the base CTL information (fullCTL) and the corresponding Delta CTL (deltaCTL) following the data structures' format specified in ETSI TS 102 941 [2].

The receiving C-ITS stations shall maintain and store the latest certificate trust lists to apply signature and certificate chain validation on received messages (as specified in ETSI TS 103 097 [3]). The transmission and distribution process of certificate trust lists to all the C-ITS stations and to the CCMS entities should be provided efficiently and in a timely manner.

For interoperability purpose, ETSI TS 102 941 [2] specifies the interface with the DC to distribute the base CTL and corresponding delta CTL information and the interface with the CPOC to distribute the base ECTL and corresponding delta ECTL information. In ETSI TS 102 941 [2], clause D.1, a basic mandatory protocol is specified using HTTP v1.1 GET. Other optional protocols may be proposed e.g. for broadcasting over a short-range wireless communication or other radio broadcasting technologies (e.g. LTE, 5G, satellite or terrestrial broadcast system).

4.2.1.2 UC-SEC-03: On demand request of a FullCTL

This use case allows an ITS-S to update its certificate trust list information by requesting the Full CTL to the corresponding CPOC (which distributes the ECTL published by a TLM) or DC (which distributes the CTL published by a RCA).

In this use case, the ITS-S shall use the communication profile as specified in ETSI TS 102 941 [2], clause D.1. It is agnostic from the underlying communication medium.

Use Case ID:	***UC-SEC-03***
Use Case Name:	Get Certificate Trust List.
Priority:	Mandatory.
Related Requirement:	V-ITS-S or R-ITS-S stores CPOC or DC access point received at initialization or via the prior base ECTL or CTL. V-ITS-S or R-ITS-S has an available cellular network connection (3G/4G, LTE or 5G NR) or a short-range wireless interface to a RSU providing internet communication.

Primary Actor	ITS station.
Description	ITS Station wants to update the signed list of trusted PKI authorities published by the TLM (ECTL) or the CTL published by its own Root CA or by other Root CAs (CTL distributed by a Distribution Centre).
Preconditions	-
Success End Condition	ITS station received the latest (base) CTL or ECTL and was able to check its validity and store it in its local secure memory storage.
Failed End Condition	-
Involved components	CPOC or DC, Security layer of the ITS-S, HTTP over TCP-IP, cellular or ITS-G5 communication via a R-ITS-S connected to Internet.
Main Success Scenario	1) ITS Station sends request to CPOC or DC. The communication profile is specified in ETSI TS 102 941 [2], clause D.1 and figure C.1 for cellular communication stack. 2) CPOC or DC returns CTL.

Extensions	-
Variations (Alternatives)	ITS-S may request the more recent update of the full CTL to another ITS-S using the peer-to-peer request of a full CTL (see Use Case UC-SEC-08).
Includes	-

Security Characteristics			
Authentication	Yes	Integrity	Yes
Confidentiality	No	Authorization	-
Anonymity privacy	-	Pseudonymity privacy	-
Availability	Yes	Plausibility	No
Auditability (Accountability)	No	Jurisdictional Access	-

4.2.1.3 UC-SEC-04: On demand request of a DeltaCTL

Use Case ID:	***UC-SEC-04***
Use Case Name:	On demand request of a DeltaCTL.
Priority:	Mandatory for R-ITS-S as the R-ITS-S shall be used as a relay for distribution of Delta CTLs (see UC-SEC-07). Optional for V-ITS-S: it is not necessary that all V-ITS-Ss provide the DeltaCTL to other ITS-Ss. Only some public safety or specific V-ITS-Ss (road managers) mays support this UC.
Related Requirement:	V-ITS-S or R-ITS-S stores CPOC or DC access point received at initialization or via the prior base ECTL or CTL. V-ITS-S or R-ITS-S has an available cellular network connection (3G/4G, LTE or 5G NR). V-ITS-S or R-ITS-S is providing a relay service for CTL distribution and is providing a memory storage to store Delta CTL messages issued by a TLM and/or Delta CTL messages issued by its own RCA.

Primary Actor	V-ITS-S or R-ITS-S.
Description	V-ITS-S or R-ITS-S requests the DeltaCTL corresponding to the base CTL to the CPOC or Distribution Centre (DC).
Preconditions	V-ITS-S or R-ITS-S has received from the CPOC the latest updated ECTL (of sequence number: ctlSequence) and/or V-ITS-S or R-ITS-S has received from its Distribution Centre (DC) the latest updated CTL (of sequence number: ctlSequence).
Success End Condition	V-ITS-S or R-ITS-S received the latest DeltaCTL corresponding to the base ECTL (sequence number: ctlSequence) and was able to store it in its local memory storage.
Failed End Condition	V-ITS-S or R-ITS-S did not receive the requested DeltaCTL.
Involved components	CPOC or DC, CtlDistribution application and local data base in ITS-S, Security layer, HTTP over TCP or UDP-IP, cellular.
Main Success Scenario	1) V-ITS-S or R-ITS-S sends a request to get the DeltaCTL of sequence number (ctlSequence) to the CPOC (or DC) using its access point information (URL). The communication profile is specified in ETSI TS 102 941 [2], clause D.1. 2) DC returns the DeltaCTL. 3) V-ITS-S or R-ITS-S receives a DeltaCTL message from CPOC or DC, checks its signature validity and its parameter value (issuer identifier, sequence number, type of CTL format, nextUpdate) then stores it in its memory storage.
Extensions	If the Main Success Scenario does not work for any reason, the V-ITS-S may resume the DeltaCTL request after a given time-out until it reaches the time when the current base CTL is considered expired (nextUpdate).
Variations (Alternatives)	V-ITS-S may also receive the last updated DeltaCTL issued by the TLM (TlmCertificateTrustListMessage) and/or issued by RCA (RcaCertificateTrustListMessage) using a Terrestrial or satellite broadcast network.
Includes	-

Security Characteristics			
Authentication	Yes	Integrity	Yes
Confidentiality	No	Authorization	-
Anonymity privacy	-	Pseudonymity privacy	-
Availability	Yes	Plausibility	No
Auditability (Accountability)	No	Jurisdictional Access	-

NOTE: The requesting ITS Station may also send the DeltaCTL request via a WLAN consumer network using IEEE 802.11 [i.1] or any other kind of available connectivity such as a Wired communication.

4.2.1.4 UC-SEC-05: ITS-S based DeltaCTL distribution

This use case focuses on end-entities such as R-ITS-S or V-ITS-S that have the capabilities of distributing Delta ECTL or Delta CTL using their short-range wireless communication interface. The receiving ITS-S is a mobile ITS station, as the fixed ITS Station shall use other Use cases for requesting the updated ECTL or CTL using wired or cellular communication link (i.e. UC-SEC-03 or UC-SEC-04). These capabilities shall be stated using the PICS template as specified in annex A.

Use Case ID:	***UC-SEC-05***
Use Case Name:	ITS-S based DeltaCTL distribution.
Priority:	Mandatory for R-ITS-S, Optional for V-ITS-S.
Related Requirement:	ITS-S stores CPOC or DC access point received at initialization or via the prior base ECTL or CTL. ITS-S is providing a local service and local data base for DeltaCTL broadcasting over short-range wireless communication. The data base is used to store DeltaCTL messages issued by a TLM (TlmCertificateTrustListMessage) and/or CTL messages issued by its RCA (RcaCertificateTrustListMessage) as specified in ETSI TS 102 941 [2] (see note 1).

<table>
<tr><td><b>Primary Actor</b></td><td colspan="3">ITS-S, receiving V-ITS-Ss.</td></tr>
<tr><td><b>Description</b></td><td colspan="3">ITS-S broadcasts periodically DeltaCTL messages stored locally on short-range wireless communication.</td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">ITS-S has received from the CPOC the current DeltaCTL corresponding to the base ECTL and has checked its validity before re-transmitting and/or ITS-S has received from its Distribution Centre (DC) the current DeltaCTL corresponding to the base CTL and has checked its validity before forwarding.</td></tr>
<tr><td><b>Success End Condition</b></td><td colspan="3">Receiving V-ITS-Ss in the communication range of the ITS-S received the latest DeltaECTL/DeltaCTL corresponding to the base ECTL/CTL (sequence number: ctlSequence) and were able to update their ECTL/CTL from the prior base ECTL/CTL stored (of sequence number: ctlSequence -1).</td></tr>
<tr><td><b>Failed End Condition</b></td><td colspan="3">V-ITS-Ss did not receive the DeltaECTL/DeltaCTL distributed by the ITS-S, or were not able to update their ECTL/CTL information based on their prior base ECTL/CTL stored.</td></tr>
<tr><td><b>Involved components</b></td><td colspan="3">CtlDistribution application and local data base in ITS-S, Security layer, GN, IEEE 802.11 [i.1], available ITS channel for DeltaCTL broadcasting.</td></tr>
<tr><td><b>Main Success Scenario</b></td><td colspan="3">1) V-ITS-S is within radio communication range of the sending ITS-S.
2) ITS-S periodically broadcasts DeltaCTL messages using GeoNetworking (single hop broadcast) with frequency f (transmission rate should be lower than CAM transmission rate if a safety channel is used and should be reduced or even stopped based on the current channel congestion level). ITS-S broadcasts DeltaCTL messages for a duration of d days upon reception. The broadcast stops if the DeltaCTL is expired, or if the sending ITS-S receives a new DeltaCTL or if the ITS-S detects that another ITS-S is broadcasting the same DeltaCTL.
3) V-ITS-S receives a DeltaCTL message, checks its signature validity and its parameter value (issuer identifier, sequence number, type of DeltaCTL format, nextUpdate) then stores it in a storage memory.
4) Using the received DeltaCTL, the V-ITS-S computes the new base fullCTL information for the corresponding issuer and store it in its memory.</td></tr>
<tr><td><b>Extensions</b></td><td colspan="3">If the Main Success Scenario does not work for any reason, the V-ITS-S may try to request the base CTL to the CPOC/DC using any of the available communication types (e.g. cellular, WLAN, diagnostic system at a garage, ITS-G5 via a R-ITS-S, etc.). The communication profile is specified in ETSI TS 102 941 [2], clause D.1.</td></tr>
<tr><td><b>Variations (Alternatives)</b></td><td colspan="3">If the ITS-S has the FullCTL message issued by the TLM or the RCA in its memory, it may also broadcast the FullCTL (see UC-SEC-10).</td></tr>
<tr><td><b>Includes</b></td><td colspan="3">-</td></tr>
<tr><td colspan="4"><b>Security Characteristics</b></td></tr>
<tr><td>Authentication</td><td>Yes</td><td>Integrity</td><td>Yes</td></tr>
<tr><td>Confidentiality</td><td>No</td><td>Authorization</td><td>Yes</td></tr>
<tr><td>Anonymity privacy</td><td>No</td><td>Pseudonymity privacy</td><td>No</td></tr>
<tr><td>Availability</td><td>Yes</td><td>Plausibility</td><td>No</td></tr>
<tr><td>Auditability (Accountability)</td><td>Yes</td><td>Jurisdictional Access</td><td>-</td></tr>
</table>

NOTE 1: The R-ITS-S may distribute the Delta CTL issued by its own RCA (home PKI) in order to update all passing mobile ITS-Ss belonging to the same PKI (home PKI). It may also offer the same distribution service described in this use case for the distribution of Delta CTLs from other PKIs depending on the stakeholders' business model. For instance, in a trans-European CORRIDOR where the motorways are crossing several countries, the motorway operator may provide distribution of CTL or CRL from other PKIs, i.e. national authorities or private organizations (car manufacturers or device operators).

NOTE 2: f and d values need to be defined. Examples of values are f = 500 mHz, d = 7 days.

4.2.1.5 UC-SEC-06: Delay-tolerant peer-2-peer DeltaCTL distribution

Use Case ID:	***UC-SEC-06***
Use Case Name:	Delay-tolerant peer-2-peer DeltaCTL distribution.
Priority:	Mandatory.
Related Requirement:	ITS-S (neighbour) has received from the CPOC the current DeltaCTL corresponding to the base ECTL and has checked its validity. ITS-S is providing a memory storage to store DeltaCTL messages issued by a TLM and/or DeltaCTL messages issued by its own RCA. ITS-S has an available V-ITS-S present in the radio range.

Primary Actor	ITS-S (neighbours), Requesting V-ITS-Ss.		
Description	V-ITS-S requests the DeltaCTL corresponding to the base CTL to the ITS-Ss present in the radio range.		
Preconditions	ITS-S has received from the CPOC the latest updated ECTL (of sequence number: ctlSequence) and/or ITS-S has received from its Distribution Centre (DC) the latest updated CTL (of sequence number: ctlSequence).		
Success End Condition	V-ITS-S received the latest DeltaECTL/DeltaCTL corresponding to the base ECTL/CTL (sequence number: ctlSequence) and was able to check its validity and store it in its local memory storage.		
Failed End Condition	V-ITS-S did not receive the requested DeltaECTL/DeltaCTL.		
Involved components	CtlDistribution application and local data base in V-ITS-S, Security layer, GN, IEEE 802.11 [i.1].		
Main Success Scenario	1) V-ITS-S sends a request to get the DeltaECTL/DeltaCTL of sequence number (ctlSequence) to ITS-Ss (ITS-S neighbours) present in the radio range. 2) ITS-S neighbour returns the corresponding DeltaECTL or DeltaCTL. 3) V-ITS-S receives a DeltaECTL or DeltaCTL message, checks its signature validity and its parameter value (issuer identifier, sequence number, type of CTL format, nextUpdate) then stores it in its memory storage. 4) Using the received DeltaECTL or DeltaCTL, the receiving V-ITS-S computes the new base fullECTL or fullCTL information for the corresponding issuer and stores it in a secure memory.		
Extensions	If the Main Success Scenario does not work for any reason, the V-ITS-S may resume the DeltaECTL/DeltaCTL request after a given time-out or it will try to request DeltaECTL/DeltaCTL as described in UC-SEC-04 until it reaches the time when the current base ECTL/CTL is considered expired (next Update) or until the DeltaECTL/DeltaCTL reception as described in UC-SEC-03, UC-SEC-04.		
Variations (Alternatives)			
Includes	**-**		
Security Characteristics			
Authentication	Yes	Integrity	Yes
Confidentiality	No	Authorization	Yes
Anonymity privacy	-	Pseudonymity privacy	-
Availability	Yes	Plausibility	No
Auditability (Accountability)	Yes	Jurisdictional Access	-

NOTE: The ECTL/CTL request message may use an in-band protocol mechanism using the periodically broadcast messages (e.g. secured data in CAMs) similar to the certificate request protocol specified in ETSI TS 103 097 [3].

4.2.1.6 UC-SEC-10: ITS-S based FullCTL distribution

This use case focuses on end-entities such as R-ITS-S or V-ITS-S that have the capabilities of distributing ECTL or CTL using their short-range wireless communication interface. The receiving ITS-S is a mobile ITS station, as the fixed ITS Station shall use other Use cases for requesting the updated ECTL or CTL using wired or cellular communication link (i.e. UC-SEC-03 or UC-SEC-04). These capabilities shall be stated using the PICS template as specified in annex A.

