ETSI TS 103 301 V2.3.1 (2026-04)

TECHNICAL SPECIFICATION

Intelligent Transport Systems (ITS);
Facilities Layer;
Infrastructure Services;
Release 2

Reference
RTS/ITS-001995

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

Modal verbs terminology

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

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

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 related 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 in the ETSI docbox.

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] Void.

[2] ETSI TS 102 894-2: "Intelligent Transport Systems (ITS);Facilities Layer; Part 2: Common data dictionary (CDD); Release 2".

[3] Void.

[4] Void.

[5] Void.

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

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

[8] ETSI TS 103 899: "Intelligent Transport Systems (ITS); Vehicular Communications; Geographical Area Definition; Release 2".

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

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] Void.

[i.2] ISO/TS 17423: "Intelligent transport systems — Application requirements and objectives".

[i.3] ISO/TS 14823-1: "Intelligent transport systems — Graphic data dictionary — Part 1: Specification".

[i.4] Void.

[i.5] Void.

[i.6] Void.

[i.7] Void.

[i.8] Void.

[i.9] Void.

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

[i.11] CEN ISO/TS 19091: "Intelligent transport systems - Cooperative ITS - Using V2I and I2V communications for applications related to signalized intersections".

[i.12] Void.

[i.13] ISO/TS 17427-1: " Intelligent transport systems — Cooperative ITS — Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s)".

[i.14] ETSI TS 103 836-4-1: "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality; Release 2".

[i.15] Void.

[i.16] ETSI TS 103 900: "Intelligent Transport Systems (ITS); Facilities Layer; Cooperative Awareness Service; Release 2".

[i.17] ETSI TS 103 831: "Intelligent Transport Systems (ITS); Facilities Layer; Decentralized Environmental Notification Service; Release 2".

[i.18] ETSI TS 102 965: "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration; Release 2".

[i.19] ETSI TR 103 902: "Intelligent Transport Systems (ITS); ITS Framework; Terms, Symbols and Abbreviations; Release 2".

[i.20] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions — Part 1: Country code".

[i.21] Recommendation ITU-T S.1: "International Telegraph Alphabet No. 2".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 103 902 [i.19] apply.

3.2 Symbols

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

IS_Control	Interface required by the IS to management plane entity(ies)
IS_DataIn	Interface required by the IS to gather IS PDUs and other data
IS_DataOut	Interface required by the IS to pass IS PDUs to other entities
IS_DataProviding	Interface provided by the IS for making collected IS PDUs available
IS_Security	Interface required by the IS to security plane entity(ies)
IS_Triggering	Interface provided by the IS for controlling IS PDU dissemination

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 103 902 [i.19] and the following apply:

GPCH	General Purpose Channel
SFCH	SaFety Channel

4 Infrastructure services introduction

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 (NTL) with a set of communication parameters.

NOTE: In other specifications referred by the present document, the term message, payload, data structure may have different meanings e.g. in CEN ISO/TS 19091 [i.11] and in CEN ISO/TS 19321 [7]. Therefore, the current convention is defined for clarification purposes.

4.2 Services provided by IS

The infrastructure services refer to Facilities layer entities that manage the generation, transmission and reception of infrastructure-related messages from the infrastructure to Vehicle or Personal ITS-S or vice-versa. Figure 1 illustrates a high level functional architecture of the infrastructure services within the ITS communication architecture. The messages are Facilities layer PDUs that are exchanged among ITS-Ss. The payload is generated by ITS applications in the transmitting 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 a Roadside ITS-S and disseminated to a Vehicle 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 Manoeuvre" - 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.

