ETSI TS 103 301 V2.1.1 (2021-03)

Intelligent Transport Systems (ITS);
Vehicular Communications;
Basic Set of Applications;
Facilities layer protocols and communication requirements for infrastructure services;
Release 2

Reference
RTS/ITS-001948

Keywords
application, data, ITS, protocol, requirements

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

Contents

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).

The present document includes the integration of infrastructure based application protocols within the ITS message environment.

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.

Introduction

The infrastructure services are application support facilities provided by the Facilities layer that construct, manage and process messages distributed from infrastructure to end-users or vice-versa based on payload received from the application. The infrastructure services specified in the present document support infrastructure-based applications in order to achieve communication interoperability, and may be implemented in parallel to other services in an ITS-S.

1 Scope

The present document provides specifications of infrastructure related ITS services to support communication between infrastructure ITS equipment and traffic participants using ITS equipment (e.g. vehicles, pedestrians). It defines services in the facilities layer for communication between the infrastructure and traffic participants. The specifications cover the protocol handling for infrastructure-related messages as well as requirements to lower layer protocols and to the security entity.

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 EN 302 665 (V1.1.1): "Intelligent Transport Systems (ITS); Communications Architecture".

[2] ETSI TS 102 894-2 (V1.3.1): "Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary".

[3] ETSI EN 302 636-4-1 (V1.4.1): "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".

[4] ETSI EN 302 636-5-1 (V2.2.1): "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol".

[5] Void.

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

[7] ISO/TS 19321-2020: "Intelligent transport systems - Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures", (produced by CEN).

[8] ISO/TS 19091-2019: "Intelligent transport systems - Cooperative ITS - Using V2I and I2V communications for applications related to signalized intersections", (produced by CEN).

[9] ETSI EN 302 931 (V1.1.1): "Intelligent Transport Systems (ITS); Vehicular Communications; Geographical Area Definition".

[10] ISO/TS 17427-1:2018: "Intelligent transport systems - Cooperative systems - Part 1: Roles and responsibilities in the context of cooperative ITS based on architecture(s) for cooperative systems".

[11] Recommendation ITU-T X.691/ISO/IEC 8825-2 (1997-12): "Information technology - ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)".

[12] ETSI EN 302 637-2: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[13] ETSI EN 302 637-3: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".

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

[15] ETSI TS 103 248 (V1.3.1): "Intelligent Transport Systems (ITS); GeoNetworking; Port Numbers for the Basic Transport Protocol (BTP)".

[16] ETSI EN 302 663: "Intelligent Transport Systems (ITS); ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band".

[17] ETSI TS 136 300: "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (3GPP TS 36.300)".

[18] ETSI TS 102 636-4-2: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5".

[19] ETSI TS 103 301 (V1.3.1): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services".

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] Void.

[i.2] ISO/TS 17423:2018: "Intelligent Transport Systems - Cooperative Systems - Application requirements for selection of communication profiles".

[i.3] ISO/TS 14823: "Traffic and travel information - Messages via media independent stationary dissemination systems - Graphic data dictionary for pre-trip and in-trip information dissemination systems".

[i.4] IEEE 802.11™-2016: "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.5] ETSI TS 102 723-5 (V1.1.1): "Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 5: Interface between management entity and facilities layer".

[i.6] IANA Service Name and Transport Protocol Port Number Registry (2016-04-07).

NOTE: Available at https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt.

[i.7] IETF RFC 791: "IETF Internet Protocol".

[i.8] IETF RFC 768: "IETF User Datagram Protocol".

[i.9] IETF RFC 793: "IETF Transmission Control Protocol".

[i.10] SAE J2945/5-202002: "Service Specific Permissions and Security Guidelines for Connected Vehicle Applications".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

destination area: geographic area in which a message is disseminated

NOTE: The definition is compliant to ETSI EN 302 637-3 [13].

driver awareness zone: area in which the driver will be informed about upcoming situations

NOTE: The definition is compliant to ISO/TS 19321 [7].

ITS-G5: access technology to be according to ETSI EN 302 663 [16]

long range: communication with coverage of more than 500 m (e.g. cellular systems)

LTE-V2X sidelink: access technology using V2X sidelink communication according to ETSI TS 136 300 [17]

MAPEM: road/lane topology and traffic maneuver message

NOTE: As defined in Annex A including the corresponding extensions defined in ISO/TS 19091 [8].

minimum dissemination area: minimum area where an information is disseminated by an ITS-S based on application requirements

NOTE: The definition is compliant to ISO/TS 19321 [7].

relevance zone: area where the information is applicable

NOTE: The definition is compliant to ISO/TS 19321 [7].

short range: communication with coverage of approximately 500 m (e.g. WLAN)

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
AC	Access Category
AC_BE	Access Category Best Effort
AC_BK	Access Category BacKground
AC_VI	Access Category Video
AC_VO	Access Category VOice
ADU	Application Data Unit
AID	Action IDentifier
ASN	Abstract Syntax Notation
BTP	Basic Transport Protocol
CA	Certification Authority
C-ITS	Cooperative ITS
C-ITS-S	Cooperative ITS-Station
CPS	Communication Parameter Setting

CSP	Communication Service Parameter
DAZ	Driver Awareness Zone
DE	Data Element
DEN	Decentralized Environmental Notification
DENM	DEN Message
E-UTRA	Evolved UTRA
GBC	GeoBroadCast
GN	GeoNetworking
GNSS	Global Navigation Satellite System
GPC	GNSS Positioning Correction
GPCH	General Purpose Channel
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
IS	Infrastructure Services
ISM	Industrial, Scientific and Medical
ITIS	International Traveller Information Systems
ITS	Intelligent Transport System
ITS-AID	ITS-Application IDentifier
ITS-S	ITS Station
ITU-T	International Telecommunication Union - Telecommunication
IVI	Infrastructure to Vehicle Information
IVIM	Infrastructure to Vehicle Information Message
LTE	Long Term Evolution
LTE-V2X	LTE-Vehicle to Everything
MAPEM	MAP (topology) Extended Message
MDA	Minimum Dissemination Area
MF-SAP	Management Facilities layer SAP
MSB	Most Significant Bit
MTU	Maximum Transmit Unit
PDU	Protocol Data Unit
PER	Packet Encoding Rule
R-ITS-S	Roadside ITS Station
RLT	Road and Lane Topology
RTCM	Radio Technical Commission for Maritime services
RTCMEM	RTCM Extended Message
RTK	Real Time Kinematic
RZ	Relevance Zone
SAP	Service Access Primitive
SCH	Service CHannel
SFCH	SaFety CHannel
SHB	Single Hop Broadcast
SPATEM	Signal Phase And Timing Extended Message
SREM	Signal Request Extended Message
SSEM	Signal request Status Extended Message
SSID	Service Set Identifier
SSP	Service Specific Permissions
TC ID	Traffic Class IDentity
TC	Traffic Class
TCC	Traffic Control Center
TCP	Transmission Control Protocol
TCP-IP	Transport Control Protocol - Internet Protocol
TLC	Traffic Light Control
TLM	Traffic Light Maneuver
TS	Technical Specification
UDP	User Datagram Protocol
UTRA	Universal Terrestrial Radio Access
UTRAN	UMTS Terrestrial Radio Access Network
V2X	Vehicle-to-Everything
V-ITS-S	Vehicular and personal ITS Station
WLAN	Wireless Local Area Network

4 Infrastructure services introduction and general requirements

4.1 Naming convention

Within the scope of the present document, the term "message" refers to the Facilities layer PDU; the term "payload" refers to the applications layer ADU. The payload is generated by the application and provided to the corresponding service of the Facilities layer. The Facilities service merges the *ItsPduHeader* with the payload, in order to construct a message. The message is then delivered to the ITS Networking & Transport Layer with a set of communication parameters.

NOTE: In other standards referred by the present document, the term message, payload, data structure may have different meanings e.g. in ISO/TS 19091 [8] and in ISO/TS 19321 [7]. Therefore, the current convention is defined for clarification purposes.

4.2 Infrastructure services in the ITS communications architecture

The infrastructure services refer to Facilities layer entities that manage the generation, transmission and reception of infrastructure-related messages from the infrastructure (C-ITS-S or R-ITS-S) to V-ITS-S or vice-versa. Figure 1 illustrates a high level functional architecture of the infrastructure services within the ITS communication architecture, as specified in ETSI EN 302 665 [1]. The messages are Facilities layer PDUs that are exchanged among ITS-Ss. The payload is generated by ITS applications in the transmitting ITS-S or other connected ITS-S (e.g. a C-ITS-S). At the transmitting ITS-S, the transmission of a message is triggered by applications or by forwarding mechanisms. For this purpose, the applications may connect to other entities of the Facilities layer or to external entities, in order to collect relevant information for the generation of the payload. Once the message is generated, the services may repeat the transmission, until the applications requests the termination of the transmission, or trigger another request to generate updated messages. At the receiving ITS-S, the messages are processed by the services and the content of the message is delivered to applications or to other Facilities layer entity. In one typical application, the message is transmitted by an R-ITS-S and disseminated to V-ITS-S within a target destination area, in which the information included in the message is considered as relevant to traffic participants.

In the scope of the present document, the infrastructure services supports the management of the following message types. As result, the infrastructure services include a set of service entities as listed below:

- SPATEM as defined in Annex A. The corresponding service entity is referred as "Traffic Light Maneuver" - TLM service in the present document. TLM service is specified in clause 5 of the present document.
- MAPEM as defined in Annex A. The corresponding service entity is referred as "Road and Lane Topology" - RLT service in the present document. RLT service is specified in clause 6 of the present document.
- IVIM as defined in Annex A. The corresponding service entity is referred as "Infrastructure to Vehicle Information" - IVI service in the present document. IVI service is specified in clause 7 of the present document.
- SREM as specified in Annex A. The corresponding service entity is referred as "Traffic Light Control" - TLC service in the present document. TLC service is specified in clause 8 of the present document.
- SSEM as specified in Annex A. The corresponding service is referred as " Traffic Light Control" - TLC service in the present document. TLC service is specified in clause 8 of the present document.

NOTE: Other messages may be supported by infrastructure services in the future.

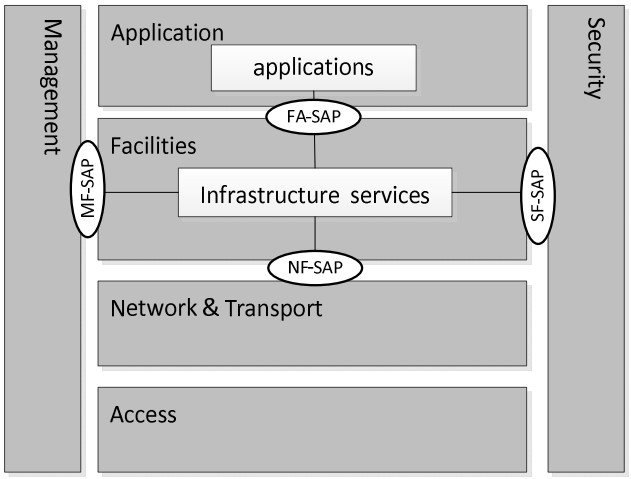

Figure 1: Infrastructure services within the ITS-S architecture

The infrastructure service shall provide at least the following functions.

