



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

*ITeS ANNA PREVIEW*  
*(standards.iteh.ai)*  
*Full standards/sist/c88-067-889-*  
*https://standards.iteh.ai/catalog/standards/sist/c88-067-889-10*  
*4e42-bbe9-1e73f62b6dd8/etsi-103601-v1.1.1-2020-10*

---

**Reference**

DTS/ITS-00550

---

**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 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

---

**Important notice**

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

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

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2020.

All rights reserved.

**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.

# Contents

Intellectual Property Rights .....	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope .....	6
2 References .....	6
2.1 Normative references .....	6
2.2 Informative references.....	7
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	7
3.3 Abbreviations .....	8
3.4 Notation.....	8
4 Services description: use cases and requirements .....	9
4.1 Certificate provisioning service.....	9
4.1.1 Service description.....	9
4.1.1.1 Overview.....	9
4.1.1.2 UC-SEC-01: EC initial request or re-keying.....	10
4.1.1.3 UC-SEC-02: AT reloading.....	10
4.1.1.4 Use cases and communication profiles mapping.....	11
4.1.2 Requirements .....	11
4.1.2.1 Security requirements.....	11
4.2 CTL distribution service.....	12
4.2.1 Service description.....	12
4.2.1.1 Overview.....	12
4.2.1.2 UC-SEC-03: On demand request of a FullCTL.....	12
4.2.1.3 UC-SEC-04: On demand request of a DeltaCTL.....	13
4.2.1.4 UC-SEC-05: ITS-S based DeltaCTL distribution .....	14
4.2.1.5 UC-SEC-06: Delay-tolerant peer-2-peer DeltaCTL distribution .....	15
4.2.1.6 Use cases and communication profiles mapping.....	16
4.2.2 Requirements .....	16
4.2.2.1 System requirements .....	16
4.2.2.2 Security requirements.....	17
4.3 CRL distribution service .....	17
4.3.1 Service description.....	17
4.3.1.1 Overview.....	17
4.3.1.2 UC-SEC-07: On demand request of a CRL .....	17
4.3.1.3 UC-SEC-08: ITS-S based CRL distribution .....	18
4.3.1.4 UC-SEC-09: Delay-tolerant peer-2-peer CRL distribution.....	19
4.3.1.5 Use cases and communication profiles mapping.....	20
4.3.2 Requirements .....	20
4.3.2.1 System requirements .....	20
4.3.2.2 Security requirements.....	20
5 Use cases specific protocols description .....	21
5.1 Enrolment Management with repetition mechanism.....	21
5.1.1 EC retry overview.....	21
5.1.2 EC retry protocol .....	21
5.1.3 Message and version.....	21
5.1.4 EC retry requirements.....	22
5.1.5 Service communication parameter.....	22
5.2 Authorization Management with repetition mechanism.....	23
5.2.1 AT retry overview.....	23
5.2.2 AT retry protocol .....	23
5.2.3 Message and version.....	24
5.2.4 AT retry requirements.....	24

5.3	Peer-to-peer CRL/CTL distribution protocol .....	25
5.3.1	Overview .....	25
5.3.2	Peer-to-peer CRL/CTL request/response protocol.....	25
5.3.3	Message and version .....	26
5.3.4	Peer-to-peer CRL/CTL request message .....	26
5.3.4.1	General .....	26
5.3.4.2	Generation of a Peer-to-peer CRL request .....	27
5.3.4.3	Generation of a Peer-to-peer CTL request .....	27
5.3.5	Peer-to-peer CRL/CTL response message .....	28
5.3.6	P2P CRL/CTL request message trigger, repetition and termination.....	28
5.3.7	Protocol communication parameter .....	29
5.4	ITS-S based CRL/CTL broadcast protocol .....	29
5.4.1	Overview .....	29
5.4.2	CRL/CTL broadcast protocol .....	29
5.4.3	Message and version .....	30
5.4.4	Protocol communication parameter .....	32
6	Communication profiles .....	33
6.1	CPS_001 .....	33
6.2	CPS_002 .....	33
6.3	CPS_003 .....	34
6.4	CPS_004 .....	34
<b>Annex A (normative): PICS pro forma .....</b>		<b>35</b>
A.1	The right to copy .....	35
A.2	Guidance for completing the PICS pro forma .....	35
A.2.1	Purposes and structure .....	35
A.2.2	Abbreviations and conventions .....	35
A.2.3	Instructions for completing the PICS pro forma .....	36
A.3	Identification of the Equipment .....	37
A.3.1	Introduction .....	37
A.3.2	Date of the statement .....	37
A.3.3	Equipment Under Test identification .....	37
A.3.4	Product supplier .....	37
A.3.5	Client .....	38
A.3.6	PICS contact person .....	38
A.4	Identification of the protocol .....	39
A.5	Global statement of conformance .....	39
A.6	PICS pro forma tables .....	39
<b>Annex B (informative): EC Retry scenario examples .....</b>		<b>42</b>
B.1	EC Request lost .....	42
B.2	EC response lost .....	42
History .....		44

---

# Intellectual Property Rights

## Essential patents

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

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

## 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.

---

# 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 (V1.3.1): "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".
- [2] ETSI TS 102 941 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".
- [3] ETSI TS 103 097 (V1.4.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".
- [4] ETSI TS 103 248 (V1.3.1): "Intelligent Transport Systems (ITS); GeoNetworking; Port Numbers for the Basic Transport Protocol(BTP)".
- [5] ETSI EN 302 636-4-1: "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".
- [6] ETSI TS 102 965: "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration".