Use Case ID:	***UC-SEC-10***
Use Case Name:	ITS-S based FullCTL distribution.
Priority:	Mandatory for R-ITS-S, Optional for V-ITS-S.
Related Requirement:	ITS-S stores CPOC or DC access point received at initialization or via the prior base ECTL or CTL. ITS-S is providing a local service and local data base for CTL broadcasting over short-range wireless communication. The data base is used to store CTL messages issued by a TLM (TlmCertificateTrustListMessage) and/or CTL messages issued by its RCA (RcaCertificateTrustListMessage) as specified in ETSI TS 102 941 [2] (see note 1).

<table>
<tr><td colspan="2"><b>Primary Actor</b></td><td colspan="2">ITS-S, receiving V-ITS-Ss.</td></tr>
<tr><td colspan="2"><b>Description</b></td><td colspan="2">ITS-S broadcasts periodically Full CTL messages stored locally on short-range wireless communication.</td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="2">ITS-S has received from the CPOC the latest updated Full CTL of sequence number ctlSequence and has checked its validity before re-transmitting and/or ITS-S has received from its Distribution Centre (DC) the latest Full CTL of sequence number ctlSequence and has checked its validity before forwarding.</td></tr>
<tr><td colspan="2"><b>Success End Condition</b></td><td colspan="2">receiving V-ITS-Ss in the communication range received all the segments of the full CTL (see note 3) and were able to reassemble the complete full CTL message and to update their ECTL/CTL (i.e. the received FullCTL has a ctlSequence higher than the current base ECTL/CTL).</td></tr>
<tr><td colspan="2"><b>Failed End Condition</b></td><td colspan="2">V-ITS-Ss did not receive the Full ECTL/CTL distributed by the ITS-S.</td></tr>
<tr><td colspan="2"><b>Involved components</b></td><td colspan="2">CtlDistribution application and local data base in ITS-S, Security layer, GN, ITS Access Layer, available ITS channel for CTL broadcasting.</td></tr>
<tr><td colspan="2"><b>Main Success Scenario</b></td><td colspan="2">1) V-ITS-S is within radio communication range of the sending ITS-S.
2) ITS-S periodically broadcasts Full CTL messages using GeoNetworking (single hop broadcast) with frequency f (transmission rate should be lower than CAM transmission rate if a safety channel is used and should be reduced or even stopped based on the current channel congestion level). ITS-S broadcasts Full CTL messages for a duration of d days upon reception. The broadcast stops if the Full CTL is expired, or if the sending ITS-S receives a new Full CTL or if the ITS-S detects that another ITS-S is broadcasting the same Full CTL.
3) V-ITS-S receives a Full CTL message, checks its signature validity and its parameter value (issuer identifier, sequence number, type of CTL format, nextUpdate) then stores it in a storage memory.</td></tr>
<tr><td colspan="2"><b>Extensions</b></td><td colspan="2">-</td></tr>
<tr><td colspan="2"><b>Variations (Alternatives)</b></td><td colspan="2">If the Main Success Scenario does not work for any reason, the V-ITS-S may try to request the base CTL to the CPOC/DC using any of the available communication types (e.g. cellular, WLAN, diagnostic system at a garage, localized short-range communication via a R-ITS-S, etc.). The communication profile is specified in ETSI TS 102 941 [2], clause D.1.</td></tr>
<tr><td colspan="2"><b>Includes</b></td><td colspan="2">-</td></tr>
<tr><td colspan="4"><b>Security Characteristics</b></td></tr>
<tr><td>Authentication</td><td>Yes</td><td>Integrity</td><td>Yes</td></tr>
<tr><td>Confidentiality</td><td>No</td><td>Authorization</td><td>Yes</td></tr>
<tr><td>Anonymity privacy</td><td>No</td><td>Pseudonymity privacy</td><td>No</td></tr>
<tr><td>Availability</td><td>Yes</td><td>Plausibility</td><td>No</td></tr>
<tr><td>Auditability (Accountability)</td><td>Yes</td><td>Jurisdictional Access</td><td>-</td></tr>
</table>

NOTE 1: The R-ITS-S may distribute the Delta or Full CTL issued by its own RCA (home PKI) in order to update all passing mobile ITS-Ss belonging to the same PKI (home PKI). It may also offer the same distribution service described in this use case for the distribution of Delta or Full CTLs from other PKIs depending on the stakeholders' business model. For instance, in a trans-European CORRIDOR where the motorways are crossing several countries, the motorway operator may provide distribution of CTL or CRL from other PKIs, i.e. national authorities or private organizations (car manufacturers or device operators).

NOTE 2: f and d values need to be defined. Examples of values are f = 500 mHz, d = 7 days.

NOTE 3: As the full CTL is a large data file whose size may be higher than the maximum payload size allowed in a packet, the sending ITS-S applies segmentation and transmits the full CTL content in one or more consecutive segments (including the associated segmentation information). The max segment size (m) is limited by the network Maximum Transmission Unit (MTU) and depends of the underlying network and MAC layers. The payload containing the FullCTL is split in N_{total} segment such as N_{total}-1 x m < CTL size <= N_{total} x m

4.2.1.7 UC-SEC-11: Delay-tolerant peer-2-peer FullCTL distribution

Use Case ID:	***UC-SEC-11***
Use Case Name:	Delay-tolerant peer-2-peer DeltaCTL distribution.
Priority:	Mandatory.
Related Requirement:	ITS-S (neighbour) has received from the CPOC or from the DC the latest updated (E)CTL and has checked its validity. ITS-S is providing a memory storage to store FullCtl messages issued by a TLM and/or FullCtl messages issued by its own RCA. ITS-S has an available V-ITS-S present in the radio range.

Primary Actor	ITS-S (neighbours), Requesting V-ITS-Ss.
Description	V-ITS-S requests the latest FullCtl to the ITS-Ss present in the radio range.
Preconditions	ITS-S has received from the CPOC the latest updated Full ECTL (of sequence number: ctlSequence or higher) and/or ITS-S has received from its Distribution Centre (DC) the latest updated Full CTL (of sequence number: ctlSequence or higher).
Success End Condition	V-ITS-S received all the consecutive segments containing the latest Full (E)CTL, was able to rebuild the Full (E)CTL of sequence number ctlSequence or higher, and to check its validity and store it in its local memory storage.
Failed End Condition	V-ITS-S did not receive the requested Full (E)CTL.
Involved components	CtlDistribution application and local data base in V-ITS-S, Security layer, GN, ITS Access Layer.
Main Success Scenario	1) V-ITS-S sends a request to get the latest updated FullCtl to ITS-Ss (ITS-S neighbours) present in the radio range. 2) ITS-S neighbour returns the consecutive segments containing the FullCtl. 3) V-ITS-S receives the consecutive segments containing the FullCtl, rebuild the FullCtl from the N_{total} segments, checks its signature validity and its parameter value (issuer identifier, sequence number, type of CTL format, nextUpdate), then stores it in its memory storage.
Extensions	If a receiving V-ITS-S did not receive all the segments constituting the FullCtl, it may request the missing segment(s) to the sending neighbour ITS-S.
Variations (Alternatives)	If the Main Success Scenario does not work for any reason, the V-ITS-S may resume the Full (E)CTL or the Delta (E)CTL Peer-2-peer request after a given time-out or it will try to request Full (E)CTL as described in UC-SEC-03 or request the Delta (E)CTL as described in UC-SEC-04.
Includes	**-**

Security Characteristics			
Authentication	Yes	Integrity	Yes
Confidentiality	No	Authorization	Yes
Anonymity privacy	-	Pseudonymity privacy	-
Availability	Yes	Plausibility	No
Auditability (Accountability)	Yes	Jurisdictional Access	-

NOTE: The ECTL/CTL request message may use an in-band protocol mechanism using the periodically broadcast messages (e.g. carried by a secured CAMs) using the security Header Info extension mechanism specified in ETSI TS 103 097 [3].

4.2.1.8 Use cases and communication profiles mapping

Table 2 summarizes the communication profiles that can be used for each use case. Details of the communication profiles are provided in clause 6.

Table 2: Mapping between use cases and communication profiles

	CPS_001	CPS_002	CPS_003	CPS_004
UC-SEC-03	X	X		
UC-SEC-04	X	X		
UC-SEC-05			X	
UC-SEC-06			X	
UC-SEC-10			X	
UC-SEC-11			X	

NOTE: The communication profiles defined for use cases UC-SEC-06 and UC-SEC-11 in table 2 are applicable for the ITS-S responder in the peer-to-peer distribution service. The request can be attached to any Facilities Layer message using the security Header Info extension mechanism specified in ETSI TS 103 097 [3].

4.2.2 Requirements

4.2.2.1 System requirements

The system requirements for this service are as follows:

- Notification of trust list information: the system shall notify explicitly or implicitly to every entities of the C-ITS trust domain all updated trust list information (CTL, CRL) which are necessary for their correct operation (e.g. in their operation context such as time, space).

- Efficiency: the system shall provide an efficient trust list distribution that enables fast update of the trust list information while limiting the communication overhead and the use of computational resources. Allocation of a small amount of bandwidth shall be sufficient to distribute the trust list information to all trusted ITS entities in a timely manner.

4.2.2.2 Security requirements

The PKI management protocols shall satisfy the following basic set of security objectives:

- **Authentication/authorization control:** authentication consists to be sure of the identity which sends data. Authorization control is the verification of an access policy, based on a trusted authentication. Authenticate all entities participating in the protocol is required to prevent illegitimate persons to enter in the system, or to access some unauthorized resources or services.

- **Integrity:** the integrity of all transmitted data is important to ensure that the contents of the received data are not altered.

- **Availability:** access to and the operation of services by authorized users should not be prevented by malicious activity within the ITS-S environment.

The following list gives the basic set of security objectives which do not require to be satisfied by the PKI management protocols:

- **Confidentiality/Privacy:** data should only be accessed by authorized entities. The real identity of ITS Station has to be protected, by cryptographic mechanisms and depending on the type of data sent.

4.3 CRL distribution service

4.3.1 Service description

4.3.1.1 Overview

Within the CCMS framework, the CRL is generated and issued by the Root CA and published by a DC to be made available to all the participants of the trusted C-ITS system, as specified in ETSI TS 102 940 [1]. The issuance of a new CRL should be done periodically as well as on specific conditions triggered by a security management event or a security incident such as the revocation of an entity of the CCMS.

For each update of the CRL issued by a Root CA, the Root CA shall provide to its DC the CRL information as specified in ETSI TS 102 941 [2], with thisUpdate field set to the time when generating the new CRL by the RootCA. The generation time (thisUpdate) of the new CRL shall be after the generation time of the previous CRL and the nextUpdate time shall be equal or after the one in the previous CRL issued by the Root CA.

The receiving C-ITS stations shall maintain and store the latest certificate revocation lists to apply signature and certificate chain validation on received messages as specified in ETSI TS 103 097 [3]. The transmission and distribution process of certificate revocation lists to all the C-ITS stations and to the CCMS entities should be provided efficiently and in a timely manner.

In case a CRL is outdated and the ITS-S is not able to receive the updated CRL (due to communication problem), the ITS-S should try another communication profile. If the problem persists, the ITS-S enters a fail operational mode. In such mode, the vehicle continues receiving messages. An alert that the revocation information is not available, should be raised.

For interoperability purpose, ETSI TS 102 941 [2] specifies the interface with the DC to distribute the CRL information. In ETSI TS 102 941 [2] (clause D.1), a basic mandatory protocol is specified using HTTP v1.1 GET. Other optional protocols may be proposed e.g. for broadcasting over a short-range wireless communication or other radio broadcasting technologies (e.g. LTE, 5G, satellite or terrestrial broadcast system).

4.3.1.2 UC-SEC-07: On demand request of a CRL

This use case allows an ITS-S to update a certificate revocation list information by requesting the CRL to the DC (which distributes the CRL published by a RCA).

In this use case, the ITS-S shall use the communication profile as specified in ETSI TS 102 941 [2], clause D.2. It is agnostic from the underlying communication medium.

Use Case ID:	***UC-SEC-07***
Use Case Name:	On demand Certificate Revocation List request.
Priority:	Mandatory.
Related Requirement:	ITS-S stores DC access point received at initialization or via the prior base ECTL or CTL. ITS-S has an available cellular network connection (3G/4G, LTE or 5G NR) or a short-range wireless interface to a RSU providing internet communication.

Primary Actor	ITS station.
Description	ITS Station wants to update its revocation list, published by the DC, signed by its own Root CA or by another Root CAs.
Preconditions	-
Success End Condition	ITS station received the latest CRL and was able to check its validity and store it in its local secure memory storage.
Failed End Condition	-
Involved components	DC, Security layer, HTTP over TCP-IP, cellular or short-range wireless communication via a R-ITS-S connected to Internet.
Main Success Scenario	1) ITS Station sends request to DC. The communication profile is specified in ETSI TS 102 941 [2], clause D.2. 2) DC returns CRL.
Extensions	-
Variations (Alternatives)	-
Includes	-

Security Characteristics			
Authentication	Yes	Integrity	Yes
Confidentiality	No	Authorization	-
Anonymity privacy	-	Pseudonymity privacy	-
Availability	Yes	Plausibility	No
Auditability (Accountability)	No	Jurisdictional Access	-

4.3.1.3 UC-SEC-08: ITS-S based CRL distribution

This use case allows end-entities such as R-ITS-S or V-ITS-S to broadcast the certificate revocation list information (signed by the RCA) to all the participants of the trusted C-ITS system using their short-range wireless communication interface.

Use Case ID:	***UC-SEC-08***
Use Case Name:	ITS-S based Certificate Revocation List distribution.
Priority:	Mandatory for R-ITS-S, Optional for V-ITS-S.
Related Requirement:	ITS-S stores DC access point received at initialization or via the prior base ECTL or CTL. ITS-S has an available cellular network connection (3G/4G, LTE or 5G NR).

Primary Actor	ITS-S, receiving V-ITS-Ss.
Description	ITS-S receives a new CRL signed by the RCA and wants to broadcast the update to all the ITS-S within its radio coverage.
Preconditions	-
Success End Condition	Receiving V-ITS-Ss within the coverage of the sending ITS-S has received the latest CRL and was able to check its validity and store it in its local secure memory storage.
Failed End Condition	-
Involved components	CtlDistribution application and local data base in ITS-S, Security layer, GN, IEEE 802.11 [i.1], available radio channel for CRL broadcasting.
Main Success Scenario	1) ITS-S broadcasts CRL update via available communication profile. The communication profile is specified in ETSI TS 102 941 [2], clause D.3. 2) ITS-S receives the CRL.
Extensions	-
Variations (Alternatives)	-
Includes	-

Security Characteristics			
Authentication	Yes	Integrity	Yes
Confidentiality	-	Authorization	-
Anonymity privacy	-	Pseudonymity privacy	-
Availability	Yes	Plausibility	No
Auditability (Accountability)	No	Jurisdictional Access	-

4.3.1.4 UC-SEC-09: Delay-tolerant peer-2-peer CRL distribution

Use Case ID:	***UC-SEC-09***
Use Case Name:	Delay-tolerant peer-2-peer CRL distribution.
Priority:	Mandatory.
Related Requirement:	ITS-S (neighbour) has received from the DC an updated CRL and has checked its validity. ITS-S is providing a memory storage to store CRL messages issued by a DC. ITS-S has an available ITS-S present in the radio range.