For the transmission service:

- Message encoding.
- Transmission management.

For the reception service:

- Message decoding.
- Reception management.

4.3 Infrastructure services in the ITS organizational architecture

Within the role "System Operation" as defined in ISO/TS 17427-1 [10], the following sub roles are relevant for the infrastructure services:

- "Content Provision" is responsible for generating the information that is conveyed in the message. This task is included in any application providing information to the application which generates the payload.
- "Service Provision" is responsible for the generation of the payload and the transmission of the message using an ITS-S. This task is managed by the application making use of the infrastructure services.
- "Service Presentation" is responsible for the reception of the messages and its processing and presentation. This task is managed by the infrastructure services and the application.

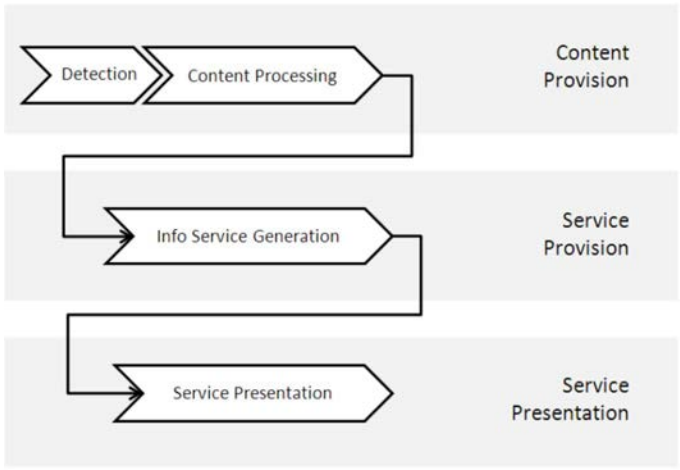

Figure 2: Identification of sub-roles of the role system (lifecycle) operation in the ITS organizational architecture

4.4 Interfaces of the infrastructure services

4.4.1 Interface between Application layer and Facilities layer

The infrastructure services within the Facilities layer provide APIs to applications for the processing of the payload at the transmitting ITS-S and the receiving ITS-S. An application may execute requests to the infrastructure services in the Facilities layer to trigger, update or terminate transmission of a message. In addition, a set of Facilities control information is passed as specified in Table 1.

Table 1 presents the Facilities control Information (SAP primitives) contained in an application request.

Table 1: Facilities control information (SAP primitives)

Category	Data	Definition
Data passed from application to infrastructure services	Infrastructure message identification	Identification of the message
	Request type	Trigger, update or ending of transmission
	Dissemination parameter	For more details, see the dissemination profile for each service in the clauses 5 to 8
	Traffic class	GN traffic class as defined in ETSI EN 302 636-4-1 [3], if GeoNetworking/BTP is used
	Payload	Information contained in payload
Data returned from I2V service to the requesting application	actionID or other applicable identifier	The infrastructure service returns the message identification or other applicable identifier created by the infrastructure service to the requesting application
	Failure notification	The infrastructure service returns a failure notification to the requesting application

4.4.2 Interface between Facilities layer and Management entity

The infrastructure services may exchange information with the Management entity. This includes the default service communication parameters specified in clauses 5 to 8. The interface MF-SAP may be realized as the MF-SAP ETSI TS 102 723-5 [i.5].

4.4.3 Interface between Facilities layer and Security entity

The infrastructure service may exchange information with the Security entity.

4.4.4 Interface between Facilities layer and the N&T layer

The infrastructure services deliver the message as payload to the ITS Networking & Transport Layer for dissemination via the NF-SAP.

The ITS Networking & Transport Layer indicates the reception of an ITS message to the infrastructure services.

4.5 Common protocol requirements for infrastructure services

4.5.1 Security for messages used by infrastructure

The security mechanisms for messages used by the infrastructure service as specified in the present document shall use the message authentication with signatures to be verified at the receiving ITS-S with public keys contained in certificates. A certificate indicates its holder's permissions, i.e. what statements the holder is allowed to make or privileges it is allowed to assert in a message signed by that certificate. The format for the certificates shall be as specified in ETSI TS 103 097 [6].

All defined messages in the present document shall be signed using private keys associated to Authorization Tickets that contain the appPermissions item with the AID of the Service and corresponding SSPs of type BitmapSsp as specified in ETSI TS 103 097 [6].

Service permissions are indicated by a pair of identifiers within a certificate, the ITS-AID and the SSP. The ITS-Application Identifier (ITS-AID) as given in ETSI TS 102 965 [14] indicates the overall type of permissions being granted.

The Service Specific Permissions (SSP) is a field that indicates specific sets of permissions within the overall permissions indicated by the ITS-AID. The originating ITS-S shall provide SSP information in its certificate for all generated, signed messages. The SSP permissions are defined for each message in the corresponding clause. The common approach that is used for all messages is that the SSP information is constructed out of N octets with a maximum length as specified in ETSI TS 103 097 [6]. For each octet, the most significant bit (MSB) shall be the leftmost bit. The transmission order shall always be the MSB first. The first octet shall control the SSP version and be interpreted in the following way:

0: NULL version, length 1 octet; the value shall only be used for testing purposes.

1..n: SSP version as defined in the present document for each service (see "SSP version control").

At reception of a message, the ITS-S shall check whether the message content is consistent with the SSP contained in the certificate in its signature. If the consistency check fails, the message shall be discarded.

4.5.2 Message payload encapsulation

The *ItsPduHeader* header as defined in ETSI TS 102 894-2 [2] shall be used to encapsulate the payload in order to construct messages. The ITS PDU header includes the following elements:

- *protocolVersion*: Version of the ITS payload contained in the message as defined for the specific infrastructure service.
- *messageID*: Type of the ITS payload contained in the message as defined for the specific infrastructure service.
- *stationID*: Identifier of the ITS-S that generated the message.

The *messageID* data element allows the receiver to identify the ITS message and to make it available to the corresponding Facilities layer service.

The *protocolVersion* data element allows the receiver to correctly deal with different versions of the protocol specification for the message.

More detailed information is covered in the Annex A.

4.5.3 Message encoding scheme

Unless specified otherwise, the unaligned PER encoding scheme as specified in Recommendation ITU-T X.691 [11] shall be used for the encoding of the messages specified in the present document.

4.6 Protocol version

4.6.1 Protocol version definition

The value of the protocol version for the messages SPATEM, MAPEM, IVIM, SREM, SSEM, RTCMEM is individual and independent of each other. It is defined in the *ItsPduHeader* for each message and identified by the *protocolVersion* data element (see clauses 5 to 8).

4.6.2 Protocol version handling

If the ASN.1 definition of the protocol is extended without compromising the backwards compatibility, the data element *protocolVersion* will not be increased. This allows the receiving ITS-S to process the message correctly (except the extensions) without the need for immediate update. An update for protocol interoperability is not needed, unless the receiving ITS-Station is intended to correctly interpret also the added extensions.

The *protocolVersion* data element is increased only in case of non-backwards compatible changes in the protocol specification to allow the receiving ITS-S to handle the message appropriately.

An example of how a receiving ITS-Station deals with messages according to the *protocolVersion* data element is shown in Table 2.

In the example the Version "V1" is the published version (*protocolVersion* = 1). Private extensions indicate extensions that are either not standardized or only recognized in a specific application context, e.g. applications implementing extensions for usage within local geographical regions. Version "V2" indicates a published, non-backwards compatible extension (*protocolVersion* = 2).

It is recommended that all changes to the protocol specification are additions using the ASN.1 extensions mechanism. These can be:

- Private (non-standardized) extensions: the support for this is limited and its use is discouraged.
- Standardized extensions as part as new version of published standards.

Table 2: Example for handling of messages with different protocol versions

Sending ITS-S Implemented version of the protocol	Receiving ITS-S Implemented version of the protocol	Receiving ITS-S Decoding result
V1	V1	Support of V1
V1 with private extensions	V1	Support of V1 and no support of private extensions
V1 with private extensions	V1 with same private extensions as the sending ITS-S	Support of V1 and and support of private extensions from the sending ITS-S
V1 with private extensions	V1 with other private extensions as the sending ITS-S	Support of V1 and no support of private extensions from the sending ITS-S
V1 with private extensions	V2	No support of V1 and no support of private V1 extensions
V2 (V1 with published extensions, included after the extension mark)	V1	Support of V1
V2 (V1 with published extensions, included after extension mark)	V2 with published extensions	Support of V2
V2 (changes in the data elements, included before the extension mark)	V2	No support of V2

5 Traffic Light Maneuver (TLM) service

5.1 TLM service overview

The TLM service is one instantiation of the infrastructure services to manage the generation, transmission and reception of SPATEM messages. The TLM service includes safety-related information for supporting traffic participants (vehicles, pedestrians, etc.) to execute safe maneuvers in an intersection area. The goal is to enter and exit an intersection "conflict area" in a controlled way. The TLM service informs in real-time about the operational states of the traffic light controller, the current signal state, the residual time of the state before changing to the next state, the allowed maneuvers and provides assistance for crossing. Additionally the TLM service foresees the inclusion of detailed green way advisory information and the status for public transport prioritization.

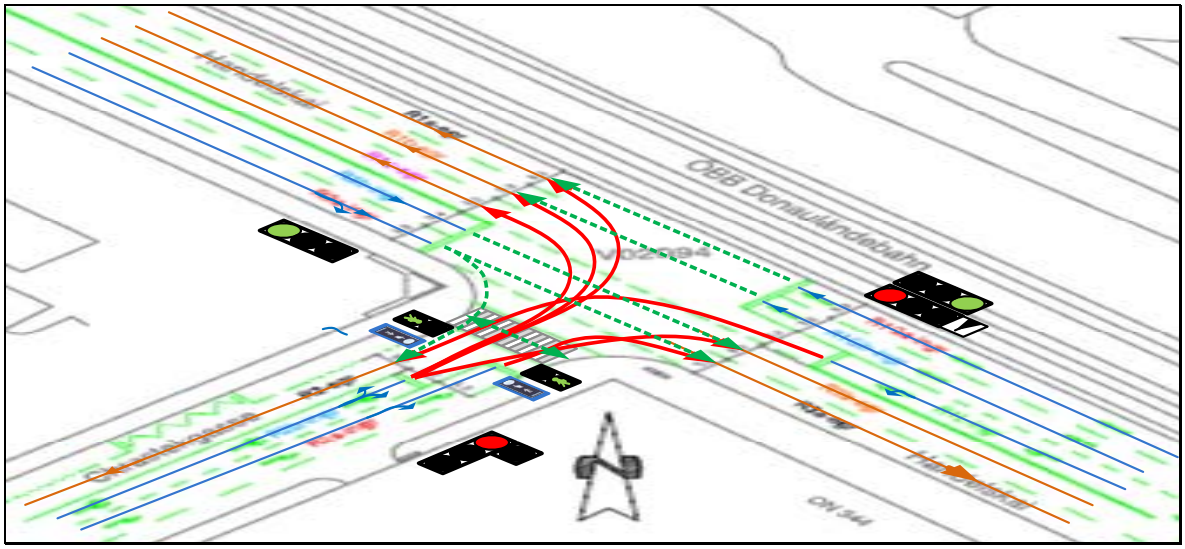

Figure 3: Signalling status of the maneuvers in an intersection

Figure 3 gives an example of the TLM service describing the driving permissions given to the traffic streams. The connection lanes (see clause 6), which describe the allowed maneuver, are highlighted based on the signalling status of the traffic light controller. The status information (e.g. "stop", "go") transmitted by the traffic controller is depicted in Figure 3 with red and green connection lines, respectively.