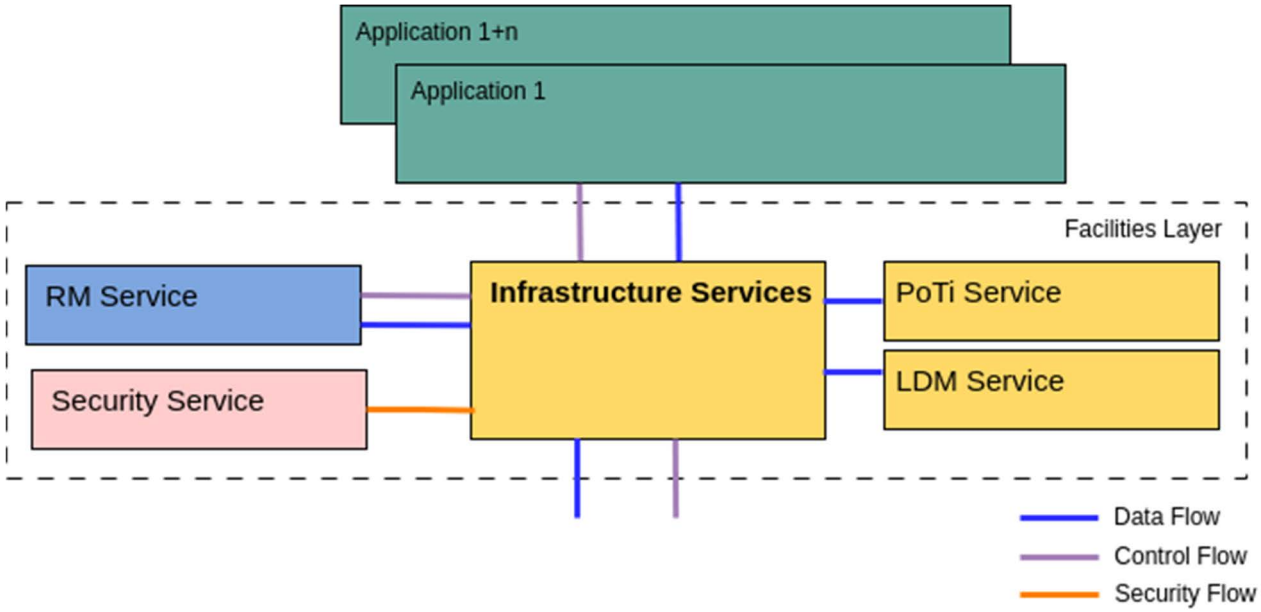

Figure 1: Infrastructure services and logical interfaces

The infrastructure services shall provide at least the following functions.

For the transmission service:

- Message encoding.
- Dissemination management.

For the reception service:

- Message decoding.
- Collection management.