<table>
<tr><td><b>Primary Actor</b></td><td colspan="3">ITS-S (neighbours), Requesting V-ITS-Ss.</td></tr>
<tr><td><b>Description</b></td><td colspan="3">V-ITS-S requests the latest CRL updated & signed by its own Root CA or by another Root CA to the ITS-Ss present in the radio range.</td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">ITS-S has received from the DC of its own Root CA (or of another Root CA) the latest updated CRL issued by its Root CA (or another Root CA).</td></tr>
<tr><td><b>Success End Condition</b></td><td colspan="3">Receiving V-ITS-Ss within the coverage of the sending ITS-S has received the latest CRL and was able to check its validity and store it in its local secure memory storage.</td></tr>
<tr><td><b>Failed End Condition</b></td><td colspan="3">V-ITS-S did not receive the requested updated CRL or no ITS-S in the neighbourhood answered or no new updated CRL was available.</td></tr>
<tr><td><b>Involved components</b></td><td colspan="3">CrlDistribution application and local data base in V-ITS-S, Security layer, GN, IEEE 802.11 [i.1].</td></tr>
<tr><td><b>Main Success Scenario</b></td><td colspan="3">1) V-ITS-S sends a request to get the CRL of thisUpdate time higher than the previous CRL generation time to ITS-Ss neighbours present in the radio range.
2) ITS-S neighbour returns the updated CRL if thisupdateTime is higher than the generation time set in the request.
3) V-ITS-S receives a CRL message, checks its validity and its then stores it in its memory storage.
4) Using the received CRL, the receiving V-ITS-S updates its revocation information used for the revocation process (list of trust anchors TAs such as the list of trusted Root CAs, its own EA or AA certificates…) and stores them in a secure memory.</td></tr>
<tr><td><b>Extensions</b></td><td colspan="3">If the Main Success Scenario does not work for any reason, the V-ITS-S may resume the CRL request after a given time-out or it will try to request CRL as described in UC-SEC-07.</td></tr>
<tr><td><b>Variations (Alternatives)</b></td><td colspan="3"></td></tr>
<tr><td><b>Includes</b></td><td colspan="3">-</td></tr>
<tr><td colspan="4"><b>Security Characteristics</b></td></tr>
<tr><td>Authentication</td><td>Yes</td><td>Integrity</td><td>Yes</td></tr>
<tr><td>Confidentiality</td><td>No</td><td>Authorization</td><td>Yes</td></tr>
<tr><td>Anonymity privacy</td><td>-</td><td>Pseudonymity privacy</td><td>-</td></tr>
<tr><td>Availability</td><td>Yes</td><td>Plausibility</td><td>No</td></tr>
<tr><td>Auditability (Accountability)</td><td>Yes</td><td>Jurisdictional Access</td><td>-</td></tr>
</table>

4.3.1.5 Use cases and communication profiles mapping

Table 3 summarizes the communication profiles that can be used for each use case. Details of the communication profiles are provided in clause 6.

Table 3: Mapping between use cases and communication profiles

	CPS_001	**CPS_002**	**CPS_003**	**CPS_004**
UC-SEC-07	X	X		
UC-SEC-08			X	
UC-SEC-09			X	

NOTE: The communication profiles defined for use cases UC-SEC-09 in table 3 are applicable for the ITS-S responder in the peer-to-peer distribution service. The request can be attached to any Facilities Layer message using the security Header Info extension mechanism specified in ETSI TS 103 097 [3].

4.3.2 Requirements

4.3.2.1 System requirements

The system requirements for this service are as follows:

- Notification of trust list information: the system shall notify explicitly or implicitly to every entities of the C-ITS trust domain all updated trust list information (CTL, CRL) which are necessary for their correct operation (e.g. in their operation context such as time, space).
- Efficiency: the system shall provide an efficient trust list distribution that enables fast update of the trust list information while limiting the communication overhead and the use of computational resources. Allocation of a small amount of bandwidth shall be sufficient to distribute the trust list information to all trusted ITS entities in a timely manner.

4.3.2.2 Security requirements

The following list gives the basic set of security objectives which should be satisfied by the PKI management protocols:

- **Authentication/authorization control:** authentication consists to be sure of the identity which sends data. Authorization control is the verification of an access policy, based on a trusted authentication. Authenticate all entities participating in the protocol is required to prevent illegitimate persons to enter in the system, or to access some unauthorized resources or services.
- **Integrity:** the integrity of all transmitted data is important to ensure that the contents of the received data are not altered.
- **Availability:** access to and the operation of services by authorized users should not be prevented by malicious activity within the ITS-S environment.

The following list gives the basic set of security objectives which do not require to be satisfied by the PKI management protocols:

- **Confidentiality/Privacy:** data should only be accessed by authorized entities. The real identity of ITS Station has to be protected, by cryptographic mechanisms and depending on the type of data sent.

5 Use cases specific protocols description

5.1 Enrolment Management with repetition mechanism

5.1.1 EC retry overview

The EC retry aims at managing the failure of EC request or EC response service. The ITS-S shall be able to re-send an EC request following the EC request/response service specified in ETSI TS 102 941 [2], clause 6.2.3.2 and by using the same cryptographic key (session encryption key) used for the first transmission of the EC request. The service failure may be either due to a communication problem, a network congestion or a server overload/breakdown. It may result either in EC request loss or in EC response loss. The service shall be mandatory for all ITS-S (Vehicle ITS-S or Roadside ITS-S).

5.1.2 EC retry protocol

The EC retry service shall provide repetition mechanism in case of a loss of the EC request or the EC response and shall include the following functionalities:

- When the requesting ITS-S initiates an EC request, it creates and stores the EnrolmentRequest message as specified in ETSI TS 102 941 [2], clause 6.2.3.2.1.

- The ITS-S repeats the same EnrolmentRequest message which it has generated and sent for the first attempt of the EC request service until it receives the corresponding EC response (with either positive or negative response code).

- As specified in ETSI TS 102 941 [2], clause 6.2.0.2, at each generation of a new EnrolmentRequest message, the request initiator shall generate a new AES symmetric key k which is used to encrypt the EnrolmentRequest and shall store it in memory until it receives and processes the corresponding EnrolmentResponse message. The request initiator shall erase the encryption symmetric key (k) in memory when one of the following conditions is fulfilled:

    - Case 1: It receives successfully the EnrolmentResponse.

    - Case 2: It does not receive successfully the EnrolmentResponse and the maximum number of retries is reached (N1) or the maximum waiting time is elapsed (TH2).

NOTE: In ETSI TS 102 941 [2], the exception case (case 2) is not fully specified. The present document provides the complete specification for both cases.

The EC Retry service specified in this clause is related to use case UC-SEC-01 and provides the EC retry mechanism in case of a failed request.

- To allow the re-sending of the EC response in case the EC response was lost, the Enrolment Authority shall have the capabilities to store the context information for each new received EC Request: the EA computes and stores the hash of the EC Request received from the ITS-S (`requestHash`) as specified in ETSI TS 102 941 [2], clause 6.2.3.2.2 and the generated EC response (`EnrolmentResponseMessage`). Two options are considered:

    - the PKI is maintaining cache information on the received requests information for a maximum time duration (TH3);

    - the PKI is retrieving the generated EC by accessing its own data base where the information on the previous incoming EC requests is stored.

5.1.3 Message and version

The message used in EC request/response retry service are the same messages as specified in ETSI TS 102 941 [2], clause 6.2.3.2. The version is unchanged.

5.1.4 EC retry requirements

The EC retry service shall comply to the "Enrolment/Authorization assumption and requirements" defined in ETSI TS 102 941 [2], clause 6.2.2 and support additionally the following requirements:

- The ITS-S shall set a timer T1 (interval between two successive EC requests) to the value TH1. I.e. the end of timer T1 occurs when it reaches the value TH1 (timeout). This timer value (TH1) shall not be smaller than the minimum delay to receive an EC response.

- The specification of TH1 should also take into account the time necessary for the ITS-S to establish a network connection as the ITS-S has only intermittent connectivity to the PKI infrastructure (e.g. ITS-S may use short-range communication via a RSU connected to the Internet).

- The ITS-S shall set a second timer T2. The timer value TH2 shall be higher than TH1 x N1 (where N1 is the maximum number of allowed attempts for sending the same EC request).

NOTE 1: Recommended values for the TH2 may be proposed. For instance, this threshold may be set to 60 minutes.

- The ITS-S shall terminate the EC Retry service in both case of success or negative termination (abort) as follows:

    - Case 1: the ITS-S receives the EC response with either positive or negative response code as specified in ETSI TS 102 941 [2], clause 6.2.3.2.2.

  - Case 2: the ITS-S shall abort the procedure when one of the following condition is reached: the maximum number of retries is reached (N1) or the maximum waiting time is elapsed (TH2).

NOTE 2: in case of the EC retry procedure did not succeed (case 2), a recovery procedure may be provided. This recovery procedure is out of scope of the present document.

- The EA shall have the capabilities to support the EC retry protocol:
  - The Enrolment Authority shall start a timer T3 (the time interval it is keeping the context information of the initial EC Request) and shall authorize the resumption of the EC request within a maximum time-interval (TH3). This timer value TH3 shall be higher or equal to the value TH2.
- The EA shall check the validity of the received EC Request as specified in ETSI TS 102 941 [2], clause 6.2.3.2.1. The EA shall check consistency with the generation time of the received EC Request (verification checks in the future and in the past based on the generation time).

NOTE 3: Concerning these consistency checks on the EA, recommended values for the time-interval between the EC Request message generation time and the receiving EA's current time may be proposed. For instance, the time-interval may be comprised between a few seconds in the future and 60 minutes in the past.

- The EA computes the request hash on the received EC request and verifies if the hash of the received EC request already exists in its data base/cache.
- If the timer has not reached maximum threshold TH3, the EA retrieves the EC response already generated corresponding to the computed request hash and resends it to the ITS-S. Otherwise, it sends an EC response with negative response code set to `deniedrequest` (as specified in ETSI TS 102 941 [2], clause A.2.5.1).

5.1.5 Service communication parameter

Service communication parameters are specified in clause 6.1 (CPS_001) and clause 6.2 (CPS_002).

5.2 Authorization Management with repetition mechanism

5.2.1 AT retry overview

The AT retry aims at managing the failure of AT request or AT response service. The ITS-S should be able to re-send an AT request following the AT request/response service specified in ETSI TS 102 941 [2], clause 6.2.3.3 and by using the same cryptographic key (session encryption key) used for the first failed AT request. The failure can be either due to a communication problem, a network congestion or other and the service failure can result either in AT request loss or in AT response loss.

[Itss_NoPrivacy] The ITS-Ss belonging to this category should perform the AT retry mechanism as defined in this clause.

[Itss_WithPrivacy] It shall not be performed by ITS-Stations belonging to the category.

5.2.2 AT retry protocol

The AT Retry service specified in this clause is related to use case UC-SEC-02 and provides the AT retry mechanism in case of a failed end condition.

The AT retry service shall provide repetition mechanism in case of a loss of the AT request or the AT response and shall include the following functionalities:

- When the requesting ITS-S initiates an AT request, it creates and stores the AuthorizationRequest message as specified in ETSI TS 102 941 [2], clause 6.2.3.3.1.
- The ITS-S repeats the same AuthorizationRequest message which it has generated and sent for the first attempt of the AT request service until it receives the corresponding AT response (with either positive or negative response code).

- As specified in ETSI TS 102 941 [2], clause 6.2.0.2, at each generation of a new AuthorizationRequest message, the request initiator shall generate a new AES symmetric key k which is used to encrypt the AuthorizationRequest and shall store it in memory until it receives and processes the corresponding AuthorizationResponse message. The request initiator shall erase the encryption symmetric key (k) in memory when one of the following conditions is fulfilled:
    - Case 1: It receives successfully the AuthorizationResponse.
    - Case 2: It does not receive successfully the AuthorizationResponse and the maximum number of retries is reached (N2) or the maximum waiting time is elapsed (T4_requestID).
- For each new generated AuthorizationRequest, the requesting ITS-S shall compute and store the `requestHash` of the AuthorizationRequest message as specified in ETSI TS 102 941 [2], clause 6.2.3.3.2 and shall use this request hash value as the request identifier (requestID). The requesting ITS-S shall start a different set of counters (N2_requestID) and timers (T4_requestID and T5_requestID) per each parallel request.

NOTE: Many Authorization Tickets can be requested in parallel.

- To allow the re-sending of the AT response in case the AT response was lost, the Authorization Authority shall have the capabilities to store the context information for each new received AT Request: the AA computes and stores the hash of the AT Request received from the ITS-S (`requestHash`) as specified in ETSI TS 102 941 [2], clause 6.2.3.2.2 and the generated AT response (`AuthorizationResponseMessage`). Two options are considered:
    - the PKI is maintaining cache information on the received requests information for a maximum time duration (timer T6 set to value TH6);
    - the PKI is retrieving the generated AT by accessing its own data base where the information on the previous incoming AT requests is stored.

5.2.3 Message and version

The message used in AT request/response retry service are the same messages as specified in ETSI TS 102 941 [2], clause 6.2.3.3. The version is unchanged.

5.2.4 AT retry requirements

The AT retry service shall comply to the "Enrolment/Authorization assumption and requirements" defined in ETSI TS 102 941 [2], clause 6.2.2 and support additionally the following requirements:

- The ITS-S shall set a timer T4_requestID (time interval before repeating an AT request) to the value TH4. I.e. the end of timer T4 occurs when it reaches the value TH4 (timeout). This timer value (TH4) should not be smaller than the minimum delay to receive an AT response (Round-trip time).
- The specification of TH4 should also take into account the time necessary for the ITS-S to establish a network connection as the ITS-S has only intermittent connectivity to the PKI infrastructure (e.g. ITS-S may use short-range communication via a RSU connected to the Internet).
- The ITS-S shall set a second timer T5_requestID. The timer value TH5 shall be higher than TH5 x N2 (where N2 is the maximum number of allowed attempts for sending the same AT request).

NOTE 1: Recommended values for the TH5 may be proposed. For instance, this threshold may be set to 60 minutes.

- The ITS-S shall terminate the AT Retry service in both case of success or negative termination (abort) as follows:
    - Case 1: the ITS-S receives the AT response with either positive or negative response code as specified in ETSI TS 102 941 [2], clause 6.2.3.3.2.
    - Case 2: the ITS-S shall abort the procedure when one of the following condition is reached: the maximum number of retries is reached (N2) or the maximum waiting time is elapsed (TH5).

NOTE 2: in case of the AT retry procedure did not succeed (case 2), a recovery procedure may be provided. This recovery procedure is out of scope of the present document.