5.2 TLM service

The TLM service instantiated in an ITS-Station shall provide the communication services defined in clause 4.2.

5.3 TLM service message and version

The TLM service uses the message SPATEM as defined in Annex A. The header of SPATEM shall be as specified in the data dictionary ETSI TS 102 894-2 [2]. The data elements of SPATEM payload shall be as specified in ISO/TS 19091 [8].

The *protocolVersion* (defined in the header) of SPATEM message based on the present document is set to value "2".

5.4 TLM service dissemination

5.4.1 TLM service identification

The TLM service provides real-time information of the traffic light signal phase and timing of an intersection or parts of an intersection identified by the intersection reference identifier. The timestamp indicates the order of messages within the given time system as defined in ISO/TS 19091 [8]. There is no additional identifier needed to distinguish a SPATEM from a previous one.

5.4.2 TLM service trigger, update, repetition and termination

The application triggers the TLM service for the transmission of SPATEM. The application provides all data content included in a SPATEM payload. The TLM service constructs a SPATEM and delivers it to the ITS Networking & Transport Layer for dissemination. The SPATEM is not repeated.

The TLM service shall be terminated, if the ITS-S application requests the termination.

5.4.3 TLM service communication requirements

5.4.3.1 TLM service communication overview

The TLM service uses SPATEM to disseminate the status of the traffic light controller, traffic lights and intersection traffic information. It transmits continuously in real-time the information relevant for all maneuvers in the area of an intersection. The goal is to address all traffic participants using the intersection for travel or cross walking. Due to different equipment of end users, the SPATEM may be disseminated using different access technologies for short range or for long range communication.

5.4.3.2 TLM service communication requirements for short range access technologies

Table 3 provides the requirements for the broadcast communication. The structure of the requirements is in accordance with ISO/TS 17423 [i.2].

The ITS station management uses the communication requirements to select suitable ITS-S communication protocol stacks. Some examples of communication profile settings that fulfil these requirements are specified in clause 11.

Table 3: TLM service communication requirements for short range access technologies

Requirement	Value	Comment
Operational parameters		
CSP_LogicalChannelType	SFCH	
CSP_SessionCont	n.a.	No continuous connectivity
CSP_AvgADUrate	255, 1 second (default)	
CSP_FlowType	n.a.	
CSP_MaxPrio	254	
CSP_PortNo	2 004	Port Number of the transport protocol (see ETSI TS 103 248 [15])
CSP_ExpFlowLifetime	n.a.	
Destination related parameters		
CSP_DestinationType	1: broadcast transmission 16: geocast transmission to an area given by geo-coordinates.	If the MDA is within direct communication range of the sending ITS-S, destination type 1 shall be used. If the MDA exceeds the direct communication range or is not within the direct communication range, destination type 16 shall be used
CSP_DestinationDomain	site-local	
CSP_CommDistance	400 m radius (default value)	
CSP_Directivity	n.a.	
Performance communication service parameters		
CSP_Resilience	High	Repeated transmission of the same message
CSP_MinThP	n.a.	
CSP_MaxLat	ms100 (8)	Response within less than 100 ms
CSP_MaxADU	Max message size allowed by access technology	
Security related parameters		
CSP_DataConfidentiality	n.a.	
CSP_DataIntegrity	required	
CSP_NonRepudiation	required	
CSP_SourceAuthentication	required	
Protocol related parameter		
Protocol-Req	n.a.	

TLM Application Identifier (AID)

The ITS AID of the TLM service is allocated in ETSI TS 102 965 [14].

TLM service security parameters

For security against misuse of keys also for stationary installations it is necessary to change the pseudonym identity regularly. The default time for is given in Table 4. For special cases like offline working traffic light controllers where manually driven provision of pseudonym identity keys is necessary, longer periods of e.g. half a year are allowed and shall be agreed with the operator.

Table 4: TLM service security parameters

TLM service security parameters	
Authorization ticket validity	2 months (default value)

TLM Service Specific Permissions (SSP):

The interpretation of the SSP octet scheme is defined as depicted in Figure 4.

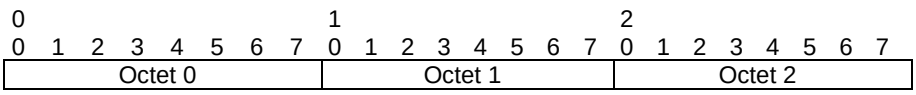

Figure 4: Format for the Octets

The SSP for the TLM service shall correspond to the octet scheme of Table 5.

Table 5: Octet Scheme for TLM service SSPs

Octet #	Description	Value
0	SSP version control	1
1	Service-specific parameter	see Table 6

Table 6: TLM service specific permissions

Octet position	Bit position	SPATEM data Item	Bit Value
1	0 (80h) (MSBit)	Signal Phase and Timing {SPATEM.spat.intersections. IntersectionState.states}	0: certificate not allowed to sign 1: certificate allowed to sign
1	1 (40h)	Public transport prioritization status response {SPATEM.spat.intersections. IntersectionState.regional.SEQUENCE. regExtValue. IntersectionState-aggGrpC.activePrioritizations}	0: certificate not allowed to sign 1: certificate allowed to sign
1	2 (20h)	Maneuver assisting information {SPATEM.spat.intersections. IntersectionState.maneuverAssistList} and {SPATEM.spat.intersections. IntersectionState.states.MovementState. maneuverAssistList}	0: certificate not allowed to sign 1: certificate allowed to sign
NOTE: All other bits of the SSP are not used and set to 0.			

5.4.3.3 TLM service communication requirements for long range communication

This clause provides the requirements for the long range unicast communication (e.g. usage of cellular network) in accordance with ISO/TS 17423 [i.2].

Table 7: TLM service communication requirements for long range access technologies

Requirement	Value	Comment
Operational communication service parameters		
CSP_LogicalChannelType	SFCH	
CSP_SessionCont	n.a.	
CSP_AvgADUrate	n.a.	
CSP_FlowType	n.a.	
CSP_MaxPrio	n.a.	
CSP_PortNo	2 004	Port Number of the transport protocol (see ETSI TS 103 248 [15])
CSP_ExpFlowLifetime	n.a.	
Destination communication service parameters		
CSP_DestinationType	4: unicast	
CSP_DestinationDomain	global	
CSP_CommDistance	n.a.	
CSP_Directivity	n.a.	
Performance communication service parameters		
CSP_Resilience	required	
CSP_MinThP	n.a.	
CSP_MaxLat	n.a.	
CSP_MaxADU	Max message size allowed by access technology	
Security communication service parameters		
CSP_DataConfidentiality	n.a.	
CSP_DataIntegrity	required	
CSP_NonRepudiation	required	
CSP_SourceAuthentication	required	
Protocol communication service parameter		
Protocol-Req	n.a.	

6 Road and Lane Topology (RLT) service

6.1 RLT service overview

The RLT service is one instantiation of the infrastructure services to manage the generation, transmission and reception of a digital topological map, which defines the topology of an infrastructure area. It includes the lane topology for e.g. vehicles, bicycles, parking, public transportation and the paths for pedestrian crossings and the allowed maneuvers within an intersection area or a road segment. In future enhancements the digital map will include additional topology-descriptions like traffic roundabouts.

The area of an intersection described by the topology covers about 200 m of the approaches, starting from the position of the stop line. If a neighbor intersection is closer than 400 m, the description may be done up to an extent of approximately the half distance between the intersections.

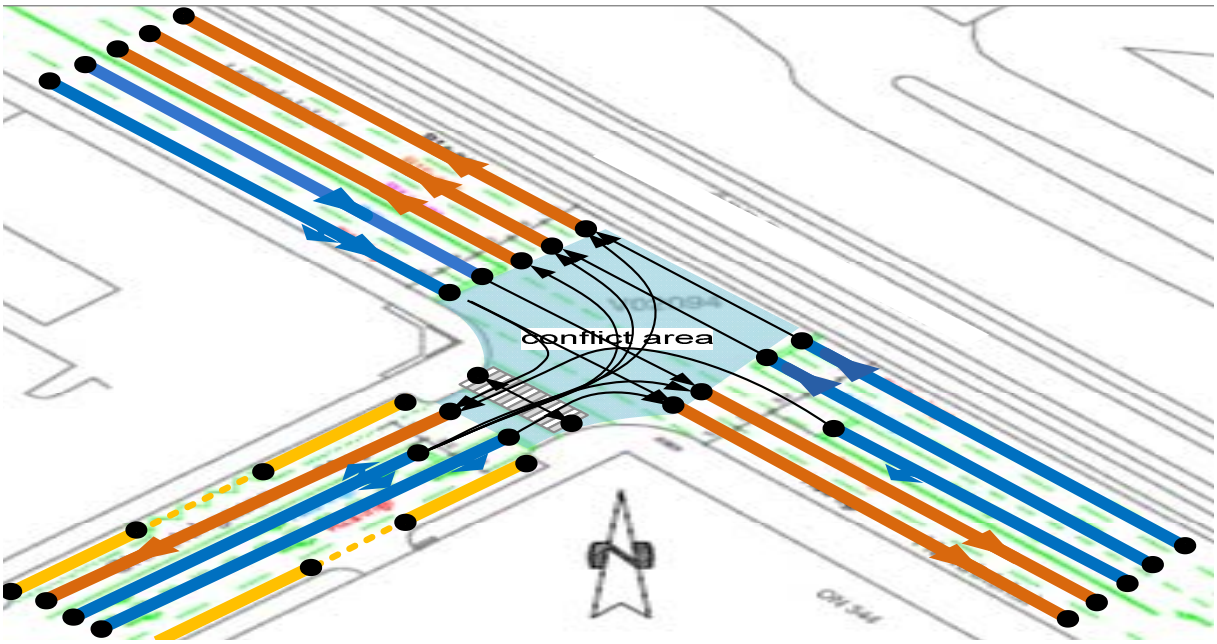

Figure 5: Lane topology and corresponding connection

Figure 5 gives an example of the topology of an intersection. The topology is organized in several approaches (three approaches in the given example) and a "conflict area" in the junction of the approaches. Each approach holds "ingressing" (driving direction towards the conflict area) and "egressing" lanes (driving direction away from the "conflict area"). Each lane (e.g. vehicle, pedestrian, etc.) consists of two or more waypoint (positioned in the middle of the lane). Basically each ingress lane is connected with one or more egress lanes which define the allowed maneuvers in the intersection. This "connection" includes the signal group identifier, which is the link for signalization between the topology and the corresponding signalling.

6.2 RLT service

The Road and Lane Topology service instantiated in an ITS-Station shall provide either the transmission or the reception service defined in clause 4.2. Additionally the Road and lane Topology service supports the following functionality:

- Continuous transmission for infinity of the MAPEM. As the MAPEM message is not changed very often in time, a stable release is stored within the ITS-S for continuous broadcast.
- Assembly and disassembly fragmented MAPEM fragments on an Application level as defined by the data element *{MAPEM.map.layerID}* ISO/TS 19091 [8].