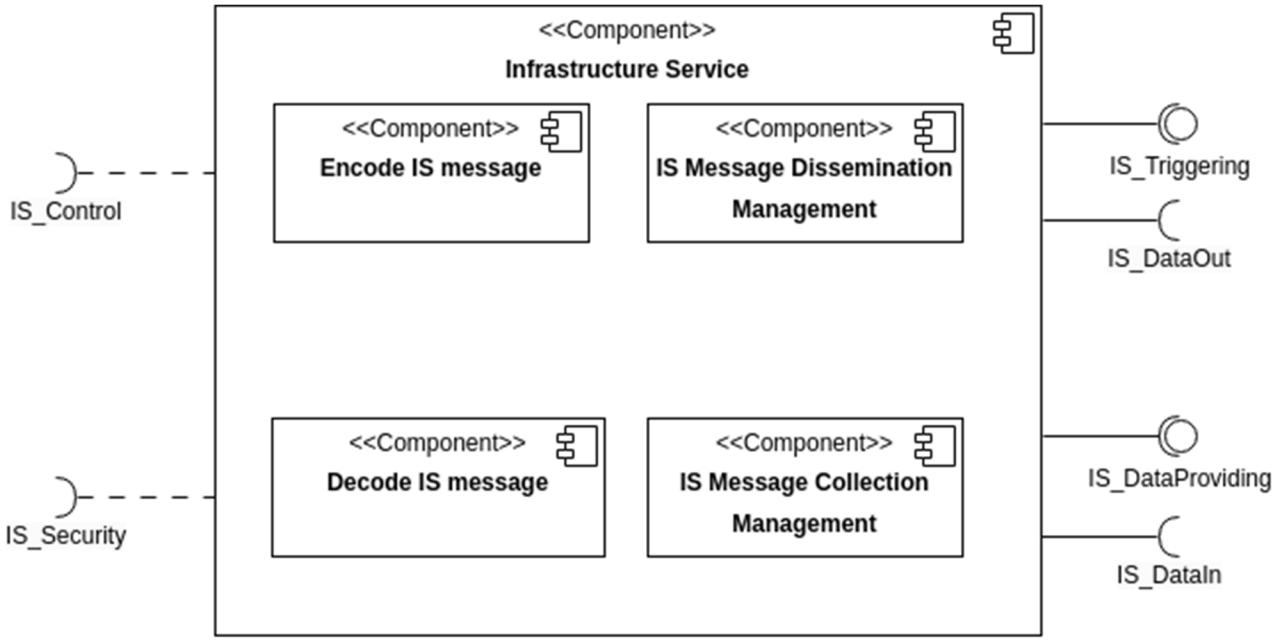

Figure 2: Infrastructure service component diagram

4.3 Infrastructure services in the ITS organizational architecture

Within the role "System Operation" as defined in ISO/TS 17427-1 [i.13], 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.

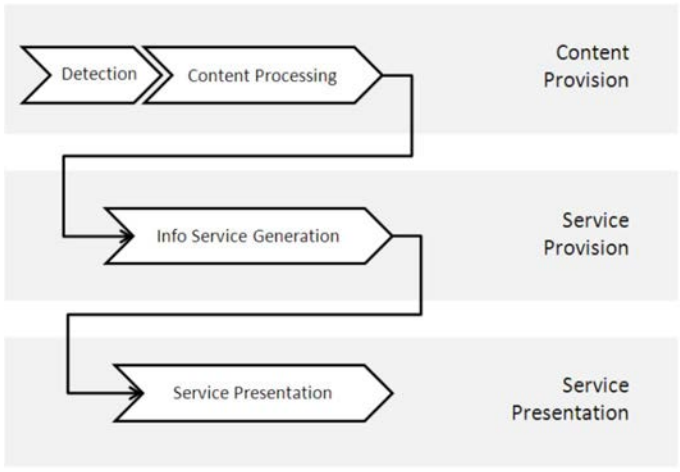

Figure 3: Identification of sub-roles of the role system (lifecycle) operation in the ITS organizational architecture

4.4 Interfaces of the infrastructure services

4.4.1 Interface to the ITS-S applications

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 data contained in an application request.

Table 1: Interfaces to ITS-S applications

Category	Data	Definition
Data passed from application to infrastructure services (IS_Triggering)	Infrastructure message identification	Identification of the message
	Request type	Trigger, update or ending of transmission
	Dissemination parameter	Conditional PCI and SCI data for IS_DataOut (see Table 2) like e.g. GN traffic class as defined in ETSI TS 103 836-4-1[i.14], if GeoNetworking/BTP is used For more details, see the dissemination profile for each service in clauses 5 to 8
	Payload	Information contained in payload
Data returned from infrastructure services to the requesting application (IS_Triggering)	Infrastructure message identification or Another 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
Data provided from infrastructure services to application (IS_DataProviding)	Infrastructure message identification	Identification of the message
	Payload	Information contained in message as payload
	Collection parameter	Conditional PCI and SCI data from IS_DataIn (see Table 2)

4.4.2 Interface to management plan entities

The infrastructure services may exchange information with the entity(ies) in the ITS management plane via the interface IS_Control.

NOTE: The specifications of the interface between the infrastructure services and the management entity is out of scope of the present document.

4.4.3 Interface to security plan entities

In case ETSI ITS security at the facilities layer is used, the infrastructure services exchange information directly with the entity(ies) in the security plane via the interface IS_Security.

NOTE: The specifications of the interface between the infrastructure services and the security entity is out of scope of the present document.