- The AA shall have the capabilities to support the AT retry protocol:
  - The Authorization Authority shall start a timer T6_requestID (the time interval it is keeping the context information of the initial AT Request) and shall authorize the resumption of the AT request within a maximum time-interval (TH6). This timer value TH6 shall be higher or equal to the value TH2.
- The AA shall check the validity of the received AT Request as specified in ETSI TS 102 941 [2], clause 6.2.3.2.1. The AA shall check consistency with the generation time of the received AT Request (verification checks in the future and in the past based on the generation time).

NOTE 3: Concerning these consistency checks on the AA, recommended values for the time-interval between the AT Request message generation time and the receiving AA's current time may be proposed. For instance, the time-interval may be comprised between a few seconds in the future and 60 minutes in the past.

- The AA computes the request hash on the received AT request and verifies if the hash of the received AT request already exists in its data base/cache.
- If the timer has not reached maximum threshold TH6, the AA retrieves the AT response already generated corresponding to the computed request hash and resends it to the ITS-S. Otherwise, it sends an AT response with negative response code set to `deniedrequest` (as specified in ETSI TS 102 941 [2], clause A.2.5.2).

5.3 Peer-to-peer CRL/CTL distribution protocol

5.3.1 Overview

The present document specifies the Peer-to-Peer CRL/CTL Distribution (P2PCXLD) service.

This service refers to Security Management or Facilities Layer entities that provide the CRL, DeltaCTL and FullCTL distribution service as defined in Use Cases UC-SEC-O5, UC-SEC-O6 and UC-SEC-O8 to UC-SEC-11. It allows to manage the generation, transmission and reception of Security Management messages (SM-PDU) from an ITS-S to other ITS-Ss. It is specified in clauses 5.3, 5.4 and 5.5.

Clause 5.3 specifies the requirements to enable an ITS-S to request a new updated CRL, FullCTL or DeltaCTL which is known to be issued or is identified as a more recent update by this ITS-S. Clauses 5.4 and 5.5 detail the requirements for the transmission of the CRL or the CTL information by an ITS-S which wants to share its latest update.

To provide the peer-to-peer distribution service, the ITS-Ss shall provide the following capabilities:

- The ITS-S requester shall provide functionalities to add a missing CRL/CTL request field using the ETSI originating's Header Info extension specified in ETSI TS 103 097 [3] clause 4.2.2, which is inserted in a transmitted secure F-PDU (e.g. a CAM, etc.) to request other ITS-Ss to provide the missing CRL/CTL and to receive the response using the in-band communication (short-range communication via a ITS 5,9 GHz channel, e.g. SCH).

NOTE: For the purpose of peer-to-peer distribution of CTL and CRL, the ETSI TC ITS group has specified three extensions in its reserved contributed extension block: `etsiTs102941CrlRequest`, `etsiTs102941DeltaCtlRequest` and `etsiTs102941FullCtlRequest`.

- The neighbour ITS-Ss which receive a missing CRL/DeltaCTL request from the requesting ITS-S shall provide the functionalities of CRL/CTL Broadcasting service, shall search the requested information via its local CTL/CRL Distribution Application (CXLDA)'s memory storage and shall start the broadcasting of the corresponding response if available using the in-band communication (short-range communication via a ITS 5,9 GHz channel, e.g. SCH). The ITS-S responders shall stop to broadcast the response when either they reach some predefined sending conditions or detect other responders ITS-Ss which broadcast exactly the same response. The response mechanism does not use a specific response message or a response appended to the transmitted F-PDUs (e.g. a CAM, etc.) of the responder, but uses the same S-PDU format as specified in ETSI TS 102 941 [2], clause 6.3.

- The neighbour ITS-Ss which receive a missing Full CTL request from the requesting ITS-S shall provide the functionalities of exchanging large data file using a message broadcasting communication service which allows to transmit large response message in several pieces (called segments). The responder ITS-S shall search the latest known Full CTL information via its local CTL/CRL Distribution Application's memory storage and it shall start the broadcasting of the corresponding response only if the stored Full CTL is more recent than the one indicated in the request using the in-band communication (short-range communication via a ITS 5,9 GHz channel, e.g. SCH). The ITS-S responders shall stop to broadcast the response when either they reach some predefined sending conditions or detect other responder ITS-Ss which broadcast the same CTL identified by its CTL identifier computed as the output of the SHA-256 of the CTL message. The response mechanism uses a specific PDU called Segmented CTL Response Message (SCRM) which is specified in the present document (Annex D).

The peer-to-peer CRL/CTL distribution service is a combination of functionalities provided by an ITS-S requesting a missing trust list information (requester role) and of functionalities provided by other ITS-Ss which receive the missing CRL/DeltaCTL request and start to broadcast the corresponding response (responder role).

It combines ITS-S based broadcast service such as described in UC-SEC-05, UC-SEC-08 and UC-SEC-10 and the peer-2-peer distribution functionality (Requester role) as described in UC-SEC-06, UC-SEC-09 and UC-SEC-11 thus allowing to fulfil the service.

This CRL/DetaCTL distribution mechanism should enable to provide an efficient, scalable approach for trust lists distribution with notification of newly issued CTL/CRL to the ITS-Ss.

The detailed P2P distribution service requirements for the Requester role are given in clause 5.3.4. The detailed specification and requirements for the Responder role are given in clause 5.4.

5.3.2 Peer-to-peer CRL/CTL request/response protocol

The Peer-to-peer CRL/CTL distribution (P2PCXLD) service shall provide the communication service for the support of transmission of requests/reception of responses using the in-band message communication and provide the following functionalities:

- Generation of a secured F-PDU (e.g. CAM) inserting a single request to get the next updated version of the DeltaECTL issued by the TLM. The request shall indicate the `ctlSequence` value of the last valid received or rebuilt ECTL by the ITS-S requester.

- Generation of a secured F-PDU (e.g. CAM) inserting a single request to get the next updated version of the DeltaCTL issued by its own RCA identified by its Certificate Identifier (HashedId8). The request shall indicate the `ctlSequence` value of the last valid received or rebuilt CTL of its RCA by the requester.

- Generation of a secured F-PDU (e.g. CAM) inserting a single request to get the next updated version of the CRL issued by its own RCA or by another trusted Root CA identified by its Certificate Identifier (HashedId8). The request shall indicate the `thisUpdate` value of the last received CRL of the identified RCA by the requester.

- Generation of a secured F-PDU (e.g. CAM) inserting a single request to get the next updated version of the Full CTL issued by the TLM or by a RCA. The request shall indicate the `ctlSequence` value of the last valid received or rebuilt ECTL/CTL by the ITS-S requester.

- Reception of the response message which may be broadcasted by a neighbour ITS-S which has the DeltaCTL corresponding to the next version of the requested CTL (its sequence number is equal to `ctlSequence` +1) or has a more recent version of the requested CRL (its value of `thisUpdate` is higher than the one received in the request). The requested CRL/DeltaCTL are included directly in GN packets transmitted by the triggered ITS-S using the same communication medium, i.e. an ITS safety or non-safety channel.

If the requested information is a CRL or a DeltaCTL, the response message sent by an ITS-S Responder is consisting of a SM-PDU of one of the following data formats as specified in ETSI TS 102 941 [2], clause A.2:

- `TlmCertificateTrustListMessage` containing a `certificateTrustListTlm` of type `DeltaCtl`,

- `RcaCertificateTrustListMessage` containing a `certificateTrustListRca` of type `DeltaCtl`,

- `CertificateRevocationListMessage` containing a `certificateRevocationList.`

If the requested information is a Full CTL, the response messages sent by an ITS-S Responder are consisting of SM-PDUs of the following data format as specified in clause 5.5.3:

- `SegmentedCtlResponseMessage`, a specific `SegmentPDU` containing a segment of the CTL to be transmitted which shall fit to the MTU constraints of the Network/transport layer.

The Peer-to-peer response service for CRL and Delta CTL is specified in clause 5.4.2. The Peer-to-peer response service for the Full CTL is specified in clause 5.5.2.

5.3.3 Message and version

The ITS-S Responder which initiates the Broadcast service shall use the response message format corresponding to the request (see clause 5.4.3).

5.3.4 Peer-to-peer CRL/CTL request message

5.3.4.1 General

This clause specifies the ITS-S requester functionalities to support the Peer-to-Peer CRL/CTL Request service using the Short-Range communication profile over a ITS safety or non-safety channel (CPS_003).

The ITS-S requesting a new updated CRL DeltaCTL, or FullCTL shall use the corresponding ContributedExtensions fields (and precisely the ETSI originating extension fields) in the `HeaderInfo` of the `EtsiTs103097Data` which contains a `SignedData` structure as specified in ETSI TS 103 097 [3]. See table 4.

The requesting ITS-S starts to transmit P2P CRL/CTL Distribution (P2PCXLD) request inserted in the secured F-PDU (e.g. CAM, etc.) under precise trigger conditions which are specified in clause 5.3.6.

Table 4: HeaderInfo with contributed extensions of type ETSI originating headerInfo extensions

```
HeaderInfo ::= SEQUENCE  {
    psid                       Psid,
    generationTime             Time64 OPTIONAL,
    expiryTime                 Time64  OPTIONAL,
    generationLocation         ThreeDLocation OPTIONAL,
    p2pcdLearningRequest       HashedId3 OPTIONAL,
    missingCrlIdentifier       MissingCrlIdentifier OPTIONAL,
    encryptionKey              EncryptionKey OPTIOI,
    ...,
    inlineP2pcdRequest         SequenceOfHashedId3 OPTIONAL,
    requestedCertificate       Certificate OPTIONAL,
    reserved                   INTEGER (0..255) OPTIONAL,
    contributedExtensions      ContributedExtensionBlocks OPTIONAL }
```

NOTE: Table 4 is provided for better readability, but is illustrative in the present document. The ASN.1 description of HeaderInfo component is specified in ETSI TS 103 097 [3], clause A.2.2.

Clause 5.3.4.2 specifies the requirements for the ITS-S generating a P2P CRL request. Clause 5.3.4.3 specifies the requirements for the ITS-S generating a P2P Delta CTL request. Clause 5.3.4.4 specifies the requirements for the ITS-S generating a P2P Full CTL request.

5.3.4.2 Generation of a Peer-to-peer CRL request

To create a Peer-to-peer CRL request, the ITS-S shall follow this process:

- The ITS-S shall select, from its local list of Trust Anchors (TA), the current valid certificate of the RCA which is issuing the requested CRL and shall compute the `issuerId` value as the HashedID8 of this RCA certificate (as specified in ETSI TS 103 097 [3]).

- For the selected issuer (`issuerId`), the ITS-S shall query the local Security Management Entity in charge of managing the received revocation information and shall get the `thisUpdate` time value of the latest received/stored CRL from this issuer. This time value is set to "undefined" if the Security Management Entity has never received revocation information from that issuer.
- An `EtsiTs1030971Data-Signed` structure is built containing: `hashId, tbsData, signer` and `signature`:
    - the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];
    - in the `tbsData`:
        - the `payload` field shall contain the payload of the secured F-PDU (e.g. CAM);
        - in the `headerInfo`:
            - the `psid` shall be set to value assigned for this secured F-PDU as assigned in ETSI TS 102 965 [6];
            - the `generationTime` shall be present;
            - all other components of the component `tbsData.headerInfo` shall be present or absent depending on the profile;
            - the component `contributedExtensions` identified by `HeaderInfoContributorId` set to value `etsiHeaderInfoContributorId` (2) for the ETSI originating extensions shall be present:
                - The Extension identified by ExtId set to value "1" containing the extension `EtsiTs102941CrlRequest` shall be present.
                - In the extension `EtsiTs102941CrlRequest,`the component `issuerId` shall contain the value of the selected Root CA certificate identifier (as specified above). The component `lastKnownUpdate` shall be present if the ITS-S has available the latest `received/stored CRL from this issuer`, containing the value of `thisUpdate` field of the `latest CRL`. The component shall be ABSENT, if this time value is "undefined".
    - the `signer` is declared as `certificate` containing the ITS certificate (AT) or declared as `digest` containing the HashedId8 of the ITS-S certificate (AT);
    - the `signature is` computed as specified in ETSI TS 103 097 [3].

5.3.4.3 Generation of a Peer-to-peer Delta CTL request

To create a Peer-to-peer Delta CTL request, the ITS-S shall follow this process:

- The ITS-S shall select, from its local list of Trust Anchors (TA), the current valid certificate of the RCA which is issuing the requested DeltaCTL and shall compute the `issuerId` value as the HashedID8 of this RCA certificate (as specified in ETSI TS 103 097 [3]).
- For the selected issuer (`issuerId`), the ITS-S shall query the local Security Management Entity in charge of managing the received or rebuilt CTL information and shall get the `ctlSequence` value of the latest stored CTL from this issuer. This sequence value is set to "undefined" if the Security Management Entity has never received CTL information from that issuer.
- An `EtsiTs103097Data-Signed` structure is built containing: `hashId, tbsData, signer` and `signature`:
    - the `hashId` shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];

- in the tbsData:
  - the payload field shall contain the payload of the secured F-PDU (e.g. CAM);
  - in the headerInfo:
    - the psid shall be set to value assigned for this secured F-PDU as assigned in ETSI TS 102 965 [6];
    - the generationTime shall be present;
    - all other components of the component tbsData.headerInfo shall be present or absent depending on the profile;
    - the component contributedExtensions identified by HeaderInfoContributorId set to value etsiHeaderInfoContributorId (2) for the ETSI originating extensions shall be present:
      - The Extension identified by ExtId set to value "2" containing the extension EtsiTs102941DeltaCtlRequest shall be present.
      - In the extension EtsiTs102941DeltaCtlRequest, the component issuerId shall contain the value of the selected Root CA certificate identifier (as specified above). The component lastKnownCtlSequence shall be present if the ITS-S has available the latest received or rebuilt CTL from this issuer, containing the value of ctlSequence field of the latest CTL. The component shall be ABSENT, if this sequence value is "undefined".
- the signer is declared as certificate containing the ITS certificate (AT) or declared as digest containing the HashedId8 of the ITS-S certificate (AT);
- the signature is computed as specified in ETSI TS 103 097 [3].

5.3.4.4 Generation of a Peer-to-peer Full CTL request

To create a Peer-to-peer Full CTL request, the ITS-S shall follow this process:

- The ITS-S shall select, from its local list of Trust Anchors (TA), the current valid certificate of the RCA which is issuing the requested FullCTL and shall compute the issuerId value as the HashedID8 of this RCA certificate (as specified in ETSI TS 103 097 [3]).
- For the selected issuer (issuerId), the ITS-S shall query the local Security Management Entity in charge of managing the received or rebuilt CTL information and shall get the ctlSequence value of the latest stored CTL from this issuer. This sequence value is set to "undefined" if the Security Management Entity has never received CTL information from that issuer.
- An EtsiTs103097Data-Signed structure is built containing: hashId, tbsData, signer and signature:
  - the hashId shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [3];
  - in the tbsData:
    - the payload field shall contain the payload of the secured F-PDU (e.g. CAM);
    - in the headerInfo:
      - the psid shall be set to value assigned for this secured F-PDU as assigned in ETSI TS 102 965 [6];
      - the generationTime shall be present;
      - all other components of the component tbsData.headerInfo shall be present or absent depending on the profile;

  - o the component contributedExtensions identified by HeaderInfoContributorId set to value etsiHeaderInfoContributorId (2) for the ETSI originating extensions shall be present:

    - The Extension identified by ExtId set to value "3" containing the extension EtsiTs102941FullCtlRequest shall be present.