6.3 RLT service message and version

The RLT service uses the message MAPEM as defined in Annex A. The header of MAPEM is defined in the data dictionary ETSI TS 102 894-2 [2]. The data elements of MAPEM payload are defined in ISO/TS 19091 [8], Annex G.

The *protocolVersion* (defined in *header*) of MAPEM message based on the present document is set to value "2".

6.4 RLT service dissemination

6.4.1 RLT service identification

The RLT service uses MAPEM which represents the topology/geometry of a set of lanes. E.g. considering an intersection MAPEM defines the topology of the lanes or parts of the topology of the lanes identified by the intersection reference identifier. The MAPEM does not change very often in time. The same MAPEM is retransmitted with the same content, unless the Application indicates to transmit a new MAPEM:

- If the size of the MAPEM exceeds the allowed message length (e.g. MTU), the RLT service fragments the message which will be transmitted in different messages. Each fragment is identified by the "layerID " as defined in ISO/TS 19091 [8], Annex G.

6.4.2 RLT service trigger, update, repetition and termination

The application triggers the Road and lane Topology service for the transmission of the MAPEM. The application provides all data content included in the MAPEM payload. The RLT service constructs a MAPEM and delivers it to the ITS Networking & Transport Layer for dissemination.

As the MAPEM content is only changed, e.g. if the road and lane topology is changed, the MAPEM remains stable in time. The MAPEM is re-broadcasted continuously.

The MAPEM transmission may be terminated if the ITS-S application requests the termination.

6.4.3 RLT service communication requirements

6.4.3.1 RLT service communication overview

The RLT service uses MAPEM to define all the road topological details. It uses the lane "connection" (between ingress and egress lanes) which includes the signal-group identifier which is the link to SPATEM signalling information. MAPEM shall be transmitted continuously together with the SPATEM to inform the traffic participant (driver, pedestrian, etc.) about the status of allowed maneuvers within the intersection conflict area. Due to potential different communication paths to the end users, the MAPEM may be disseminated using different access technologies for short range and long range communication.

6.4.3.2 RLT service communication requirements for short range access technologies

Table 8 provides the requirements for the broadcast communication. The structure of the requirements is in accordance with ISO/TS 17423 [i.2].

The ITS station management uses the communication requirements to select suitable ITS-S communication protocol stacks. Some examples of communication parameter settings that fulfil these requirements are specified in clause 11.

Table 8: RLT service communication requirements for short range access technologies

Requirement	Value	Comment
Operational parameters		
CSP_LogicalChannelType	SFCH	
CSP_SessionCont	n.a.	No continuous connectivity
CSP_AvgADUrate	255, 1 second (default)	
CSP_FlowType	n.a.	

Requirement	Value	Comment
CSP_MaxPrio	253	
CSP_PortNo	2 003	Port Number of the transport protocol (see ETSI TS 103 248 [15])
CSP_ExpFlowLifetime	n.a.	
Destination communication service parameters		
CSP_DestinationType	1: broadcast transmission 16: geocast transmission to an area given by geo-coordinates.	If the MDA is within direct communication range of the sending ITS-S, destination type 1 shall be used. If the MDA exceeds the direct communication range or is not within the direct communication range, destination type 16 shall be used
CSP_DestinationDomain	site-local	
CSP_CommDistance	400 m radius (default value)	
CSP_Directivity	n.a.	
Performance communication service parameters		
CSP_Resilience	High	Repeated transmission of the same message
CSP_MinThP	n.a.	
CSP_MaxLat	ms100 (8)	Response within less than 100 ms
CSP_MaxADU	Max message size allowed by access technology	
Security communication service parameters		
CSP_DataConfidentiality	n.a.	
CSP_DataIntegrity	required	
CSP_NonRepudiation	required	
CSP_SourceAuthentication	required	
Protocol communication service parameter		
Protocol-Req	n.a.	

RLT Application Identifier (AID)

The ITS AID of the RLT service is allocated in ETSI TS 102 965 [14].

RLT service security parameters

For security against misuse of keys it is necessary to change the pseudonym identity regularly. The default time for is given in Table 9. For special cases like offline working traffic light controllers where manually driven provision of pseudonym identity keys is necessary, longer periods of e.g. half a year are allowed and shall be agreed with the operator.

Table 9: RLT services security parameters

RLT service security parameters	
Authorization ticket validity	2 months (default value)

RLT Service Specific Permissions (SSP)

The interpretation of the SSP octet scheme is defined as depicted in Figure 6.

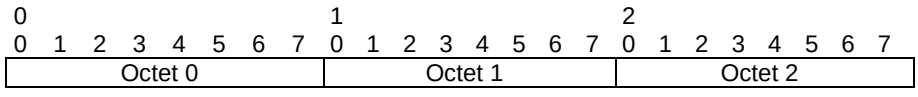

Figure 6: Format for the Octets

The SSP for the RLT service shall correspond to the octet scheme of Table 10.

Table 10: Octet Scheme for RLT service SSPs

Octet #	Description	Value
0	SSP version control	1
1	Service-specific parameter	see Table 11

The Service-specific parameter shall be as defined in Table 11.

Table 11: RLT service communication profile

Octet Position	Bit Position	RLT service SSP data Item	Bit Value
1	0 (80h) (MSBit)	Intersections geometry list allowed to transmit {MAPEM.map.intersections}	0: certificate not allowed to sign 1: certificate allowed to sign
1	1 (40h)	Road geometry list allowed to transmit {MAPEM.map.roadSegments}	0: certificate not allowed to sign 1: certificate allowed to sign
NOTE: All other bits of the SSP are not used and set to 0.			

6.4.3.3 RLT service dissemination parameters for long range communication

This clause provides the requirements for the long range unicast communication (e.g. usage of cellular network) in accordance with ISO/TS 17423 [i.2].

Table 12: RLT service communication requirements for long range access technologies

Requirement	Value	Comment
Operational communication service parameters		
CSP_LogicalChannelType	SFCH	Safety channel
CSP_SessionCont	n.a.	
CSP_AvgADUrate	n.a.	
CSP_FlowType	n.a.	
CSP_MaxPrio	n.a.	
CSP_PortNo	2 003	Port Number of the transport protocol (see ETSI TS 103 248 [15])
CSP_ExpFlowLifetime	n.a.	
Destination communication service parameters		
CSP_DestinationType	4: unicast	
CSP_DestinationDomain	global	
CSP_CommDistance	n.a.	
CSP_Directivity	n.a.	
Performance communication service parameters		
CSP_Resilience	required	
CSP_MinThP	n.a.	
CSP_MaxLat	n.a.	
CSP_MaxADU	Max message size allowed by access technology	
Security communication service parameters		
CSP_DataConfidentiality	n.a.	
CSP_DataIntegrity	required	
CSP_NonRepudiation	required	
CSP_SourceAuthentication	required	
Protocol communication service parameter		
Protocol-Req	n.a.	

7 Infrastructure to Vehicle Information (IVI) service

7.1 IVI service overview

IVI service is one instantiation of the infrastructure services to manage the generation, transmission and reception of the IVIM messages. An IVIM supports mandatory and advisory road signage such as contextual speeds and road works warnings. IVIM either provides information of physical road signs such as static or variable road signs, virtual signs or road works.

7.2 IVI service

The IVI service instantiated in an ITS-Station shall provide either the transmission or the reception service defined in clause 4.2.

The present document introduces an updated version if the IVI dictionary. But these changes are fully backward compatible, since these changes only relate to ASN.1 extension fields. Thus an ITS station conforming to ETSI TS 103 301 (V1.3.1) [19] can still decode a Release 2 IVIM - of course without recognizing the newly added content.

7.3 IVI service message and version

The IVI service uses the IVIM as defined in Annex A. The header of the IVIM is defined in the data dictionary ETSI TS 102 894-2 [2]. The data elements of the IVIM message payload are defined in ISO/TS 19321 [7].

The *protocolVersion* (defined in the header) of IVIM message based on the present document is set to value "2".

7.4 IVI service dissemination

7.4.1 IVI service identification

The IVIM identification is enabled by the parameter *{IVIM.ivi.mandatory.iviIdentificationNumber}*. Each time a new IVIM is generated upon an application request, a new *iviIdentificationNumber* (as defined in ISO/TS 19321 [7]) value shall be assigned by the IVI service.

When a iviIdentificationNumber is set, it shall be set to an recently unused value. In one possible implementation, the *iviIdentificationNumber* is randomly set to a recently unused value within the range as specified in ISO/TS 19321 [7].

An *iviIdentificationNumber* is linked to the organization providing the IVI service (e.g. the Service Provider, as defined in ISO/TS 17427-1 [10]). It enables the receiving ITS-S to differentiate IVIM messages transmitted from different service providers.

7.4.2 IVI service trigger, update, repetition and termination

IVI service trigger refers to the process of the generation and transmission of an IVIM when the IVI service of the sending ITS-S receives an application request. The IVI service shall then generate a new message with status *{IVIM.ivi.mandatory.iviStatus}* set to "*new*".

An IVIM content is updated e.g. by the service provider. The ITS-S application provides the update information to the IVI service at the sending ITS-S. The IVI service shall then generate an update IVIM with the *iviStatus* set to *update*.

An "*update"* is also used to change or add the end time to the IVIM. In some applications this corresponds to ending the service (logical end message).The parameter "*timestamp" {IVIM.ivi.mandatory.timeStamp}* is the identifier for i*viStatus* (*update*) in relation to a specific *iviIdentificationNumber*. The *timeStamp* represents the time stamp of the generation (if *IviStatus set to new*) or last change of information content (if *iviStatus set to update*) by the Service Provider.

The *iviIdentificationNumber* shall remain unchanged for *iviSStatus* set to update.

In between two consequent *iviStatus* updates, an IVIM shall be repeated by the IVI service of the sending ITS-S at a pre-defined repetition interval, in order that new ITS-S entering the MDA during the event validity duration may also receive the IVIM. This process is referred to as IVI service repetition. The IVI service repetition shall be activated under the request from the ITS-S application.

The IVI service termination indicates the end of the validity of the IVI service. An IVI service termination is either the ending of transmission, an application cancelation or an application negation: a Cancellation of the IVI service can only be provided by the organization that originally provided the IVI service; a Negation of the IVI service can be provided by other organizations. Termination of IVI service is achieved in the following ways:

- Ending of transmission by the ITS-S originally sending the IVIM:
  - The IVI service shall stop the IVIM transmission repetition automatically at the end of the repetition interval.
- IVI service cancellation by the Service Provider originating the IVIM:
  - In this case, the IVI service shall generate a cancellation IVIM with the *iviStatus* set to *cancellation*. For the generation of a cancellation IVIM, the *iviIdentificationNumber* shall be set to the *iviIdentificationNumber* of the message for which the IVI service negation refers to; the service provider identification *{IVIM.ivi.mandatory.serviceProviderId}* shall be set to the value of the originating Service Provider. The time stamp *{IVIM.ivi.mandatory.TimeStamp}* shall be set to the value of the latest received IVI of the same "iviIdentificationNumber".
- IVIM negation by another organization:
  - In this case, the IVI service of the sending ITS-S shall generate a negation IVIM, i.e. an IVIM with i*viStatus* set to *negation*. For the generation of a negation IVIM, the *iviIdentificationNumber* shall be set to the *iviIdentificationNumber* of the event for which the IVIM negation refers to; the *serviceProviderId* shall be set to the value of the originating Service Provider. The *timeStamp* shall be set to the value of the latest received IVIM of the same *iviIdentificationNumber*.