## 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".

---

## 3 Definition of terms, symbols and abbreviations

### 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

### 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 ( $N1 \geq 0$ ).
- 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 ( $N1 \geq 0$ ).
- 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

### 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
AT	Authorization Ticket
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
GBC	GeoBroadCast
GN	GeoNetworking
GN_SAP	GeoNetworking_Service Access Point
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
P2PCXLD	Peer-to-peer CRL/CTL Distribution service
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
RA	Router Advertisement
RAN	Radio Access Network
RCA	Root Certification Authority
R-ITS-S	Roadside ITS-S
RSU	Road Side Unit
SAM	Service Advertisement Message
SCH	Service CHannel
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
URL	Uniform Resource Locator
V-ITS-S	Vehicle ITS-S
WLAN	Wireless Local Area Network

### 3.4 Notation

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 fiber, 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.

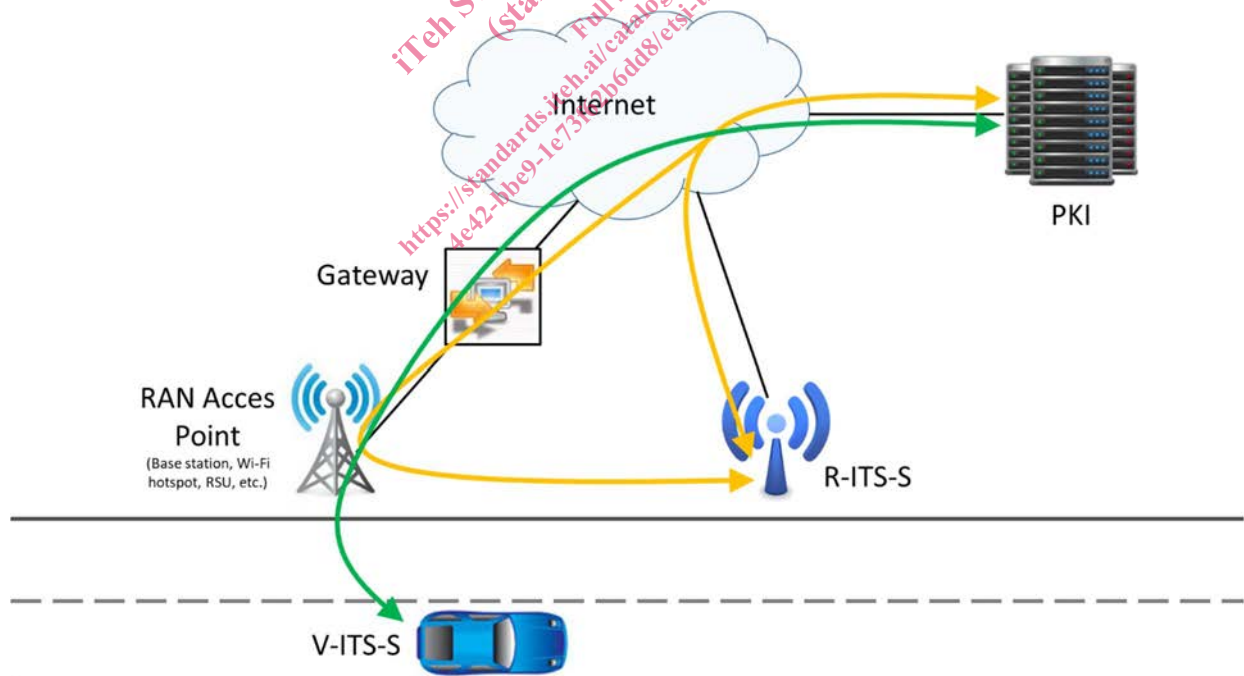


Figure 1: Example of certificates reloading service for a V-ITS-S (green) and a R-ITS-S (orange)

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

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

<b>Primary Actor</b>	ITS-S.		
<b>Description</b>	ITS-S requests an EC to the EA. After verification, the EA replies positively by sending back the requested EC to the ITS-S.		
<b>Preconditions</b>	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 using wireless connectivity, the ITS-S shall be under the radio coverage of an access point that provides Ipv6 connectivity.		
<b>Success End Condition</b>	ITS-S receives its EC from the EA.		
<b>Failed End Condition</b>	ITS-S does not receive its EC.		
<b>Involved components</b>	Security layer.		
<b>Main Success Scenario</b>	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.		
<b>Extensions</b>	None.		
<b>Variations (Alternatives)</b>	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.		
<b>Includes</b>			
<b>Security Characteristics</b>			
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

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

<b>Primary Actor</b>	ITS-S.		
<b>Description</b>	ITS-S requests an AT to the AA. After verifications, the AA replies positively by sending back the requested AT to the ITS-S.		
<b>Preconditions</b>	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 using wireless connectivity, the ITS-S shall be under the radio coverage of an access point that provides Ipv6 connectivity.		
<b>Success End Condition</b>	ITS-S receives its AT from the AA.		
<b>Failed End Condition</b>	ITS-S does not receive its AT.		
<b>Involved components</b>	Security layer.		
<b>Main Success Scenario</b>	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.		
<b>Extensions</b>	None.		
<b>Variations (Alternatives)</b>	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.		
<b>Includes</b>			
<b>Security Characteristics</b>			
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 following list gives the basic set of security objectives which shall 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.

- **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.

<b>Use Case ID:</b>	<b>UC-SEC-03</b>
<b>Use Case Name:</b>	Get Certificate Trust List.
<b>Priority:</b>	Mandatory.
<b>Related Requirement:</b>	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.