    - In the extension EtsiTs102941FullCtlRequest, the component issuerId shall contain the value of the selected Root CA certificate identifier (as specified above). The component lastKnownCtlSequence shall be present if the ITS-S has available the latest received or rebuilt CTL from this issuer containing the value of ctlSequence field of the latest known CTL. The component shall be ABSENT, if this sequence value is "undefined". The component segmentNumber shall be ABSENT, except if the ITS-S is requesting the repetition of a missing segment which number is contained in the segmentNumber component.

- the signer is declared as certificate containing the ITS certificate (AT) or declared as digest containing the HashedId8 of the ITS-S certificate (AT);

- the signature is computed as specified in ETSI TS 103 097 [3].

5.3.5 Peer-to-peer CRL/CTL response message

Requirements for the ITS-S responder are specified in clause 5.4.

5.3.6 P2P CRL/CTL request message trigger, repetition and termination

The requesting ITS-S shall initiate a P2PCXLD request to get the next updated version of the DeltaCTL issued by the TLM or by its own RCA:

- on a periodic basis depending on rules set by the CP;

- when the ITS-S receives a signed PDU which contains an ETSI originating extension block in the HeaderInfo structure (component of type ContributedExtensionBlock identified by etsiHeaderInfoCntributorId (2)) including an extension of type CTL request (EtsiTs102941DeltaCtlRequest) from another ITS-S and finds out that the value lastKnownCtlSequence associated to the certificate Identifier of the issuer (TLM or RCA) is higher than the sequence number of the CTL of TLM or RCA stored in the ITS-S memory.

The requesting ITS-S shall initiate a P2PCXLD request to get the next updated version of the CRL issued by its own RCA or another RCA:

- when the ITS-S local time is reaching the nextUpdate value set in the last received CRL of the corresponding issuing RCA (identified by its certificate Identifier);

- when the ITS-S receives secured messages from a peer ITS-S using ATs issued by an AA linked to its own RCA or another RCA. The ITS-S shall set the ETSI originating extension block in the HeaderInfo structure (component of type ContributedExtensionBlock identified by etsiHeaderInfoCntributorId (2)) containing an extension of type CRL request (EtsiTs102941CrlRequest) where the value of HashedId3 of the topmost certificate (trust anchor) of the certificate chain built from the AT used by the peer ITS-S and the lastKnownUpdate field is set to thisUpdate value of the CRL stored in the ITS-S memory.

The P2PCXLD request may be repeated after a given time-out.

The P2PCXLD request transmission shall be terminated, if one of the following conditions is reached:

- when the requesting ITS-S receives a response S-PDU which contains the CRL or the DeltaCTL corresponding to the sent request;

- when the ITS-S local time is reaching the time indicated for the next update (nextUpdate value) in its current stored CRL or base CTL corresponding to the issuer's certificate identifier.

5.3.7 Protocol communication parameter

The service communication parameters for the ITS-S requester are depending of the Facilities message (F-PDU) which carries the Peer-to-Peer CTL/CRL request and the service communication parameters for the ITS-S distributor are specified in clause 5.4.4 or 5.5.4.

5.4 ITS-S based CRL/DeltaCTL broadcast protocol

5.4.1 Overview

The ITS-S based CRL/CTL broadcasting service enables an ITS-S to manage the retrieving, the transmission and the reception of the latest available trust list information, i.e. the last known CRL, Delta ECTL or DeltaCTL which shall be repeated by the CRL/CTL broadcasting service of the sending ITS-S at a pre-defined transmission rate (frequency f) and during a maximum time period (duration d).

The ITS-S based CRL/CTL broadcast service is two-fold:

- Case 1: the sending ITS-S starts the broadcast of the last updated CRL issued by its Root CA or the last updated DeltaCTL issued by a Root CA/TLM as described in use cases UC-SEC-05 or UC-SEC-08.
- Case 2: when receiving a Peer-to-Peer CRL/CTL Request from a requesting ITS-S as specified in clause 5.3.1, if the neighbour ITS-S has the current requested `Crl` or `DeltaCtl` available, it starts broadcasting it using the pre-defined frequency f and during the maximum transmission duration d.

This clause is based on ETSI TS 102 941 [2], clause 6.3.5 and lists the requirements for the implementation of the ITS-S based CRL/CTL broadcast service.

5.4.2 CRL/DeltaCTL broadcast protocol

In the case 1, the ITS-S based CRL/CTL broadcast service shall enable the continuous transmission of the latest available trust list information, i.e. the last known CRL or Delta ECTL or DeltaCTL, at a pre-defined transmission rate (frequency f1) and during a maximum time period (duration d1). It starts a timer and when the timer reaches the maximum threshold d1, the ITS-S stops broadcasting the trust list (CRL/CTL).

NOTE 1: As the Certificate Policy in Europe requires that the maximum delay for updating a new issued CRL or CTL for all trusted ITS stations is one week, the recommended values when starting the CRL/CTL distribution (case 1) are set to f1 = 1 Hz, d1 = 1 week.

NOTE 2: An ITS-S implementation may also decrease the transmission rate f1 within the allowed maximum duration d1. E.g. f1 is set to 1 Hz at the start of service, then decrease at a regular time-period e.g. every day, up to a frequency of 0,1 Hz or 0,2 Hz.

When the ITS-S receives a Peer-to-Peer request from a requesting ITS-S (case 2), the ITS-S shall start broadcasting the requested CRL or Delta ECTL or DeltaCTL if it has the requested CRL or Delta ECTL or DeltaCTL with suitable values of frequency (f2) and duration (d2).

NOTE 3: For this specific response scenario to a P2P request, the values f2 and d2 are set to lower values than for the periodic broadcasting case. Examples of values are f2 = 1 Hz, d2 = 10 or 20 seconds.

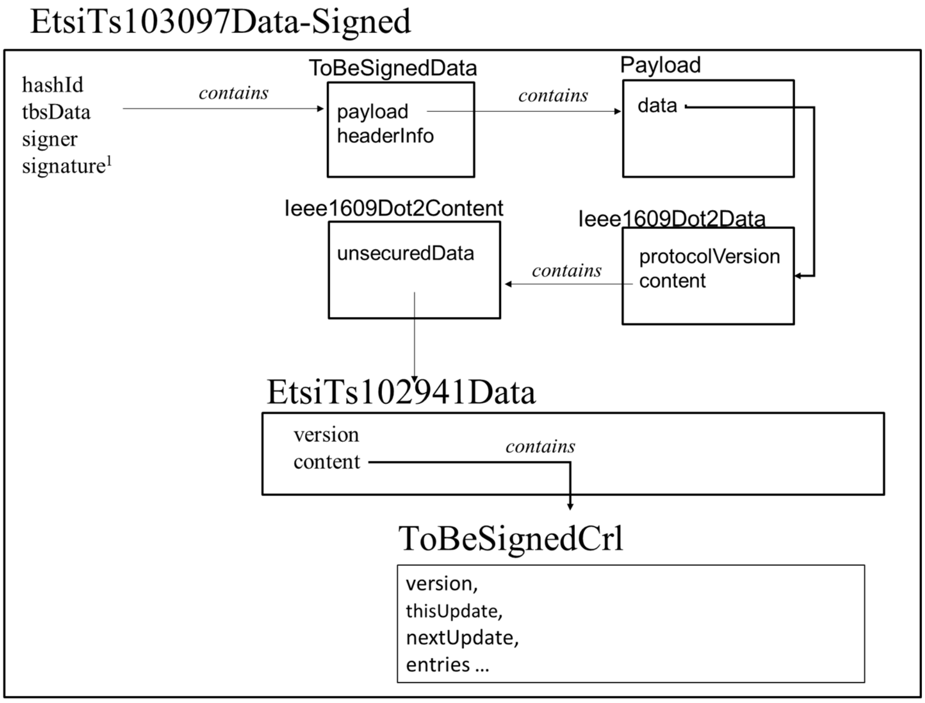
The CRL/CTL Broadcasting service is provided by the CRL/CTL Distribution Application which shall provide:

- At each start of the service, the CRL/CTL Distribution application shall retrieve the requested Crl or DeltaEctl or DeltatCtl issued by the specified issuer (identified by its `issuerId)` for continuous transmission by the sending ITS-S used as a Relay.
- It shall use the Security Processing Services entity to verify the Crl or DeltaEctl or DeltatCtl signature before transmitting it.
- The CRL/CTL Distribution entity shall send the latest valid Crl or DeltaEctl or DeltatCtl via the BTP/GeoNetworking layer using direct short-range access layer.

The GN data services shall be provided via the GN_SAP as specified in ETSI TS 103 836-4-1 [5]. The security profile in the GN-DATA.request is set to unsecure as no additional message signature is performed to the PDU at the GeoNetworking layer.

5.4.3 Message and version

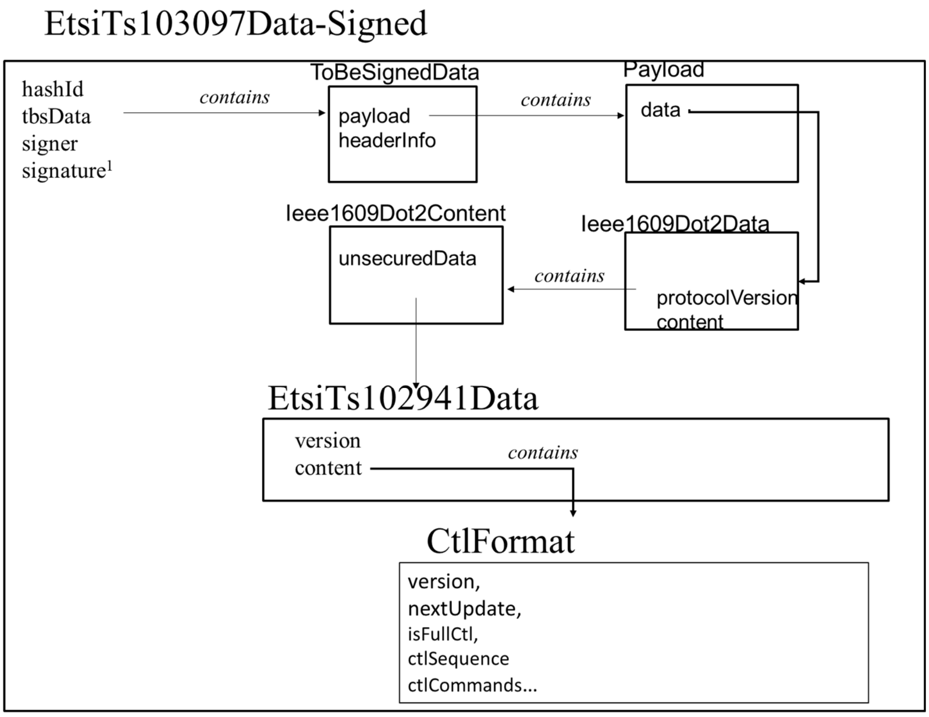
The CRL broadcast service uses the CRL message (`CertificateRevocationListMessage)`as defined in ETSI TS 102 941 [2], clause A.2. The global structure of the CRL is depicted in figure 2.



[1] Signature is computed using the private key corresponding to a valid RCA certificate

Figure 2: CertificateRevocationList Message

The DeltaCTL broadcast service uses the ECTL message (`TlmCertificateTrustListMessage`) or the CTL message (`RcaCertificateTrustListMessage`) with the parameter 'isFullCtl' in CtlFormat set to value FALSE as defined in ETSI TS 102 941 [2], clause A.2.7. The global structure of the CTL is depicted in figure 3.



[1] Signature is computed using the private key corresponding to a valid RCA certificate

Figure 3: Certificate Trust List message

The CRL/CTL Distribution Application (CXLDA) of the sending ITS-S shall start the transmission of a CRL or CTL when one of the following triggering conditions is satisfied:

- The sending ITS-S has received a new updated CRL issued by its own Root CA or another Root CA (under specific B2B contractual agreement) via a Distribution Centre (DC) and starts to broadcast it in order to transmit the updated CRL to all the surrounding ITS-Ss present within the radio communication area (single-hop message broadcasting).

- The sending ITS-S has received a new updated DeltaECTL issued by the TLM (`TlmCertificateTrustListMessage`) or a new updated DeltaCTL issued by its RCA from its DC (`RcaCertificateTrustListMessage`) and starts to broadcast it in order to transmit the updated DeltaCTL to all the surrounding ITS-Ss present within the radio communication area (single-hop message broadcasting).

- The responder ITS-S has received a Peer-to-peer CRL/CTL request and it has available the requested CRL or DeltaECTL or DeltaCTL.

In between two consecutive updates of CRL issued by its own RCA (or another Root CA under specific B2B contractual agreement), a CRL message shall be repeated by the CRL/CTL Distribution Application (CXLDA) of the sending ITS-S at a pre-defined transmission rate (frequency f) in order that new ITS-Ss entering the radio communication area during the CRL message event validity duration may also receive the CRL message (`CertificateRevocationListMessage`). This process is referred to as CRL broadcast service repetition. The CRL broadcast service repetition shall be activated under the request from the CXLDA.

In between two consecutive updates of DelatCTL issued by its own RCA (or DeltaECTL issued by TLM), a DeltaCTL message shall be repeated by the CRL/CTL Distribution Application (CXLDA) of the sending ITS-S at a pre-defined transmission rate (frequency f) in order that new ITS-Ss entering the radio communication area during the DeltaCTL message event validity duration may also receive the DeltaCTL message (`RcaCertificateTrustListMessage)`or the DeltaECTL`(TlmCertificateTrustListMessage`). This process is referred to as CTL broadcast service repetition. The CTL broadcast service repetition shall be activated under the request from the CXLDA.

The CRL/CTL broadcast service termination shall occur at the sending/responder ITS-S when one of the following conditions occurs:

- The sending/responder ITS-S reaches the end of the broadcast event validity period (d).
- The sending/responder ITS-S local time is reaching the time indicated in the field next update (nextUpdate value) in the transmitted CRL or DeltaECTL/DeltaCTL.
- The sending/responder ITS-S has received a new updated version of CRL (with a higher sequence number) or a new updated DeltaECTL/DeltaCTL (with a thisUpdate value which indicates a later date than in the current transmitted DeltaECTL/DeltaCTL).
- The sending/responder ITS-S receives the same update version of the CRL or DeltaECTL/DeltaCTL transmitted by another ITS-S.

NOTE: If the sending/responder ITS-S which started the CRL broadcast service receives a newer update version of the CRL, it stops transmitting the current CRL and it stores it in the application data storage. If the sending/responder ITS-S which started the CTL broadcast service receives a newer update version of the DeltaECTL/DeltaCTL, it stops transmitting the current DeltaECTL/DeltaCTL and it stores it in application data storage.