Once a cancellation IVIM or a negation IVIM is verified to be trustworthy by the receiving ITS-S, all information related to the previously received IVIM concerning the same *iviIdentificationNumber* may be considered as not valid any more, the IVI service may notify ITS-S applications of the event termination.

A cancellation IVIM or negation IVIM shall be transmitted at least once by the originating ITS-S per application request. It may be repeated by the IVI service of the originating ITS-S.

7.4.3 IVI service communication requirements

7.4.3.1 IVI service communication parameters for short-range communication

An IVIM shall be transmitted if applicable, e.g. when it is applicable in time (e.g. a speed limitation only valid between 8:00 and 20:00) and due to the context as determined by the sending ITS-S (e.g. a speed limitation applicable in case of fog).

An IVIM shall be disseminated to reach as many ITS-S as possible, located in the MDA. The MDA is provided by the ITS Application to the IVI service and is typically defined in a way that every receiving ITS-S has received at least once the IVIM before entering the DAZ (or if null the RZ) of the IVI.

The IVI service shall provide the MDA as destination area in the format compliant to the one as specified in ETSI EN 302 931 [9] to the ITS Networking & Transport Layer.

Table 13 provides the requirements for the broadcast communication. The structure of the requirements is in accordance with ISO/TS 17423 [i.2].

The ITS station management uses the communication requirements to select suitable ITS-S communication protocol stacks. Some examples of communication parameter settings profiles that fulfil these requirements are specified in clause 11.

Table 13: IVI service communication requirements for short range access technologies

Requirement	Value	Comment
Operational parameters		
CSP_LogicalChannelType	SFCH	
CSP_SessionCont	n.a.	
CSP_AvgADUrate	255, 1 second (default)	
CSP_FlowType	n.a.	

Requirement	Value	Comment
CSP_MaxPrio	254	
CSP_PortNo	2 006	Port Number of the transport protocol (see ETSI TS 103 248 [15])
CSP_ExpFlowLifetime	n.a.	
Destination communication service parameters		
CSP_DestinationType	1: broadcast transmission 16: geocast transmission to an area given by geo-coordinates.	If the MDA is within direct communication range of the sending ITS-S, destination type 1 shall be used. If the MDA exceeds the direct communication range or is not within the direct communication range, destination type 16 shall be used
CSP_DestinationDomain	site-local	
CSP_CommDistance	400 m radius (default value)	
CSP_Directivity	n.a.	
Performance communication service parameters		
CSP_Resilience	High	Repeated transmission of the same message
CSP_MinThP	n.a.	
CSP_MaxLat	ms100 (8)	Response within less than 100 ms
CSP_MaxADU	Max message size allowed by access technology	
Security communication service parameters		
CSP_DataConfidentiality	n.a.	
CSP_DataIntegrity	required	
CSP_NonRepudiation	required	
CSP_SourceAuthentication	required	
Protocol communication service parameter		
Protocol-Req	n.a.	

IVI Application Identifier (AID)

The ITS AID of the IVI service is allocated in ETSI TS 102 965 [14].

IVI Service Specific Permissions (SSP)

The IVIM contains the identification of the organization originating the IVIM, e.g. the Service Provider that originated it. An R-ITS-S is only allowed to send out IVIM for a defined Service Provider.

The SSP for the IVIM is defined by a variable number of octets and shall correspond to the octet scheme of Table 14. For each octet, the Most Significant Bit (MSB) shall be the leftmost bit. The transmission order shall always be the MSB first. The interpretation of the SSP octet scheme is defined as depicted in Figure 7.

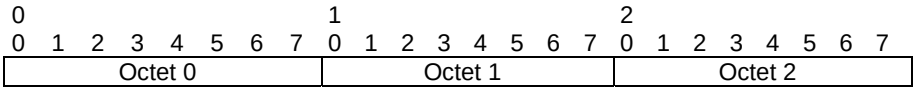

Figure 7: Format for the Octets

Table 14: Octet Scheme for IVI SSPs

Octet #	Component	Value
0	SSP version control	1
1 to 3	serviceProviderId	Identification of the Service Provider for which the R-ITS-S is allowed to send out IVIM and to which the Service-specific parameter apply, using the DE Provider from ISO/TS 19321 [7].
4 to 5	Service-specific parameter	see Table 15.
NOTE: For Release 2 the SSP encoding has not been changed (no bytes added), only the semantics of three previously unused bits has been defined. Release 1 receivers are able to decode the SSPs and are free to ignore the meaning of those previously unused bits. This is a behavior recommended also in SAE J2945/5 [i.10]. Release 2 receivers shall interpret those bits in relation to the new message content.		

The Service-specific parameter shall be as defined in Table 15.

Table 15: IVI service SSPs

Octet Position	Bit Position	IVIM data Item	Bit Value
4	0 (80h) (MSBit)	Vienna Convention Code for road sign {IVIM.ivi.optional.gic.GicPart. roadSignCodes.RSCode.code. viennaConvention}	1: The sending ITS-S is authorized to sign "General IVI container" using the Vienna convention road signs 0: The sending ITS-S is not authorized
4	1 (40h)	ISO/TS 14823 [i.3] traffic sign pictogram (danger warning) {IVIM.ivi.optional.gic.GicPart. roadSignCodes.RSCode.code. iso14823.pictogramCode. serviceCategoryCode. trafficSignPictogram.dangerWarning}	1: The sending ITS-S is authorized to sign the "General IVI container" using the ISO/TS 14823 [i.3] road signs with traffic sign pictogram set to dangerWarning 0: The sending ITS-S is not authorized
4	2 (20h)	ISO/TS 14823 [i.3] traffic sign pictogram (regulatory) {IVIM.ivi.optional.gic.GicPart. roadSignCodes.RSCode.code. iso14823.pictogramCode. serviceCategoryCode. trafficSignPictogram.regulatory}	1: The sending ITS-S is authorized to sign the "General IVI container" using the ISO/TS 14823 [i.3] road signs with traffic sign pictogram set to regulatory 0: The sending ITS-S is not authorized
4	3 (10h)	ISO/TS 14823 [i.3] traffic sign pictogram (informative) {IVIM.ivi.optional.gic.GicPart. roadSignCodes.RSCode.code. iso14823.pictogramCode. serviceCategoryCode. trafficSignPictogram.informative}	1: The sending ITS-S is authorized to sign the "General IVI container" using the ISO/TS 14823 [i.3] road signs with traffic sign pictogram set to informative 0: The sending ITS-S is not authorized
4	4 (08h)	ISO/TS 14823 [i.3] public facilities pictogram {IVIM.ivi.optional.gic.GicPart. roadSignCodes.RSCode.code. iso14823.pictogramCode. serviceCategoryCode. publicFacilitiesPictogram}	1: The sending ITS-S is authorized to sign the "General IVI container" using the ISO/TS 14823 [i.3] road signs with public facilities pictogram 0: The sending ITS-S is not authorized
4	5 (04h)	ISO/TS 14823 [i.3] ambient or road conditions pictogram (ambient condition) {IVIM.ivi.optional.gic.GicPart. roadSignCodes.RSCode.code. iso14823.pictogramCode. serviceCategoryCode. ambientOrRoadContitionPictogram.ambientCondition}	1: The sending ITS-S is authorized to sign the "General IVI container" using the ISO/TS 14823 [i.3] road signs with ambient and road conditions set to ambientCondition 0: The sending ITS-S is not authorized.
4	6 (02h)	ISO/TS 14823 [i.3] ambient or road conditions pictogram (road condition) {IVIM.ivi.optional.gic.GicPart. roadSignCodes.RSCode.code. iso14823.pictogramCode. serviceCategoryCode. ambientOrRoadContitionPictogram. roadCondition}	1: The sending ITS-S is authorized to sign the "General IVI container" using the ISO/TS 14823 [i.3] road signs with ambient and road conditions set to roadCondition 0: The sending ITS-S is not authorized.
4	7 (01h) (LSBit)	ITIS codes {IVIM.ivi.optional.gic.GicPart. roadSignCodes.RSCode.code. itisCodes}	1: The sending ITS-S is authorized to sign the "General IVI container" using the ITIS codes 0: The sending ITS-S is not authorized
5	0 (80h) (MSBit)	Lane status {IVIM.ivi.optional.gic.GicPart. laneStatus}	1: The sending ITS-S is authorized to sign the "General IVI container" using the laneStatus 0: The sending ITS-S is not authorized
5	1 (40h)	Road configuration container {IVIM.ivi.optional.rcc}	1: The sending ITS-S is authorized to sign the "Road Configuration Container" 0: The sending ITS-S is not authorized
5	2 (20h)	Text container {IVIM.ivi.optional.tc}	1: The sending ITS-S is authorized to sign the "Text Container" 0: The sending ITS-S is not authorized

Octet Position	Bit Position	IVIM data Item	Bit Value
5	3 (10h)	Layout Container {IVIM.ivi.optional.lac}	1: The sending ITS-S is authorized to sign the "Layout Container" 0: The sending ITS-S is not authorized
5	4 (08h)	IVI Status (negation) {IVIM.ivi.mandatory.iviStatus}	1: The sending ITS-S is authorized to sign use the iviStatus set to negation 0: The sending ITS-S is not authorized
5	5 (04h)	Automated Vehicle Container {IVIM.ivi.optional.avc}	1: The sending ITS-S is authorized to sign the "Automated Vehicle Container" 0: The sending ITS-S is not authorized
5	6 (02h)	Map Location Container {IVIM.ivi.optional.mlc}	1: The sending ITS-S is authorized to sign the "Map Location Container" 0: The sending ITS-S is not authorized
5	7 (01h)	Road Surface Container {IVIM.ivi.optional.rsc}	1: The sending ITS-S is authorized to sign the "Road Surface Container" 0: The sending ITS-S is not authorized
NOTE: All other bits of the SSP are not used and set to 0.			

7.4.3.2 IVI service dissemination parameters for long-range communication

This clause provides the requirements for the long range unicast communication (e.g. usage of cellular network) in accordance with ISO/TS 17423 [i.2].

Table 16: IVI service communication requirements for long range access technologies

Requirement	Value	Comment
Operational parameters		
CSP_LogicalChannelType	SCH	Safety channel
CSP_SessionCont	n.a.	No continuous connectivity
CSP_AvgADUrate	n.a.	
CSP_FlowType	n.a.	
CSP_MaxPrio	n.a.	
CSP_PortNo	2 006	Port Number of the transport protocol (see ETSI TS 103 248 [15])
CSP_ExpFlowLifetime	n.a.	
Destination communication service parameters		
CSP_DestinationType	4: Unicast	
CSP_DestinationDomain	Global	
CSP_CommDistance	n.a.	
CSP_Directivity	n.a.	
Performance communication service parameters		
CSP_Resilience	n.a.	
CSP_MinThP	n.a.	
CSP_MaxLat	sec (16)	Response within less than 10 s
CSP_MaxADU	Max message size allowed by access technology	
Security communication service parameters		
CSP_DataConfidentiality	n.a.	[i.2]
CSP_DataIntegrity	required	
CSP_NonRepudiation	required	
CSP_SourceAuthentication	required	
Protocol communication service parameter		
Protocol-Req	n.a.	