4.4.4 Interfaces IS_DataIn and IS_DataOut

The infrastructure services shall pass the message for dissemination via the IS_DataOut to either another facilities layer entity such as Resource Management or a lower layer functionality such as the NTL.

The infrastructure service shall gather messages via the IS_DataIn from either another facility layer entity such as Resource Management or a lower layer functionality such as the NTL.

Table 2: Messages exchanged over Interfaces IS_DataIn and IS_DataOut

Category	Data	Data requirement	M/O/C (see note)	Remark/Condition
Data provided by the infrastructure services via IS_DataOut	PDU	*{message}* as specified in Annex A,	M	
	SCI	Additional control information related to security such as ITS-AID and SSP which shall be listed in the Authorization Ticket associated to the private key used to sign the message at the NTL.	C	if a security scheme at the NTL (e.g. ETSI Security [6]) requiring SCI is used.
	PCI	Additional control Information depending on the protocol stack applied in the NTL.	C	If a NTL protocol requiring PCI is used.
	RMI	Additional control information related to Resource management.	C	If RM is available.
Data gathered by the infrastructure services via IS_DataIn	Received PDU	*{message}* as specified in Annex A.	M	
	SCI	Additional control information related to security such as ITS-AID and SSP that are listed in the Authorization Ticket attached to the message and the result of the security check at the NTL.	C	if a security scheme at the NTL (e.g. ETSI Security [6]) requiring SCI is used.
	PCI	Additional control Information depending on the protocol stack applied in the NTL.	C	If a NTL protocol requiring PCI is used.
NOTE: M/O/C are as follows: "M" indicates that the Data element shall always be included. "O" indicates that the Data element may or may not be included. "C" indicates that the Data element shall be included only if the condition is satisfied.				

The infrastructure services may request data from the PoTi service using IS_DataIn.

NOTE 1: The specifications of the interface between the infrastructure services and the PoTi service is out of scope of the present document.

The infrastructure services may provide messages to the LDM service using IS_DataOut.

NOTE 2: The specifications of the interface between the infrastructure services and the LDM service is out of scope of the present document.

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 ITS-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 [i.18] 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 Annex A.

4.5.3 Message encoding scheme

Unless specified otherwise, the unaligned PER encoding scheme as specified in Recommendation ITU-T X.691 [9] 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 3.

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 3: 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 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 Manoeuvre (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 manoeuvres 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 manoeuvres 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.