At service termination, CXLDA shall stop transmission of the CRL or DeltaECTL/DeltaCTL message.

5.4.4 Protocol communication parameter

Service communication parameters are specified in clause 6.3 (CPS_003).

The Port Number values of the transport protocol for the two services (CTL broadcast service and CRL broadcast service) shall be as specified in ETSI TS 103 248 [4].

5.5 ITS-S based Full CTL broadcast protocol

5.5.1 Overview

The ITS-S based full CTL broadcasting service enables an ITS-S to manage the retrieving, the transmission and the reception of the latest available ECTL or CTL which shall be repeated at a pre-defined transmission rate (frequency f) and during a maximum time period (duration d). If the value d is set to 0, there shall be no repetition.

An ITS-S which has received the latest update of an ECTL or CTL can store it in memory and redistribute it to its neighbour ITS-Ss using the CTL Response Message broadcasting protocol in Peer-to-Peer mode: this allows the sharing of large data file and may be especially effective when there is a large number of R-ITS-Ss or of mobile ITS-Ss in the road environment which provide this Full CTL broadcast protocol.

The full CTL may be larger than the size of the Maximum Transmission Unit (MTU) of the lower layers and so the ITS-S based Full CTL broadcasting service shall spread it into multiple pieces using a segmentation mechanism.

The MTU represents the maximum size of a network PDU which can be transmitted on a single MAC frame. The value of MTU depends on the access layer technology and the maximum segment size is given by the following formula:

$$m = \text{MTU} - \text{Max-GN-Header} - \text{Max-BTP-header}$$

For instance, the recommended MTU is 1 492 bytes when using ITS-G5 and the value of m is 1 428 bytes.

Different segmentation/fragmentation designs are possible and may also include coding or FEC techniques such as described in Annex C. The ITS-S based Full CTL broadcast service is two-fold:

- Case 1: the sending ITS-S starts the broadcast of the last updated CTL issued by a Root CA/TLM as described in use cases UC-SEC-10. E.g. an ITS-S which has received a fresh update of the CTL/ECTL shall start to broadcast the Full CTL message to its one-hop neighbours using the short-range wireless communication (CPS#003).

- Case 2: when receiving a Peer-to-Peer Full CTL Request from a requesting ITS-S as specified in clause 5.3.1, if the neighbour ITS-S has a newest version of the requested FullCtl available, it starts broadcasting it using the pre-defined frequency f and during the maximum transmission duration d (in seconds). In this case 2, the responder ITS-S shall use the PDU specified for the response in clause 5.5.3. The peer-to-peer response protocol shall use single-hop broadcasting as specified in clause 6.3 (CPS_003).

The present document assumes a separate segmentation/fragmentation service associated with a specific access layer technology that can be used by any application. This separate segmentation service should be located at the level of the Transport/Network level.

As shown in the following figure 4, the sending application/service shall send large file or PDU using the non-application specific segmentation service located at BTP level.

The sending segmentation service is treating the data as a blob, i.e. not semantically aware of the content of the file or PDU. It prepares the various segment PDUs in a way that should be transparent to the sending / receiving application. It should be aware of the properties of the channel being used such as the MTU, the channel error rate, etc. The sending segmentation may apply signatures to the segment PDUs.

For the distribution of the full CTL via the segmentation service, the segments called Segmented CTL Response Message (SCRM) are not signed but the full CTL which is segmented is signed by the source of the trust information list, i.e. the issuing authority (TLM or RCA) and the signature shall be verified by the receiving application/service.

The receiving segmentation service collects all the segments that are being received for a specific file or PDU intended for a specific higher layer service identified by the received ITS-AID/ PSID field in the Segment PDUs.

When the receiving segmentation service has completed the File or PDU transmitted by the ITS Sender, it forwards it to the upper-layer application /service corresponding to the sender.

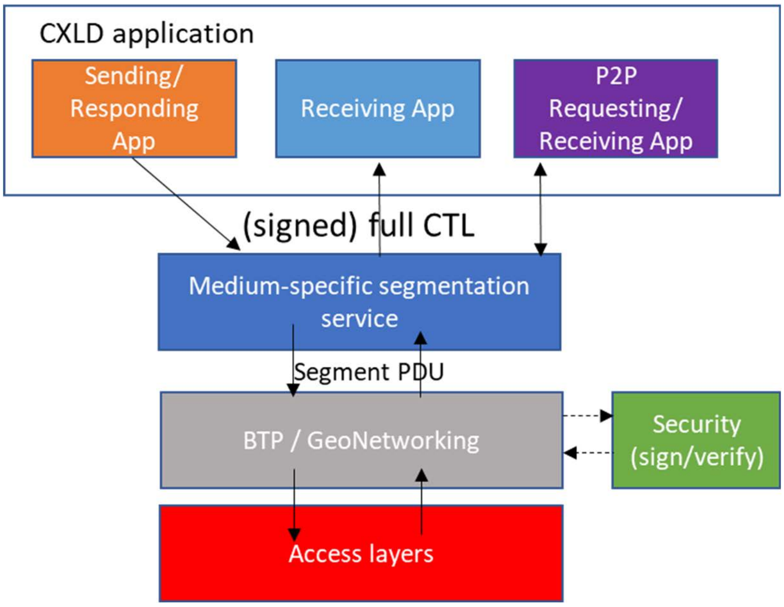


Figure 4: Non application-specific segmentation service

5.5.2 P2P Response distribution protocol

The ITS-S based Full CTL broadcast service shall enable the transmission by an ITS-S of the ECTL message (TlmCertificateTrustListMessage) or the CTL message (RcaCertificateTrustListMessage) with the parameter 'isFullCtl' in CtlFormat set to value TRUE as defined in ETSI TS 102 941 [2], clause A.2.7.

As a full CTL is a large data file, the ITS-S based Full CTL broadcast protocol is designed to support the segmentation of the ECTLmessage (TlmCertificateTrustListMessage) or the CTL message (RcaCertificateTrustListMessage).

NOTE 1: The segmentation service is provided by the Transport/Network layer as shown on figure 4.

All segments except the last one shall have a size equal to m (maximum payload size contained in a GN packet). The value of m shall be set to:

m = MTU – Max-GN-Header- Max-BTP-header = 1 428 bytes

NOTE 2: The value of m is calculated assuming that the transmission of segments is relying on Single-Hop Packets (SHB) as specified in [5] over ITS-G5 access layer. This maximum payload size (m) can be used also for other access layer technologies to guarantee interoperability of this service over different access layer technologies.

NOTE 3: The present document does not specify optimized values of m for other access layers.

The segment messages shall be transmitted in the sequence order and the structure of a segment message shall follow the ASN.1 specification of the CTL Response Message (SCRM) PDU as specified in clause 5.5.3.

If m is the maximum payload size contained in a packet, the payload containing the Full CTL shall be split into N segments such as:

N-1 x (m – controlInfo) < CTL size <= N x (m – controlInfo)

The size of the control information (controlInfo) in the Segment Message as specified in figure 5 is 22 bytes. All segment sizes but the last one are of 1 406 bytes.

NOTE 4: This size is calculated using the Octet Encoding Rules (OER) and include all the fields of the Segment PDU structure until (but not including) the first octet of the string of the `data` component in the segmentedData (see Annex D).

As there may be multiple potential senders, every potential distributor ITS-S shall start a random timer (T) which value shall be set between 0 and $T_{P2pctIdMax}$ and listen to detect whether another neighbour ITS-S has started transmitting the requested Full CTL. If it detects that another ITS-S is transmitting the same CTL, i.e. a SCRM PDU containing the same `fileId` value in the `segmentContent` of type `SegmentedData`, it shall not send the requested Full CTL.

Due to the high mobility, when a vehicle ITS-S passes along the sender ITS-S the time window for transmitting the requested CTL may be limited. Therefore, the maximum waiting time ($T_{P2pctIdMax}$) shall be set to 1 second.

In the case where the distribution is initiated by the ITS-S independently of any request received from an ITS-S (i.e. case 1 specified in clause 5.5.1), the sending ITS-S shall repeat the transmission of the consecutive segments corresponding to the Full CTL message following the same repetition mechanism as specified in clause 5.4.2.

If a receiver did not receive all the segments constituting the transmitted CTL or ECTL, it may request the missing segment using the Peer-to-Peer Full CTL request specified in clause 5.3.4.4. The component `segmentNumber` shall be PRESENT in the `EtsiTs102941FullCtlRequest` extension field and shall contain the number of the missing segment. If several segments are missing, it may send Peer-to-Peer Full CTL requests with the `segmentNumber` containing the number of each missing segment.

5.5.3 Message and version

A peer-to-peer response message is specified to enable the distribution of the Full CTL by an ITS-S which is called Segmented CTL Response Message (SCRM).

This clause provides the specification of the generic segment message structure (`SegmentPDU`) used by the segmentation service. An overview of the message structure is given in figure 5.

The `SegmentPDU` used by the segmentation service is a component composed of five fields followed by an extension mark:

- `version`: contains the version number of the PDU definition. The value of the version field of the message shall be set to value "1".
- `segmentationTime`: contains the timestamp when the segmentation operation was initiated. All the segments which are composing the same file or message to be segmented shall have the same segmentationTime value.
- `distributedAid`: contains the ITS-AID of the file.

- `fileId` : is the identifier of the file to be distributed. It is computed as the value of the SHA-256 hash function calculated on the transmitted file content.

- `segmentContent`: contains the segmented data of the message or file (see table 5).

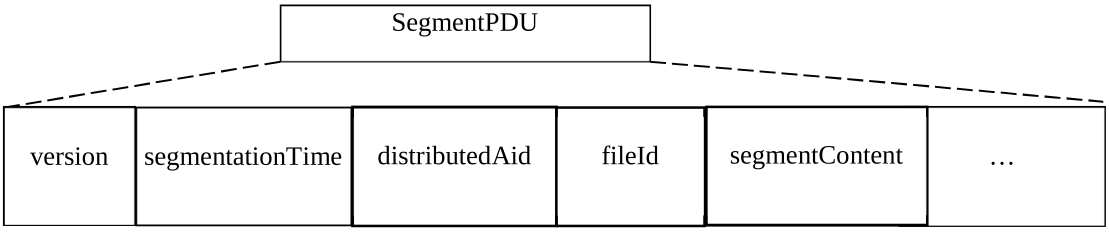


Figure 5: General structure of the generic segment message

The `SegmentPdu` is a parametrized type as shown in table 5 and the Segmented CTL Response Message (SCRM) is defined as a specialization of the SegmentedData where the psid parameter value is set to the ITS-AID value of the CTL service as specified in ETSI TS 102 965 [6] (i.e. value 624).

Table 5: ASN.1 structure of a `SegmentedData`

```
SegmentPDU {Psid} ::= SEQUENCE {
  version               Uint8,
  segmentationTime      Time32,
  distributedAid         Psid,

  fileId          HashedId8,
  segmentContent  SegmentedData},
  …
}
ctlPsid Psid ::= 624
ScrmPDU ::= SegmentPDU {Psid (ctlPsid)}
```

The ASN.1 specification of the Segmented CTL Response Message (SCRM) shall be as specified in Annex D. ASN.1 [i.4] data structures defined in the present document shall be encoded using the Canonical Octet Encoding Rules (COER) as defined in Recommendation ITU-T X.696 [7].

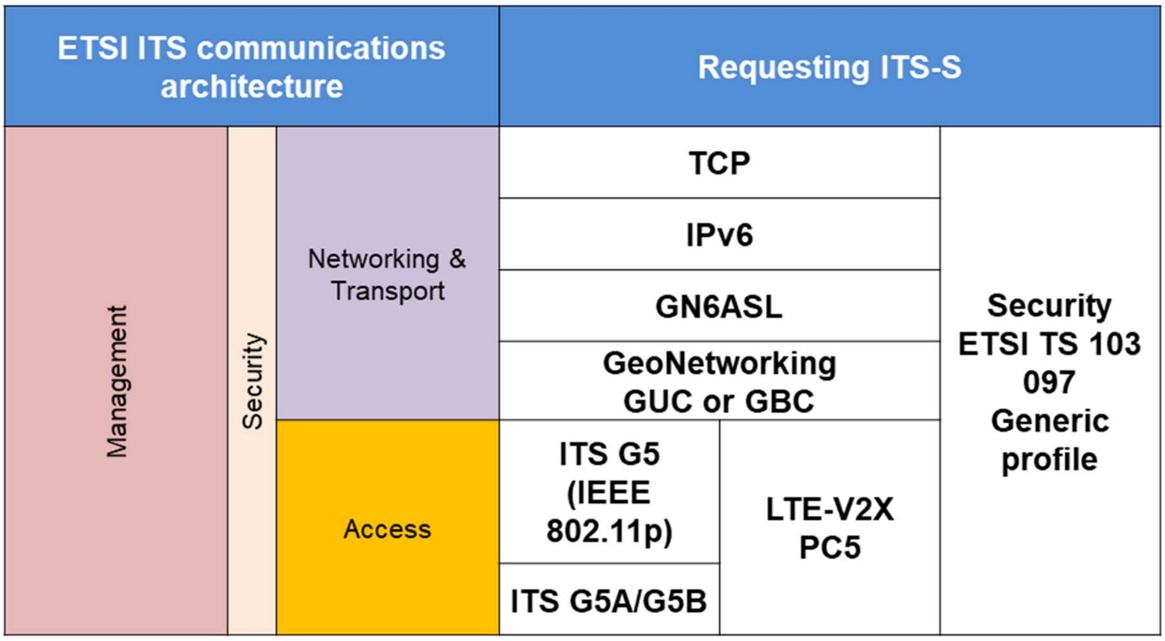
5.5.4 Protocol communication parameters

This service communication parameters are specified in clause 6.3 (CPS_003).

A Port Number value of the transport protocol is required for the segmentation service located on top of BTP and shall be as specified in ETSI TS 103 248 [4].

6 Communication profiles

6.1 CPS_001



NOTE: The ITS-S should use Ipv6 SLAAC functionality to auto-configure its Ipv6 address. The required parameters for SLAAC (i.e. RA message) should be provided by the R-ITS-S that acts as gateway as specified in ETSI TS 103 836 [i.5], e.g. via a SAM specified in ETSI EN 302 890-1 [i.2].