8 Traffic Light Control (TLC) service

8.1 TLC service overview

The Traffic Light Control service is one instantiation of the infrastructure services to manage the generation, transmission of SREM messages and SSEM messages. The TLC service supports prioritization of e.g. public transport and public safety vehicles (ambulance, fire brigade, etc.) to traverse a signalized road infrastructure (e.g. intersection) as fast as possible or using a higher priority than ordinary traffic participants. The corresponding SREM is sent by an ITS-S (e.g. vehicle) to the traffic infrastructure environment (e.g. R-ITS-S, TCC). In a signalized environment (e.g. intersection) the SREM is sent for requesting traffic light signal priority (public transport) signal pre-emption (public safety). The service may not only be requested for the approaching signalized environment but also for a sequence of e.g. intersections along a defined traffic route. In response to the request the infrastructure (e.g. R-ITS-S/TLC or TCC) will acknowledge with a SSEM notifying if the request has been granted, cancelled or changed in priority due to a more relevant signal request (e.g. ambulance).

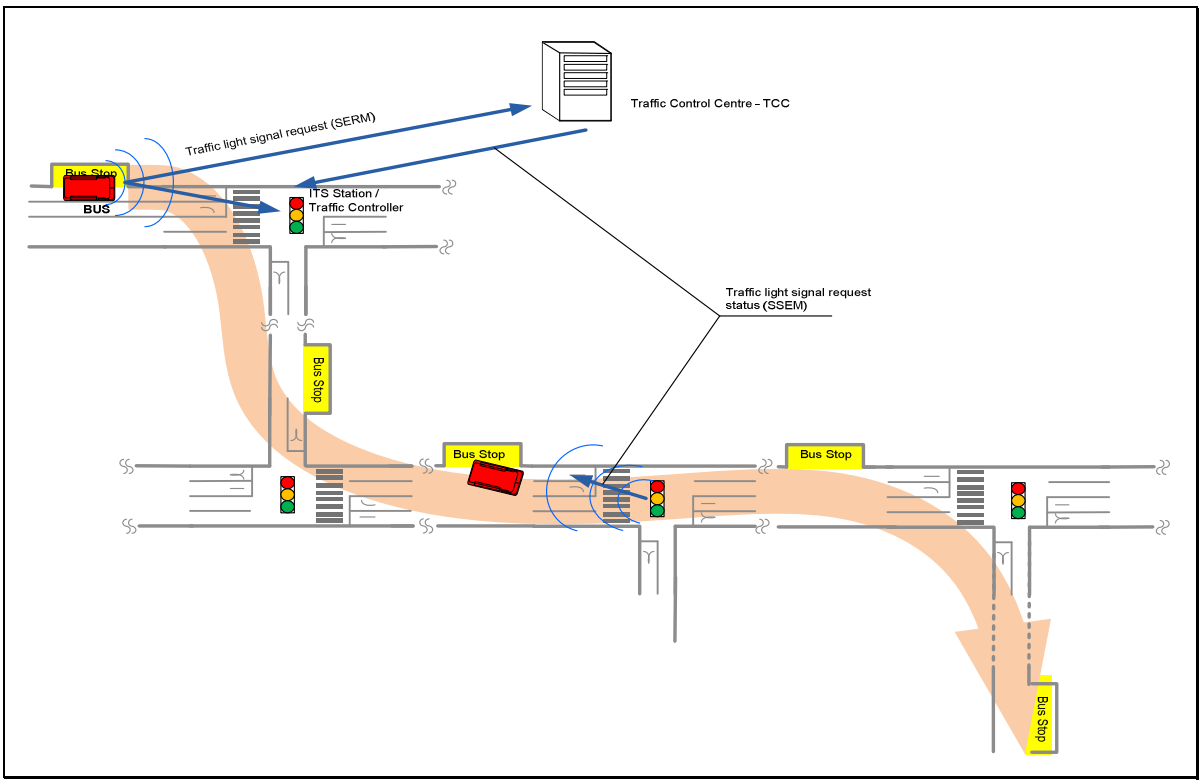

Figure 8: Traffic Light Control service example

Figure 8 gives an example of a bus requesting traffic light signal priority (using SREM) for the defined bus route to the Traffic Control Center (TCC). The request is sent via the ITS-S Station connected to the Traffic Controller or by other communication facilities. Multiple requests, related to different intersections, are possible to transmit using one SREM only. Depending on prioritization needs, a single request to the approaching Traffic Controller is also possible. The Traffic light controller analyses the request and returns a SSEM as feedback. Alternatively if the SREM request has been forwarded by the traffic controller to the TCC the SSEM reply will be generated by the TCC and distributed via the R-ITS-S of the corresponding TLC.

8.2 TLC service

The TLC service shall provide the communication service defined in clause 4.2 and support additionally the following functionality:

- Generation of SREM with a single request or sequence of signal requests (e.g. related to several signalized intersections).

- Generation of SSEM with a signal status response.
- Single or continuous transmission of SREM and SSEM.
- Reception of SREM and SSEM.

8.3 TLC service message and version

The Signal Control service uses the SREM and the SSEM as defined in Annex A. The header of the SREM and the SSEM are defined in the data dictionary ETSI TS 102 894-2 [2]. The data elements of the SREM and the SSEM payload are defined in ISO/TS 19091 [8].

The *protocolVersion* (defined in the header) of SREM based on the present document is set to value "2".

The *protocolVersion* (defined in the header) of SSEM based on the present document is set to value "2".

8.4 TLC service dissemination

8.4.1 TLC service identification

The SREM is identified by a request identification which is unique. Additionally a sequence number identifies a sequence of requests. If the request or one of the requests with the same request identification has changed, the sequence number will be incremented. For having a clear relation between an SREM request and the SSEM status response, the request identification is used in both messages.

The SSEM is a reply to a SREM. It uses the request identification of the SREM for identification.

8.4.2 TLC service trigger, update, repetition and termination

SREM

The SREM is transmitted based on the needs of the vehicle operator and triggered by applications. The application provides all data included in SREM. The traffic light control service shall construct a SREM payload and deliver it to the N&T (Networking and Transport) layer for dissemination.

The SREM may be repeated (depending on data content and on implementation).

The SREM transmission may be terminated, if one of the following conditions is reached:

- Application requests the termination of SREM transmission.
- Application does not provide update for SREM at the expiry of the current SREM content.

SSEM

An ITS-S forwards the request to the local traffic controller (TLC) or to the Traffic Control Center (TCC) for further operation. Based on the decision of the TLC or the TCC the ITS-S application generates a SSEM to inform the requestor and adjacent traffic participants (e.g. vehicles, pedestrians) about the status of the request.

The SSEM is transmitted by the infrastructure equipment (ITS-S road side unit) as response to a SREM. Based on changes or incoming SREM with higher priority requests (e.g. public safety "overrules" a Bus request) a revised SSEM will be transmitted to reflect the new status.

The application provides all data included in SSEM payload. The Traffic Light Control service shall construct a SSEM payload and deliver it to the Networking and Transport Layer for dissemination.

The SSEM may be repeated (depending on data content and on implementation).

The SSEM transmission may be terminated, if one of the following conditions is reached:

- Application requests the termination of SSEM transmission.

- Application does not provide update for SSEM at the expiry of the current SSEM content.

8.4.3 TLC service communication parameters

8.4.3.1 TLC service communication overview

The SREM is transmitted on demand (e.g. bus driver) or automatically by an application (e.g. in the bus) based on external conditions (e.g. position, reception of a specific SPATEM, etc.) It is transmitted once or continuously depending on the needs of the implementation. The SSEM is sent as response to a SREM. Both messages may use short range or wide area communication.

8.4.3.2 TLC service communication parameters for short range access technologies

Table 17 provides the requirements for the broadcast communication. The structure of the requirements is in accordance with ISO/TS 17423 [i.2].

The ITS station management uses the communication requirements to select suitable ITS-S communication protocol stacks. Some examples of communication parameter settings that fulfil these requirements are specified in clause 11.

Table 17: TLC service communication profile for short range access technologies

Requirement	Value	Comment
Operational parameters		
CSP_LogicalChannelType	SFCH	
CSP_SessionCont	n.a.	No continuous connectivity
CSP_AvgADUrate	0	No average transmission
CSP_FlowType	n.a.	
CSP_MaxPrio	254	
CSP_PortNo	2 007	SREM port number of the transport protocol (see ETSI TS 103 248 [15])
	2 008	SSEM port number of the transport protocol (see ETSI TS 103 248 [15])
CSP_ExpFlowLifetime	n.a.	
Destination communication service parameters		
CSP_DestinationType	1: broadcast transmission 16: geocast transmission to an area given by geo-coordinates.	If the MDA is within direct communication range of the sending ITS-S, destination type 1 shall be used. If the MDA exceeds the direct communication range or is not within the direct communication range, destination type 16 shall be used
CSP_DestinationDomain	site-local	
CSP_CommDistance	400 m radius (default value)	Short range communication is used
CSP_Directivity	n.a.	
Performance communication service parameters		
CSP_Resilience	High	Repeated transmission of the same message
CSP_MinThP	n.a.	
CSP_MaxLat	ms100 (8)	Response within less than 100 ms
CSP_MaxADU	Max message size allowed by access technology	
Security communication service parameters		
CSP_DataConfidentiality	n.a.	
CSP_DataIntegrity	required	
CSP_NonRepudiation	required	
CSP_SourceAuthentication	required	
Protocol communication service parameter		
Protocol-Req	n.a.	

TLC Application Identifier for SREM and SSEM (AID)

The ITS AIDs are allocated in ETSI TS 102 965 [14]:

- TLC Request Service (SREM)
- TLC Status Service (SSEM)

TLC service security parameters

For security against misuse of keys also for fix installations it is necessary to change the pseudonym identity regularly. The default time for is given in Table 4. For special cases like offline working traffic light controllers where manually driven provision of pseudonym identity keys is necessary, longer periods of e.g. half a year are allowed and should be agreed with the operator.

Table 18: TLC service security parameters

TLC service security parameters	
Authorization ticket validity	2 months (default value)

TLC Service Specific Permissions (SSP)

The interpretation of SSP octet scheme is defined as depicted in Figure 9.

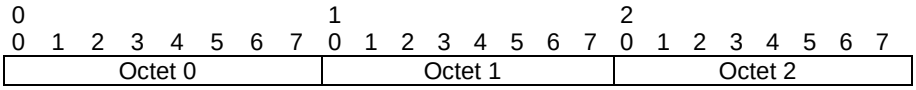

Figure 9: Format for the Octets

The SSP for the SREM shall correspond to the octet scheme of Table 19.

Table 19: Octet scheme for TLC Request service (SREM) SSPs

Octet #	Description	Value
0	SSP version control	2
1-3	Service-specific parameter	see Table 20

The service-specific parameter for SREM shall be as defined in Table 20.