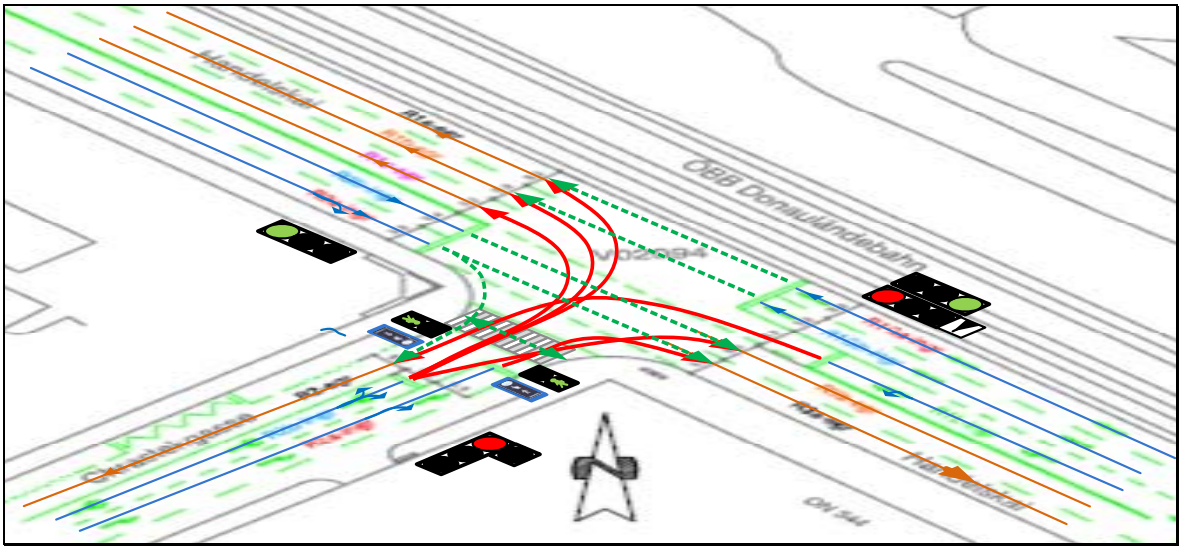

Figure 4: Signalling status of the manoeuvres in an intersection

Figure 4 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 manoeuvre, 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 4 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 in Annex A.

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 Annex A. 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 TLM service shall not execute a SPATEM repetition process.

NOTE: This does not exclude that consecutively triggered SPATEMs can contain exactly the same content in case there is no new information from the traffic light controller.

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 manoeuvres 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 direct and for indirect communication.

5.4.3.2 TLM service communication requirements for direct communication technologies

Table 4 provides the requirements for the direct 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.

Table 4: TLM service communication requirements for direct communication 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
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	
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

The ITS-AID of the TLM service is allocated in ETSI TS 102 965 [i.18].

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 is given in Table 5. 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 5: 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 5.

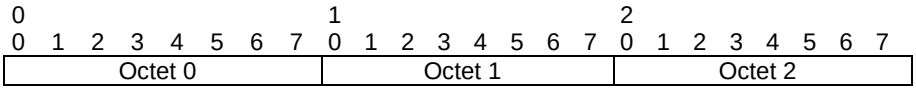

Figure 5: Format for the Octets

The SSP for the TLM service shall correspond to the octet scheme of Table 6.

Table 6: Octet Scheme for TLM service SSPs

Octet #	Description	Value
0	SSP version control	1
1	Service-specific parameter	See Table 7

Table 7: 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)	Manoeuvre assisting information {SPATEM.spat.intersections. IntersectionState.manoeuvreAssistList} and {SPATEM.spat.intersections. IntersectionState.states.MovementState. manoeuvreAssistList}	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 indirect communication

The requirements for the indirect communication (e.g. usage of cellular network) shall be as in Table 8. The structure of the requirements is in accordance with ISO/TS 17423 [i.2].

Table 8: TLM service communication requirements for indirect communication 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
CSP_ExpFlowLifetime	n.a.	

Requirement	Value	Comment
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 manoeuvres 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 neighbour intersection is closer than 400 m, the description may be done up to an extent of approximately the half distance between the intersections.