Figure 6: Communication profile using GN6 over ITS-G5 or LTE-V2X PC5

6.2 CPS_002

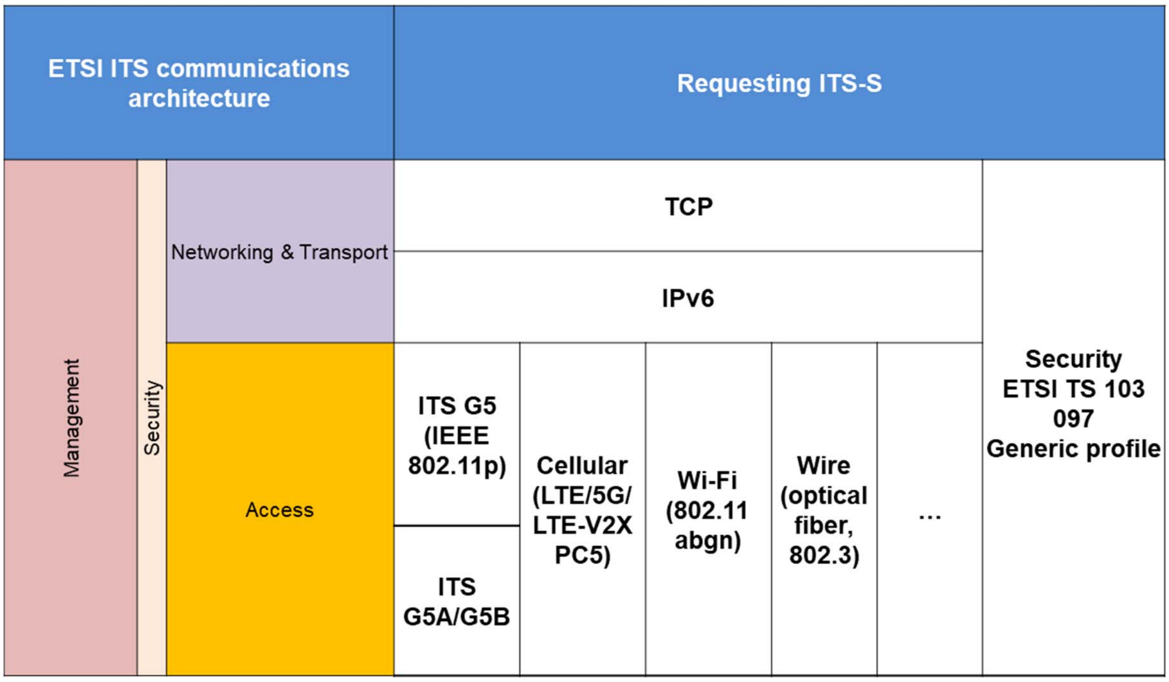
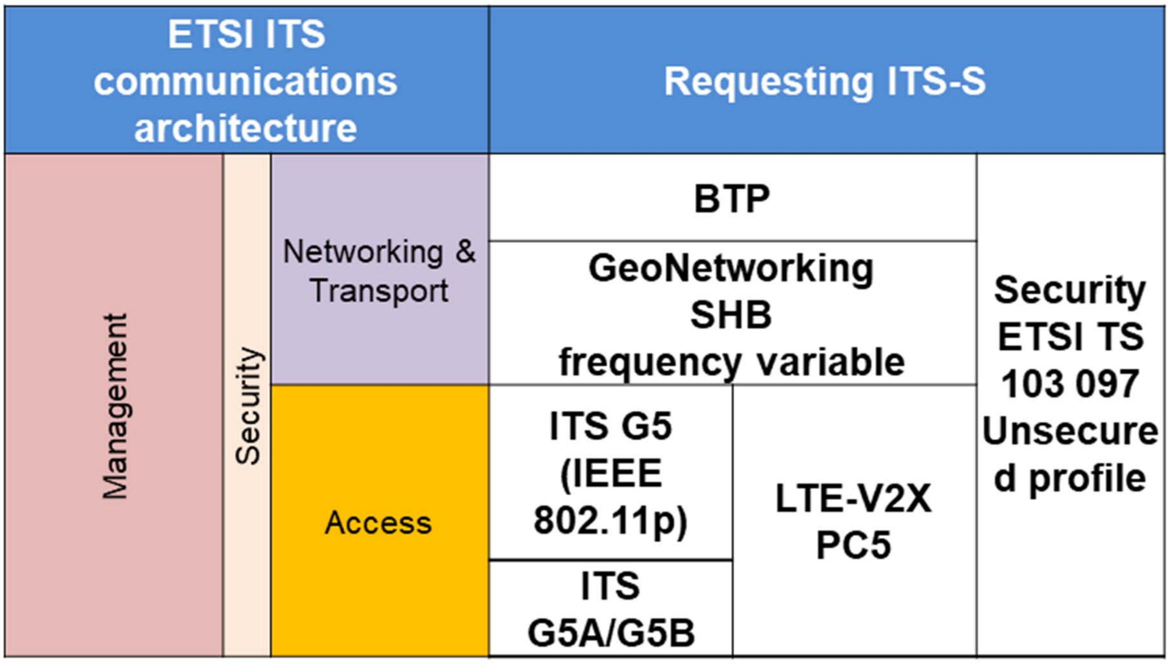

ETSI ITS communications architecture
Requesting ITS-S
Management
Security
Networking & Transport
Access
TCP
IPv6
ITS G5 (IEEE 802.11p)
ITS G5A/G5B
Cellular (LTE/5G/ LTE-V2X PC5)
Wi-Fi (802.11 abgn)
Wire (optical fiber, 802.3)
...
Security ETSI TS 103 097 Generic profile

Figure 7: Communication profile using Ipv6 over "any" access layer

6.3 CPS_003


ETSI ITS communications architecture
Requesting ITS-S
Management
Security
Networking & Transport
Access
BTP
GeoNetworking SHB frequency variable
ITS G5 (IEEE 802.11p)
ITS G5A/G5B
LTE-V2X PC5
Security ETSI TS 103 097 Unsecured profile

NOTE: This communication profile is specified in ETSI TS 102 941 [2], clause D.3. As shown in the figure, it is agnostic from the network access layers. The figure is only repeated here for sake of clarity.

Figure 8: Communication profile using GN/BTP SHB over ITS-G5 or LTE-V2X PC5

6.4 CPS_004

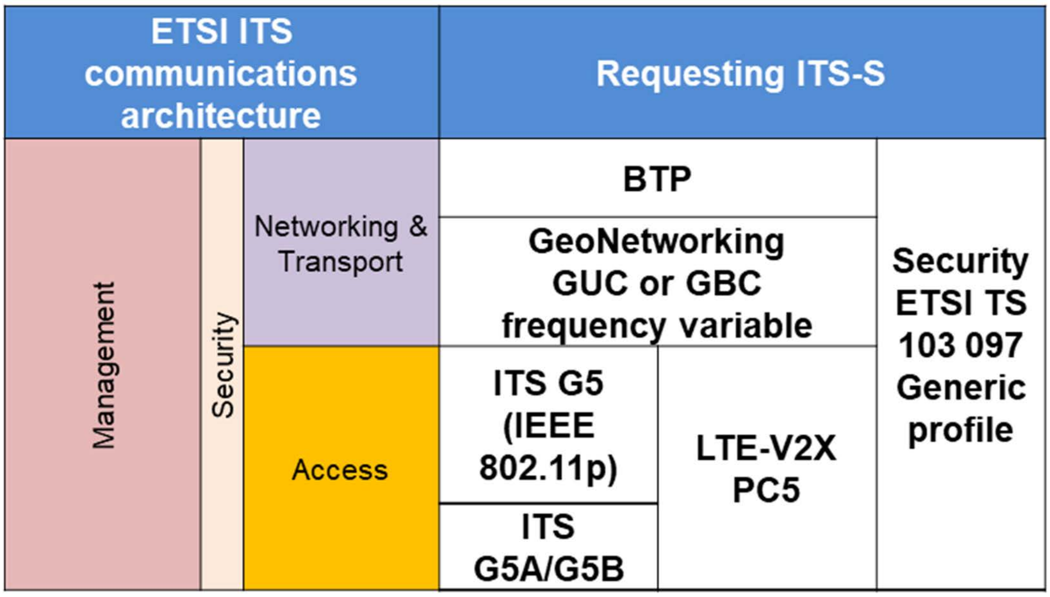

ETSI ITS communications architecture
Requesting ITS-S
Management
Security
Networking & Transport
Access
BTP
GeoNetworking GUC or GBC frequency variable
ITS G5 (IEEE 802.11p)
ITS G5A/G5B
LTE-V2X PC5
Security ETSI TS 103 097 Generic profile

Figure 9: Communication profile using GN/BTP GUC or GBC over ITS-G5 or LTE-V2X PC5

Annex A (normative): PICS pro forma

A.1 The right to copy

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the PICS pro forma in this annex so that it can be used for its intended purposes and may further publish the completed PICS pro forma.

A.2 Guidance for completing the PICS pro forma

A.2.1 Purposes and structure

The purpose of the present document is to provide a mechanism whereby a supplier of an implementation of the requirements defined in relevant specifications may provide information about the implementation in a standardized manner.

The PICS pro forma is subdivided into clauses for the following categories of information:

- instructions for completing the PICS pro forma;
- identification of the implementation;
- identification of the protocol;
- PICS pro forma tables (for example: major capabilities, etc.).

A.2.2 Abbreviations and conventions

This annex does not reflect dynamic conformance requirements but static ones. In particular, a condition for support of a PDU parameter does not reflect requirements about the syntax of the PDU (i.e. the presence of a parameter) but the capability of the implementation to support the parameter.

In the sending direction, the support of a parameter means that the implementation is able to send this parameter (but it does not mean that the implementation always sends it).

In the receiving direction, it means that the implementation supports the whole semantic of the parameter that is described in the main part of the present document.

The PICS pro forma contained in this annex is comprised of information in tabular form in accordance with the guidelines presented in ISO/IEC 9646-7.

Item column

The item column contains an identifier of the item in the table.

Item description column

The item description column describes in free text each respective item (e.g. parameters, timers, etc.). It implicitly means "is <item description> supported by the implementation".

Reference column

The reference column gives reference to the normative document.

Status column

The various status used in this annex are in accordance with the rules in table A.1.

Table A.1: Key to status codes

Status code	Status name	Meaning
M	mandatory	The capability shall be supported. It is a static view of the fact that the conformance requirements related to the capability in the reference specification are mandatory requirements. This does not mean that a given behaviour shall always be observed (this would be a dynamic view), but that it shall be observed when the implementation is placed in conditions where the conformance requirements from the reference specification compel it to do so. For instance, if the support for a parameter in a sent PDU is mandatory, it does not mean that it shall always be present, but that it shall be present according to the description of the behaviour in the reference specification (dynamic conformance requirement).
O	optional	The capability may or may not be supported. It is an implementation choice.
O.<int>	qualified optional	For mutually exclusive or selectable options from a set. "int" is an integer which identifies an unique group of related optional items and the logic of their selection which is defined immediately following the table.
n/a	not applicable	It is impossible to use the capability. No answer in the support column is required.
X	prohibited (excluded)	There is a requirement not to use this capability in the given context.
I	Irrelevant (out-of-scope)	Capability outside the scope of the reference specification. No answer is requested from the supplier.
<items>:<capability>	conditional	The requirement on the capability ("m", "o", "x" or "n/a") depends on the support of other optional or conditional **items**. Items can be grouped using logical operations AND, OR, NOT and parentheses.

Support column

The support column shall be filled in by the supplier of the implementation. The following common notations, defined in ISO/IEC 9646-7, are used for the support column:

Y or y	supported by the implementation
N or n	not supported by the implementation
N/A, n/a or -	no answer required (allowed only if the status is N/A, directly or after evaluation of a conditional status)

References to items

For each possible item answer (answer in the support column) within the PICS pro forma there exists a unique reference, used, for example, in the conditional expressions. It is defined as the table identifier, followed by a solidus c"a"acter "/", followed by the item identifier in the table.

EXAMPLE: A.5/2 is the reference to the answer of item 2 in table A.5.

A.2.3 Instructions for completing the PICS pro forma

The supplier of the implementation may complete the PICS pro forma in each of the spaces provided. More detailed instructions are given at the beginning of the different clauses of the PICS pro forma.

A.3 Identification of the Equipment

A.3.1 Introduction

Identification of the Equipment shall be filled in so as to provide as much detail as possible regarding version numbers and configuration options.

The product supplier information and client information shall both be filled in if they are different.

A person who can answer queries regarding information supplied in the PICS shall be named as the contact person.

A.3.2 Date of the statement

....

A.3.3 Equipment Under Test identification

Name:

....

....

Hardware configuration:

....

....

....

Software configuration:

....

....

....

A.3.4 Product supplier

Name:

....

Address:

....

....

....

Telephone number:

....

Facsimile number:

....

E-mail address:

....

Additional information:

....

....

....

A.3.5 Client

Name:

....

Address:

....

....

....

Telephone number:

....

Facsimile number:

....

E-mail address:

....

Additional information:

....

....

....

A.3.6 PICS contact person

Name:

....

Telephone number:

....

Facsimile number:

....

E-mail address:

....

Additional information:

....

....

A.4 Identification of the protocol

The PICS pro forma applies to the following specifications: ETSI TS 103 601, ETSI TS 102 941, ETSI TS 103 097.

A.5 Global statement of conformance

Are all mandatory capabilities implemented? (Yes/No) ....

NOTE: Answering "No" to this question indicates non-conformance to the ITS Security standard specification ETSI TS 103 097. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming, on pages attached to the PICS pro forma.

A.6 PICS pro forma tables

Unless stated otherwise, the column references of all tables below indicate the clause numbers of ETSI TS 102 941.