Table 20: SSP Definitions for SREM

Octet Position	Bit Position	SREM data Item	Bit Value
1	0 (80h) (MSBit)	Signal request {SREM.srm.requests}	0: certificate not allowed to sign 1: certificate allowed to sign
1	1 (40h)	Requestor role (public transport) {SREM.srm.requestor.type.role. publicTransport}	0: certificate not allowed to sign 1: certificate allowed to sign
1	2 (20h)	Requestor role (special transport) {SREM.srm.requestor.type.role. specialTransport}	0: certificate not allowed to sign 1: certificate allowed to sign
1	3 (10h)	Requestor role (dangerousGoods) {SREM.srm.requestor.type.role. dangerousGoods}	0: certificate not allowed to sign 1: certificate allowed to sign
1	4 (08h)	Requestor role (roadWork) {SREM.srm.requestor.type.role. roadWork}	0: certificate not allowed to sign 1: certificate allowed to sign
1	5 (04h)	Requestor role (roadRescue) {SREM.srm.requestor.type.role. roadRescue}	0: certificate not allowed to sign 1: certificate allowed to sign
1	6 (02h)	Requestor role (emergency) {SREM.srm.requestor.type.role. emergency}	0: certificate not allowed to sign 1: certificate allowed to sign
1	7 (01h)	Requestor role (safetyCar) {SREM.srm.requestor.type.role. safetyCar}	0: certificate not allowed to sign 1: certificate allowed to sign
2	0 (80h) (MSBit)	Requestor role (truck) {SREM.srm.requestor.type.role. truck}	0: certificate not allowed to sign 1: certificate allowed to sign
2	1 (40h)	Requestor role (motorcycle)	0: certificate not allowed to sign 1: certificate allowed to sign

Octet Position	Bit Position	SREM data Item	Bit Value
		{SREM.srm.requestor.type.role. motorcycle}	
2	2 (20h)	Requestor role (police) {SREM.srm.requestor.type.role. police}	0: certificate not allowed to sign 1: certificate allowed to sign
2	3 (10h)	Requestor role (fire) {SREM.srm.requestor.type.role. fire}	0: certificate not allowed to sign 1: certificate allowed to sign
2	4 (08h)	Requestor role (ambulance) {SREM.srm.requestor.type.role. ambulance}	0: certificate not allowed to sign 1: certificate allowed to sign
2	5 (04h)	Requestor role (dot) {SREM.srm.requestor.type.role. dot}	0: certificate not allowed to sign 1: certificate allowed to sign
2	6 (02h)	Requestor role (transit) {SREM.srm.requestor.type.role. transit}	0: certificate not allowed to sign 1: certificate allowed to sign
2	7 (01h)	Requestor role (slowMoving) {SREM.srm.requestor.type.role. slowMoving}	0: certificate not allowed to sign 1: certificate allowed to sign
3	0 (80h) (MSBit)	Requestor role (cyclist) {SREM.srm.requestor.type.role. cyclist}	0: certificate not allowed to sign 1: certificate allowed to sign
3	1 (40h)	Requestor role (pedestrian) {SREM.srm.requestor.type.role. pedestrian}	0: certificate not allowed to sign 1: certificate allowed to sign
3	2 (20h)	Requestor role (military) {SREM.srm.requestor.type.role. military}	0: certificate not allowed to sign 1: certificate allowed to sign
NOTE: All other bits of the SSP are not used and set to 0.			

The SSP for the SSEM shall correspond to the octet scheme of Table 21.

Table 21: Octet scheme for TLC Status service (SSEM) SSPs

Octet #	Description	Value
0	SSP version control	1

Despite the version no other fields are specified.

8.4.3.3 TLC service communication parameters for long range communication

This clause provides the communication requirements for the long range unicast communication (e.g. usage of cellular network) in accordance with ISO/TS 17423 [i.2].

Table 22: TLC service communication profile for long range access technologies

Requirement	Value	Comment
Operational parameters		
CSP_LogicalChannelType	SFCH	General purpose or Safety channel
CSP_SessionCont	n.a.	
CSP_AvgADUrate	n.a.	No repetition
CSP_FlowType	n.a.	
CSP_MaxPrio	n.a.	
CSP_PortNo	2 007	SREM port number of the transport protocol (see ETSI TS 103 248 [15])
	2 008	SSEM port number of the transport protocol (see ETSI TS 103 248 [15])
CSP_ExpFlowLifetime	n.a.	
Destination communication service parameters		
CSP_DestinationType	4: unicast	
CSP_DestinationDomain	global	

Requirement	Value	Comment
CSP_CommDistance	n.a.	
CSP_Directivity	n.a.	
Performance communication service parameters		
CSP_Resilience	required	
CSP_MinThP	n.a.	
CSP_MaxLat	n.a.	
CSP_MaxADU	Max message size allowed by access technology	
Security communication service parameters		
CSP_DataConfidentiality	n.a.	
CSP_DataIntegrity	required	
CSP_NonRepudiation	required	
CSP_SourceAuthentication	required	
Protocol communication service parameter		
Protocol-Req	n.a.	

9 GNSS Positioning Correction (GPC) service

9.1 GPC service overview

The GPS service uses positioning correction message for GNSS as defined by the RTCM (Radio Technical Commission For Maritime Services - https://www.rtcm.org/). The RTCMEM message enables several types of position corrections (e.g. GPS, GLONAS, RTK). The RTCM correction data is generated by road side equipment (stationary GNSS Base station) and used for correction in receiving mobile stations (rover).

9.2 GPC service

The GNSS positioning correction service instantiated in an ITS-Station shall provide the communication services defined in clause 4.2.

9.3 GPC service message and version

The GPC service uses the message RTCMEM defined in Annex A. The header of RTCMEM is defined in the data dictionary ETSI TS 102 894-2 [2]. The data elements of RTCMEM payload are defined in the Annex A of the present document.

The *protocolVersion* (defined in the header) of RTCMEM based on the present document is set to value "1".

9.4 GPC service dissemination

9.4.1 GPC service identification

The GPC service provides real-time information for GNSS positioning correction data, There is no additional identifier needed to distinguish a RTCMEM from a previous one.

9.4.2 GPC service trigger, update, repetition and termination

The application triggers the GPC service for the transmission of the RTCMEM. The application provides all data content included in the RTCMEM payload. The GPC service constructs a RTCMEM and delivers it to the ITS Networking & Transport Layer for dissemination. The RTCMEM is not repeated.

The RTCMEM transmission may be terminated if the ITS-S application requests the termination.

NOTE: To avoid packet collisions on air GPC should not be triggered or updated in a time synchronous manner.

9.4.3 GPC service communication requirements

9.4.3.1 GPC service communication overview

The GPC service uses RTCMEM to disseminate the GNSS correction data. It transmits continuously in real-time the information relevant for enabling accurate positioning to the surrounding moving ITS stations. The goal is to support all traffic participants to execute safely location based maneuvers (e.g. for safe execution of maneuvers across a conflict area of an intersection).

9.4.3.2 GPC service communication requirements for short range access technologies

Table 8 provides the requirements for the broadcast communication. The structure of the requirements is in accordance with ISO/TS 17423 [i.2].

The ITS station management uses the communication requirements to select suitable ITS-S communication protocol stacks. Some examples of communication parameter settings that fulfil these requirements are specified in clause 11.

Table 23: GPC service communication requirements for short range access technologies

Requirement	Value	Comment
Operational parameters		
CSP_LogicalChannelType	GPCH/SFCH	
CSP_SessionCont	n.a.	
CSP_AvgADUrate	255, 1 second (default)	
CSP_FlowType	n.a.	
CSP_MaxPrio	252	
CSP_PortNo	2 013	Port Number of the transport protocol (see ETSI TS 103 248 [15])
CSP_ExpFlowLifetime	n.a.	
Destination communication service parameters		
CSP_DestinationType	1: broadcast transmission 16: geocast transmission to an area given by geo-coordinates.	If the MDA is within direct communication range of the sending ITS-S, destination type 1 shall be used. If the MDA exceeds the direct communication range or is not within the direct communication range, destination type 16 shall be used
CSP_DestinationDomain	site-local	
CSP_CommDistance	400 m radius (default value)	
CSP_Directivity	n.a.	
Performance communication service parameters		
CSP_Resilience	High	Repeated transmission of the same message
CSP_MinThP	n.a.	
CSP_MaxLat	ms100 (8)	Response within less than 100 ms
CSP_MaxADU	Max message size allowed by access technology	
Security communication service parameters		
CSP_DataConfidentiality	n.a.	
CSP_DataIntegrity	required	
CSP_NonRepudiation	required	
CSP_SourceAuthentication	required	
Protocol communication service parameter		
Protocol-Req	n.a.	

GPC Application Identifier (AID)

The ITS AID of the GPC service is allocated ETSI TS 102 965 [14].

GPC service security parameters

For security against misuse of keys it is necessary to change the pseudonym identity regularly. The default time for is given in Table 9. For special cases like offline working traffic light controllers where manually driven provision of pseudonym identity keys is necessary, longer periods of e.g. half a year are allowed and shall be agreed with the operator.

Table 24: GPC services security parameters

GPC service security parameters	
Authorization ticket validity	2 months (default value)

GPC service specific permissions (SSP)

The interpretation of the SSP octet scheme is defined as depicted in Figure 6.

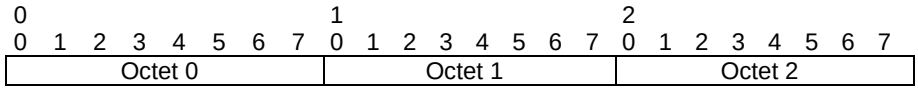

Figure 10: Format for the Octets

The SSP for the GPC service shall correspond to the octet scheme of Table 10.

Table 25: Octet Scheme for GPC service SSPs

Octet #	Description	Value
0	SSP version control	1

No Service-specific parameter defined.

9.4.3.3 GPC service dissemination parameters for long range communication

This clause provides the requirements for the long range unicast communication (e.g. usage of cellular network) in accordance with ISO/TS 17423 [i.2].

Table 26: GPC service communication requirements for long range access technologies

Requirement	Value	Comment
Operational communication service parameters		
CSP_LogicalChannelType	SFCH/GPCH	
CSP_SessionCont	n.a.	
CSP_AvgADUrate	n.a.	No repetition
CSP_FlowType	n.a.	
CSP_MaxPrio	n.a.	
CSP_PortNo	2 013	Port Number of the transport protocol (see ETSI TS 103 248 [15])
CSP_ExpFlowLifetime	n.a.	
Destination communication service parameters		
CSP_DestinationType	4: unicast	
CSP_DestinationDomain	global	
CSP_CommDistance	n.a.	
CSP_Directivity	n.a.	
Performance communication service parameters		
CSP_Resilience	required	
CSP_MinThP	n.a.	
CSP_MaxLat	n.a.	
CSP_MaxADU	Max message size allowed by access technology	
Security communication service parameters		
CSP_DataConfidentiality	n.a.	
CSP_DataIntegrity	required	
CSP_NonRepudiation	required	

Requirement	Value	Comment
CSP_SourceAuthentication	required	
Protocol communication service parameter		
Protocol-Req	n.a.	

10 Basic services running on ITS infrastructure devices

10.1 Basic service overview

Infrastructure ITS devices (e.g. road side unit) will communicate to vehicles/pedestrians and are on the other side connected to traffic controllers, traffic control centers (urban, interurban) or work in a standalone operation mode. From the application point of view, they use the same services like all other ITS stations (e.g. DEN, CA) and implement, depending on their role, additional infrastructure related applications.

10.2 DEN service on ITS infrastructure devices

Infrastructure ITS devices shall be able to transmit and to receive DENMs and provide the DEN (Decentralized Environmental Notification) service as defined in ETSI EN 302 637-3 [13]. Due to the role of the infrastructure device additional applications may run using the DEN basic service:

- Generation and transmission of DENM based on information of the directly attached devices (e.g. traffic light controller, traffic warning trailer).
- Generation and transmission of DENM based on traffic data received from the backbone traffic control infrastructure (e.g. traffic control center).
- Forwarding of DENM generated by the backbone ITS infrastructure (e.g. TCC) to other ITS stations (e.g. via ITS-G5, LTE-V2X sidelink, WLAN, UDP-IP, TCP-IP data services).
- Forwarding of DENM received from other ITS stations to the backbone ITS infrastructure (e.g. TCC).

10.3 CA service on ITS infrastructure devices

Infrastructure ITS devices shall be able to transmit CAM's and provide the CA (Common Awareness) service as defined in ETSI EN 302 637-2 [12]. Due to the role of the infrastructure device additional applications may run using the CA basic service:

- Generation of CAM's for notification of protected communication zones (e.g. Tolling stations).
- Forwarding of CAM's received from other ITS stations to the backbone ITS infrastructure (this requires sufficient backbone channel capacity).
- Aggregation of CAM's (e.g. for purpose of acquisition of probe vehicle data) for minimizing backbone channel.

11 Communication Profiles

11.1 Introduction

The messages for infrastructure services as specified in the present document shall use one of the following communication profiles:

- CPS_001 Transmission of ADU over ITS-G5.

- CPS_002 Transmission of ADU over WLAN 2,4 GHz in infrastructure mode.
- CPS_003 Transmission of ADU over WLAN 5 GHz in infrastructure mode.
- CPS_004 Transmission of ADU over LTE-V2X sidelink.
- CPS_005 Transmission of ADU using IP based data services.

Details of the profiles are described in clauses 11.2 to 11.7.

11.2 Basic communication profile settings

The communication profiles defines in the following clauses 11.3 to 11.7 use different communication access but shall all use the mandatory Geonetwork Protocol (ETSI EN 302 636-4-1 [3]) and the Basic Transport Protocol (ETSI EN 302 636-5-1 [4]). This assures interoperability, application security and authorization mechanism among different communication modes. The following communication parameters in Table 27 settings apply to the Geonetwork Protocol and the Basic Transport Protocol.

Table 27: Basic communication parameter settings

Parameter	Single_Hop (SHB)	GBC
ISO/TS 17423 [i.2] DestinationType	broadcast (1)	geoCast (16)
BTP Type	2 (BTP header type B)	
BTP Source port	N/A	
BTP Destination port	As specified in ETSI TS 103 248 [15]	
BTP Destination port info	N/A	
GN Packet transport type	SHB (Header Type: 5, Header Sub-type: 0)	GBC (Header Type:4, Header Sub-type: 0,1, or 2) The choice of sub-type is implementation-dependent based on the destination area
GN Destination address	N/A	Destination area
GN Security profile	As specified in clause 12	
GN Maximum packet lifetime	As specified in clauses 5 to 8 for the corresponding infrastructure service	
GN Repetition interval	If applicable as specified in clauses 5 to 8	
GN Maximum repetition time		
GN Maximum hop limit	N/A	Implementation dependent, based on the destination area
GN Traffic class	The traffic class is defined for each message in Table 1	
Length	Length of Facilities layer data	
Data	Facilities layer data	

11.3 CPS_001

This profile defines the communication parameter settings for dissemination of an ADU using GeoNetworking/BTP over ITS G5. The ITS station shall implement the following protocols:

- Basic Transport Protocol (ETSI EN 302 636-5-1 [4]) using parameter as defined in clause 11.2.
- GeoNetworking protocol (ETSI EN 302 636-4-1 [3]) using parameter as defined in clause 11.2.

Access layer specification for ITS Systems operating in the 5 GHz frequency band (ETSI EN 302 663 [16]).

Messages disseminated via the CPS_001 communication profile use the traffic classes as defined in Table 28.

Table 28: Traffic classes for CPS_001

CSP_MaxPrio	TC ID	AC
255	0	AC_VO
254	1	AC_VI
253	2	AC_BE
252	3	AC_BK
NOTE: For details on TC see ETSI TS 102 636-4-2 [18]. For details on AC see ETSI EN 302 663 [16].		

11.4 CPS_002

This profile defines the communication settings for dissemination of an ADU using GeoNetworking/BTP over WLAN in infrastructure mode in the 2,4 GHz frequency band (ISM). The ITS station shall implement the following protocols:

- Basic Transport Protocol (ETSI EN 302 636-5-1 [4]) using parameter as defined in clause 11.2.
- GeoNetworking protocol (ETSI EN 302 636-4-1 [3]) using parameter as defined in clause 11.2.
- WLAN (IEEE 802.11^{TM}-2016 [i.4]).
- Default Service Set Identifier - SSID: CITSWLAN.
- Default Passphrase: CooperativeItsWlan.

NOTE 1: IEEE 802.11g^{TM} is backward compatible with IEEE 802.11b, meaning that IEEE 802.11g access points will work with IEEE 802.11b wireless network adapters and vice versa.

NOTE 2: The default SSID and Passphrase are used if no special values are defined for an installation.

Messages disseminated via the CPS_002 communication profile use the traffic classes as defined in Table 29.

Table 29: Traffic classes for CPS_002

CSP_MaxPrio	TC ID	AC
255	0	AC_VO
254	1	AC_VI
253	2	AC_BE
252	3	AC_BK
NOTE: For details on TC see ETSI TS 102 636-4-2 [18]. For details on AC see ETSI EN 302 663 [16].		

11.5 CPS_003

This profile defines the communication settings for dissemination of an ADU using GeoNetworking/BTP over WLAN in infrastructure mode in the 5 GHz frequency band. The ITS station shall implement the following protocols:

- Basic Transport Protocol (ETSI EN 302 636-5-1 [4]) using parameter as defined in clause 11.2.
- GeoNetworking protocol (ETSI EN 302 636-4-1 [3]) using parameter as defined in clause 11.2.
- WLAN (IEEE 802.11^{TM}-2016 [i.4]).
- Default Service Set Identifier - SSID: CITSWLAN.
- Default Passphrase: CooperativeItsWlan.

NOTE: The default SSID and Passphrase are used if no special values are defined for an installation.

Messages disseminated via the CPS_003 communication profile use the traffic classes as defined in Table 30.

Table 30: Traffic classes for CPS_003

CSP_MaxPrio	TC ID	AC
255	0	AC_VO
254	1	AC_VI
253	2	AC_BE
252	3	AC_BK
NOTE: For details on TC see ETSI TS 102 636-4-2 [18]. For details on AC see ETSI EN 302 663 [16].		

11.6 CPS_004

This profile defines the communication parameter settings for dissemination of an ADU using GeoNetworking/BTP over LTE-V2X sidelink. The ITS station shall implement the following protocols:

- Basic Transport Protocol (ETSI EN 302 636-5-1 [4]) using parameter as defined in clause 11.2.
- GeoNetworking protocol (ETSI EN 302 636-4-1 [3]) using parameter as defined in clause 11.2.
- LTE; E-UTRA and E-UTRAN (ETSI TS 136 300 [17]).

11.7 CPS_005

This profile defines the communication settings for dissemination of an ADU using BTP/GeoNetworking encapsulated within UDP-IP/TCP-IP based data services (e.g. using cellular communication) interface. It applies tunnelling of GeoNetworking packets through UDP-IP/TCP-IP version 4/version 6. The ITS station shall implement the following protocols:

- Basic Transport Protocol (ETSI EN 302 636-5-1 [4]) using parameter as defined in clause 11.2.
- GeoNetworking protocol (ETSI EN 302 636-4-1 [3]) using parameter as defined in clause 11.2.
- User Datagram Protocol - UDP (IETF RFC 768 [i.8]).
- User Datagram Protocol - TCP (IETF RFC 793 [i.9]).
- IP version 4/version 6 (IETF RFC 791 [i.7]).

Table 31 lists the communication parameter settings.

Table 31: CPS_005 Communication parameter settings

Parameter	IP version 4	IP version 6
Transport protocol type	UDP/TCP	
Source port	Implementation dependent	
Destination port	47 101	
Destination address	IPv4 multicast or unicast address dependent on network deployment	IPv6 link-local multicast address or unicast address

NOTE 1: Port number values were chosen based on the "IANA Service Name and Transport Protocol Port Number Registry" [i.6] (https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt, Last Updated 2016-04-07). According to this document, the port number values 47 101 - 47 556 are unassigned.

NOTE 2: The setting of other communication parameters related to IPv4 or IPv6 are implementation-dependent.

12 Security Profile

The Generic security profile as defined in ETSI TS 103 097 [6] shall be applied to messages used by the TLM, RLT, IVI, TLC, GPC services. Additional HeaderField types are not allowed.

Annex A (normative): ASN.1 specification of IS Messages

The ASN.1 specifications of the data types used in the present document can be found on the ETSI ASN.1 publication site via the URL:

https://forge.etsi.org/rep/ITS/asn1/is_ts103301/blob/v2.1.1/

Table A.1: SHA-256 cryptographic hash digest TLM

Filename	SHA-256 cryptographic hash digest
SPATEM-PDU-Descriptions.asn	b98c34f961f77e3fd3fa25808c8b1b206b2cc210b20462441a3dd088c003c1e4

Table A.2: SHA-256 cryptographic hash digests RLT

Filename	SHA-256 cryptographic hash digest
MAPEM-PDU-Descriptions.asn	8aca1770f24383741c967182c1f4fcf8a9b11196c5abd69aafe6564f40970c93

Table A.3: SHA-256 cryptographic hash digests IVI

Filename	SHA-256 cryptographic hash digest
IVIM-PDU-Descriptions.asn	fcf850bc8863676e105840f490ca273c7862225fa03230518111e0b298e0a0c9

Table A.4: SHA-256 cryptographic hash digests TLC

Filename	SHA-256 cryptographic hash digest
SREM-PDU-Descriptions.asn	652bc65ced1c42c62d5c93d3959557b5457271c0c36419fcd78327d3b0081abf
SSEM-PDU-Descriptions.asn	802c6fe528fc9c64fb879d42da9427bf0a1c685f1a755ee2cdc255ede42f3b35

Table A.5: SHA-256 cryptographic hash digests GPC

Filename	SHA-256 cryptographic hash digest
RTCMEM-PDU-Descriptions.asn	30f7df5e4a021b6022e1894f77e1a828d9a5948b0e75542e1f5b81f8526fca44

History

Document history		
V1.1.1	November 2016	Publication
V1.2.1	August 2018	Publication
V1.3.1	February 2020	Publication
V2.1.1	March 2021	Publication