Table A.2: Roles of equipment

Item	Description	Reference	Status	Support
R1	ITS station		O.1	□Yes □No
R1.1	Vehicle ITS-S		R1: O.2	□Yes □No
R.1.1.1	Vehicle ITS-S distributing CTL and CRL		R1.1: O	□Yes □No
R.1.1.2	Vehicle ITS-S distributing Full CTL		R1.1: O	□Yes □No
R1.2	Roadside ITS-S		R1: O.2	□Yes □No
R1.2.1	Roadside ITS-S distributing CTL and CRL		R1.2: O	□Yes □No
R1.2.2	Roadside ITS-S providing AT reloading service		R1.2: O	□Yes □No
R1.2.3	Roadside ITS-S providing IPv6 over ITS-G5 gateway service		R1.2: O	□Yes □No
R1.2.4	Roadside ITS-S without privacy requirements [Itss_NoPrivacy]		R1.2: O	□Yes □No
R1.2.5	Roadside ITS-S distributing Full CTL		R1.2: O	□Yes □No
R2	Authorization Authority (AA)		O.1	□Yes □No
R3	Enrolment Authority (EA)		O.1	□Yes □No
R4	Root CA		O.1	□Yes □No
R5	TLM/CPOC		O.1	□Yes □No

Table A.3: Enrolment credential requests use-cases

Item	Description	Reference	Status	Support
UC-SEC-01	Enrolment credential re-keying			□Yes □No
UC-SEC-01.1	Requester side		UC-SEC-01 AND R1: M	□Yes □No
UC-SEC-01.1.1	Enrolment credential request retry		UC-SEC-01.1: M	□Yes □No
UC-SEC-01.2	Provider side		UC-SEC-01 AND R3: M	□Yes □No
UC-SEC-01.2.1	Enrolment credential request retry response		UC-SEC-01.2: M	□Yes □No

Table A.4: Authorization ticket reloading use-cases

Item	Description	Reference	Status	Support
UC-SEC-02	Authorization ticket reloading			□Yes □No
UC-SEC-02.1	Requester side		UC-SEC-02 AND R1: M UC-SEC-02 AND R1.1: O	□Yes □No
UC-SEC-02.1.1	AT request retry		UC-SEC-02.1 AND R1.2.4: O NOT R1.2.4: X	□Yes □No
UC-SEC-02.2	Provider side		UC-SEC-02 AND R2: M UC-SEC-02 AND R1.2.3 AND R1.2.2:M	□Yes □No
UC-SEC-02.2.1	AT request retry response		UC-SEC-02.2: O	□Yes □No

Table A.5: On demand request of a FullCTL

Item	Description	Reference	Status	Support
UC-SEC-03	On demand request of a FullCTL			
UC-SEC-03.1	Requester side		UC-SEC-03 AND R1: M UC-SEC-03 AND R2: O	□Yes □No
UC-SEC-03.2	Provider side		UC-SEC-03 AND R4: M UC-SEC-03 AND R5: M UC-SEC-03 AND R1.2.3:O	□Yes □No

Table A.6: On demand request of a DeltaCTL

Item	Description	Reference	Status	Support
UC-SEC-04	On demand request of a DeltaCTL			
UC-SEC-04.1	Requester side		UC-SEC-04 AND R1.2.1: M UC-SEC-04 AND R1: O	□Yes □No
UC-SEC-04.2	Provider side		UC-SEC-04 AND R4: M UC-SEC-04 AND R5: M UC-SEC-04 AND R1.2.3:O	□Yes □No

Table A.7: ITS-S based DeltaCTL distribution

Item	Description	Reference	Status	Support
UC-SEC-05	ITS-S based DeltaCTL distribution			
UC-SEC-05.1	Receiver side		UC-SEC-05 AND R1: O	□Yes □No
UC-SEC-05.2	Provider side		UC-SEC-05 AND R1.1.1: O.3 UC-SEC-05 AND R1.2.1: O.4	□Yes □No

Table A.8: Delay-tolerant peer-2-peer DeltaCTL distribution

Item	Description	Reference	Status	Support
UC-SEC-06	Delay-tolerant peer-2-peer DeltaCTL distribution			
UC-SEC-06.1	Requester side		UC-SEC-06 AND R1: O	□Yes □No
UC-SEC-06.2	Provider side		UC-SEC-06 AND R1.1.1: O.3 UC-SEC-06 AND R1.2.1: O.4	□Yes □No

Table A.9: On demand request of a CRL

Item	Description	Reference	Status	Support
UC-SEC-07	On demand request of a CRL			
UC-SEC-07.1	Requester side		UC-SEC-07 AND R1: O UC-SEC-07 AND R2: O UC-SEC-07 AND R3: O	□Yes □No
UC-SEC-07.2	Provider side		UC-SEC-07 AND R4: M	□Yes □No

Table A.10: ITS-S based CRL distribution

Item	Description	Reference	Status	Support
UC-SEC-08	ITS-S based CRL distribution			
UC-SEC-08.1	Receiver side		UC-SEC-08 AND R1: O	□Yes □No
UC-SEC-08.2	Provider side		UC-SEC-08 AND R1.1.1: O.5 UC-SEC-08 AND R1.2.1: O.6	□Yes □No

Table A.11: Delay-tolerant peer-2-peer CRL distribution

Item	Description	Reference	Status	Support
UC-SEC-09	Delay-tolerant peer-2-peer CRL distribution			
UC-SEC-09.1	Requester side		UC-SEC-09 AND R1: O	□Yes □No
UC-SEC-09.2	Provider side		UC-SEC-09 AND R1.1.1: O.5 UC-SEC-09 AND R1.2.1: O.6	□Yes □No

Table A.12: ITS-S based FullCTL distribution

Item	Description	Reference	Status	Support
UC-SEC-10	ITS-S based DeltaCTL distribution			
UC-SEC-10.1	Receiver side		UC-SEC-10 AND R1: O	□Yes □No
UC-SEC-10.2	Provider side		UC-SEC-10 AND R.1.1.2: O.3 UC-SEC-10 AND R1.2.5: O.4	□Yes □No

Table A.13: Delay-tolerant peer-2-peer FullCTL distribution

Item	Description	Reference	Status	Support
UC-SEC-11	Delay-tolerant peer-2-peer FullCTL distribution			
UC-SEC-11.1	Requester side		UC-SEC-11 AND R1: O	□Yes □No
UC-SEC-11.2	Provider side		UC-SEC-11 AND R1.1.2: O.3 UC-SEC-11 AND R1.2.5: O.4	□Yes □No

Table A.14: Communication profiles

Item	Description	Reference	Status	Support
CPS_001	GN6 over ITS-G5 or LTE-V2X PC5		UC-SEC-02.1: O UC-SEC-02.2 AND R1.2.2: M UC-SEC-07.1: O R1.2.3: M	□Yes □No
CPS_002	HTTP client over IP network		UC SEC-01.1:M UC -SEC-02.1: M UC -SEC-03.1: M UC -SEC-04.1: M UC-SEC-07.1: M	□Yes □No
	HTTP server over IP network		UC -SEC-01.2: M UC -SEC-02.2: M UC -SEC-03.2: M UC -SEC-04.2: M UC -SEC-07.2: M	□Yes □No
CPS_003	SHB over ITS-G5 or LTE-V2X PC5		UC -SEC-05.1: M UC -SEC-05.2: M UC -SEC-06.1: M UC -SEC-06.2: M UC -SEC-08.1: M UC -SEC-08.2: M UC -SEC-09.1: M UC -SEC-09.2: M UC -SEC-10.1: M UC -SEC-10.2: M UC -SEC-11.1: M UC -SEC-11.2: M	□Yes □No
CPS_004	GN/BTP GUC/GBC over ITS-G5 or LTE-V2X PC5		UC-SEC-02.1 AND R1.1: O UC-SEC-02.2 AND R1.2.2: M	□Yes □No

Annex B (informative): EC Retry scenario examples

B.1 EC Request lost

When the ITS-S is initiating a new Enrolment Request service (EC Request), it follows the steps below:

- The ITS-S creates an EC request as specified in ETSI TS 102 941 [2], clause 6.2.3.2.1.
- The ITS-S starts a timer T2 with threshold value TH2 which limits the life-time of the created EC request.
- The ITS-S starts a timer T1 with threshold value TH1 which runs until receiving the EC response.
- The ITS-S sends the EC request to the EA.

In case of EC request loss, the next steps are presented in figure B.1 and are described below:

- When the timer T1 reaches the threshold TH1 without receiving any response, the ITS-S re-sends the same EC request to the EA.
- The maximum number of retries should be smaller than the threshold N1 and the timer T2 should be lower that TH2.

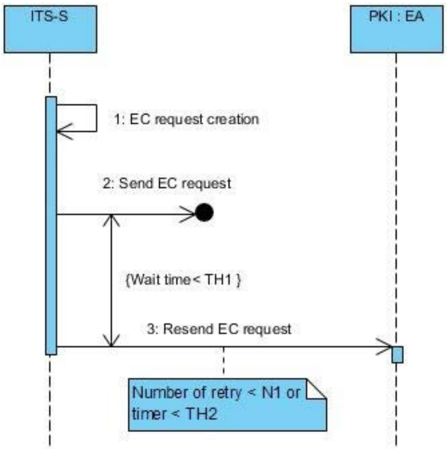


Figure B.1: Sequence diagram for EC request loss

B.2 EC response lost

When the ITS-S is initiating a new Enrolment Request service (EC Request), it follows exactly the same steps as specified in clause B.1.

In case of EC response loss, the next steps are presented in figure B.2 and are described below.

When the EA receives the EC request, it verifies whether the request is a new incoming request and if this is a new request, the EA follows the steps below:

- The EA verifies the request, and in particular the generation time validity, generates an EC for the requesting ITS-S, saves the hash of the EC Request received from the ITS-S in its cache and/or in a database.
- The EA starts a timer T3 with maximum duration equal to TH3.
- The EA generates the EC Response, saves it in its cache/database and returns it to the ITS-S.

When the ITS station initiates an EC request, the ITS-S waits for the EC response until the timer T1 reaches TH1.

- When the timer T1 finishes, the ITS-S re-sends the same EC request to the EA.
- When one of the EC retry procedure's ending trigger is reached, the ITS-S aborts the procedure.

When the EA receives the EC Request retry, the EA follows the steps below:

- The EA computes the request hash on the received EC request and verifies if the hash of the received EC request already exists in its data base/cache. If the hash exists, that means that the EC response has been sent to the ITS-S but it is lost (due to network problem).
- If the timer has not reached maximum threshold TH3, the EA retrieves the EC response already generated corresponding to the computed request hash and resends it to the ITS-S. Otherwise, it sends an EC response with negative response code set to `deniedrequest` (as specified in ETSI TS 102 941 [2], clause A.2.5.1).

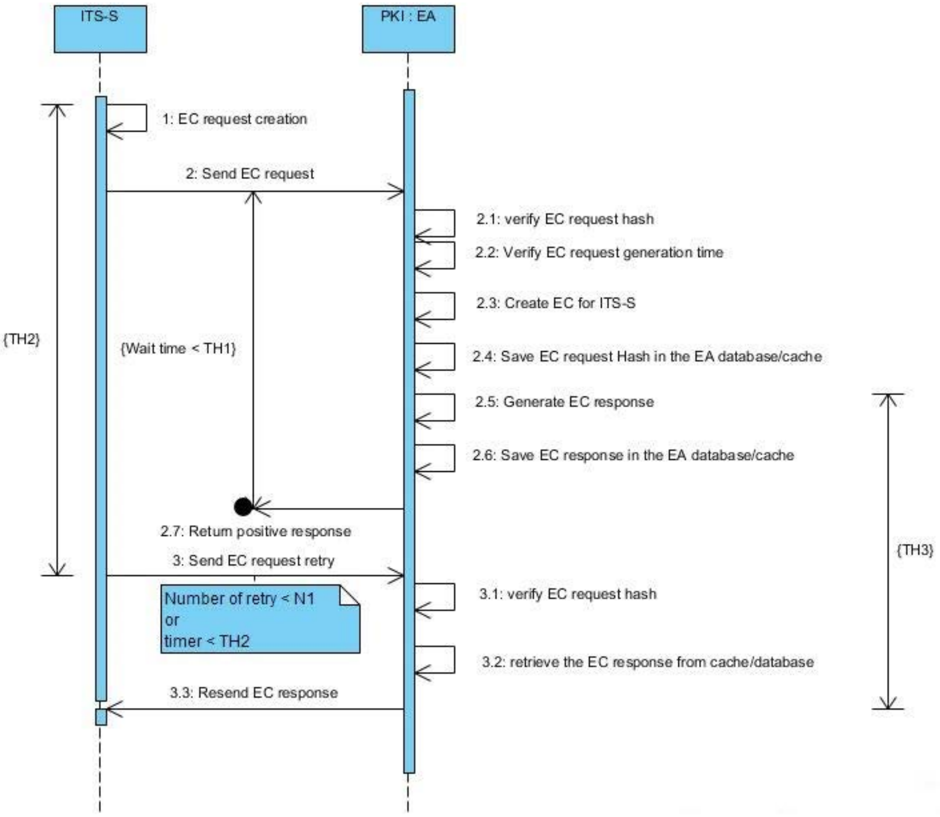

ITS-S
PKI : EA
1: EC request creation
2: Send EC request
2.1: verify EC request hash
2.2: Verify EC request generation time
2.3: Create EC for ITS-S
{TH2}
{Wait time < TH1}
2.4: Save EC request Hash in the EA database/cache
2.5: Generate EC response
2.6: Save EC response in the EA database/cache
2.7: Return positive response
3: Send EC request retry
{TH3}
Number of retry < N1
or
timer < TH2
3.1: verify EC request hash
3.2: retrieve the EC response from cache/database
3.3: Resend EC response

Figure B.2: Sequence diagram for EC response loss

Annex C (informative):
Survey of fragmentation/segmentation mechanisms and coding techniques

The ITS-S based Full CTL broadcasting service enables the transmission of the payload containing the Full CTL which may be larger than the MTU. For such purpose, it may apply a segmentation mechanism provided either by the facility layer or the distribution application (CXLDA).

It may also rely on other techniques provided by lower protocol layers such as Forward Error Correction codes (FEC) [i.10], network coding ([i.6], [i.7], [i.8], [i.9]) or fragmentation/reassembling mechanism at layer 2 that can be used transparently by all applications.

As presented in [i.9], network coding is a technique in which the data flow is optimized in the network by transmitting a composite of two or several messages. Messages are broken into chunks and formed into packets that encode information about one or multiple chunks. If one packet is lost, the data in other packets is used to reconstruct any lost data at receiver side. This allows the receiver to obtain the original message in a constant number of received packets and without requiring interaction with the sender, e.g. to request missing packets.

Network coding may be used with different FEC techniques for the presentation of various FEC families) and have been applied to many different protocol layers as well as for application specific solutions, e.g. file downloading in unicast or multicast modes over the internet or Wireless networks such as mobile networks or wireless/ ad-hoc-networks ([i.9]).

The IETF RMT group has specified a reliable multicast transport protocol called "File Delivery over Unidirectional Transport" (FLUTE) in IETF RFC 6726 [i.11] which allows a robust delivery of files on unidirectional transport to a group of multi-cast receivers. FLUTE is built on Asynchronous Layered Coding (ALC) which combines a Layered Coding Transport building block [i.12] and a FEC building block allowing to use many specific FEC codes [i.13]. FLUTE defines an in-band mechanism using File Delivery Table (FDT) to inform clients about files which are transmitted on sessions, allowing clients to start downloading files.

All these technological components are presented as examples but are not used in the present document. Such extensions are left for future study.

Annex D (normative): ASN.1 specification of the Segmented CTL Response Message

This clause provides the normative ASN.1 module containing the definitions of the data types specified in the present document. The ASN.1 module shall import data types from the ASN.1 modules defined in IEEE Std 1609.2™ [8].

The `EtsiTs103601Module` ASN.1 module is identified by the Object Identifier {itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103601) p2pctlresponse(1) major-version-1(1) minor-version-1(1)}. The module can be downloaded as a file as indicated in table D.1. The associated SHA-256 cryptographic hash digest of the referenced file offers a means to verify the integrity of that file.

Table D.1: `EtsiTs103601Module` ASN.1 module information

Module name	`EtsiTs103601Module`
OID	{itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) ts(103601) p2pctlresponse(1) major-version-1(1) minor-version-1(1)}
Link	https://forge.etsi.org/rep/ITS/asn1/sdp_ts103601/-/raw/v2.1.1/EtsiTs103601Module.asn
SHA-256 hash	e50b69ddf894e0397959d99640d86524b0c853108148f85ec9bc2834d73fac73

Annex E (informative): Change History

Date	Version	Information about changes
February 2023	V1.1.1	First Version.
March 2024	V2.1.1	Implementation of approved CR #0001 (Correct specification of the requirements for the P2P CRL/CTL request service in clause 5.3). Extension of use cases to enable Full CTL broadcasting/ P2P request. Specification of the Full CTL distribution service.

History

Document history		
V1.1.1	October 2020	Publication
V2.1.1	March 2024	Publication