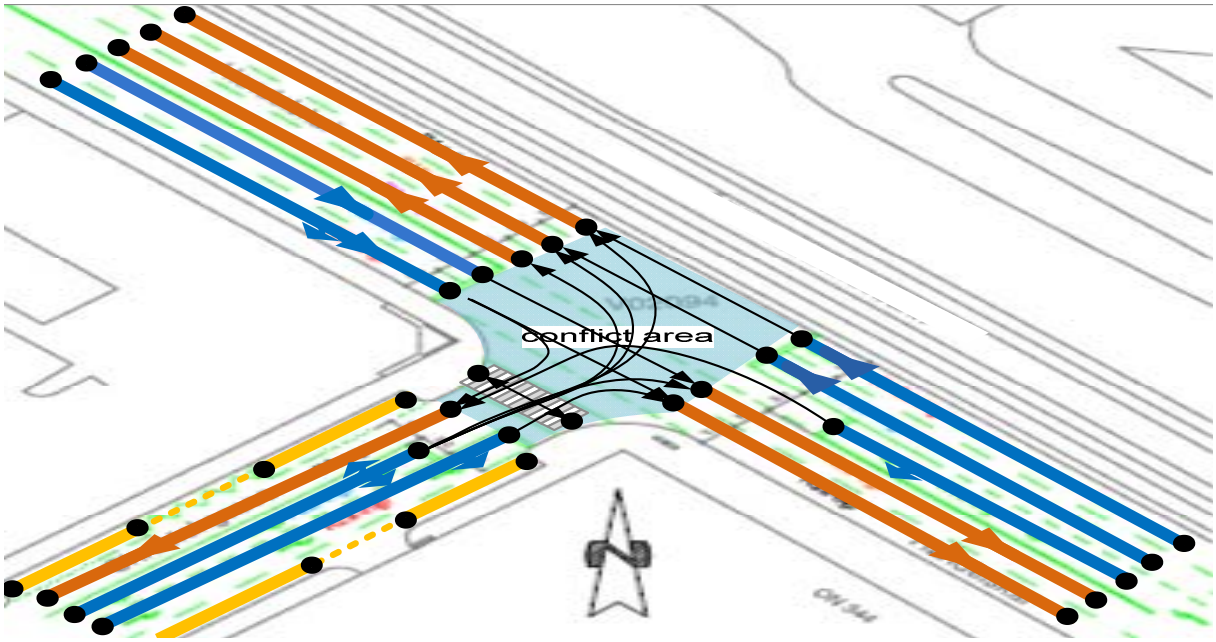

Figure 6: Lane topology and corresponding connection

Figure 6 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 manoeuvres 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 transmission.
- Assembly and disassembly fragmented MAPEM fragments on an Application level as defined by the data element *{MAPEM.map.layerID}* in Annex A.

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 Annex A.

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 Annex A.

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 manoeuvres 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 direct and indirect communication.

6.4.3.2 RLT service communication requirements for direct communication technologies

The requirements for the direct communication shall be as in Table 9. 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.

Table 9: RLT service communication requirements for direct communication 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	253	
CSP_PortNo	2 003	Port Number of the transport protocol
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

The ITS-AID of the RLT service is allocated in ETSI TS 102 965 [i.18].

RLT service security parameters

For security against misuse of keys it is necessary to change the pseudonym identity regularly. The default time is given in Table 10. 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 10: RLT service 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 7.

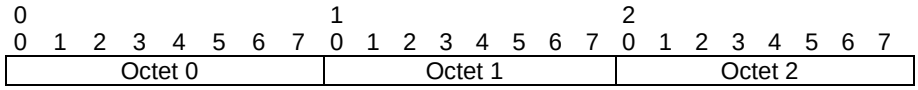

Figure 7: Format for the Octets

The SSP for the RLT service shall correspond to the octet scheme of Table 11.

Table 11: Octet Scheme for RLT service SSPs

Octet #	Description	Value
0	SSP version control	1
1	Service-specific parameter	See Table 12

The Service-specific parameter shall be as defined in Table 12.

Table 12: 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 indirect communication

The requirements for the indirect communication (e.g. usage of cellular network) shall be as in Table 13. The structure of the requirements is in accordance with ISO/TS 17423 [i.2].

Table 13: RLT service communication requirements for indirect communication 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
CSP_ExpFlowLifetime	n.a.	

Requirement	Value	Comment
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.

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 CEN 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 CEN ISO/TS 19321 [7]) value shall be assigned by the IVI service.

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

An *iviIdentificationNumber* is linked to the organization providing the IVI service (e.g. the Service Provider, as defined in CEN ISO/TS 19321 [7]. 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 anymore, 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 direct 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 TS 103 899 [8] to the ITS Networking & Transport Layer.

The requirements for the direct communication shall be as in Table 14. 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.

Table 14: IVI service communication requirements for direct communication technologies

Requirement	Value	Comment
Operational parameters		
CSP_LogicalChannelType	SFCH	
CSP_SessionCont	n.a.	
CSP_AvgADUrate	255, 1 second (default)	
CSP_FlowType	n.a.	
CSP_MaxPrio	254	
CSP_PortNo	2 006	Port Number of the transport protocol
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

The ITS-AID of the IVI service is allocated in ETSI TS 102 965 [i.18].

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 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 15. 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 8.

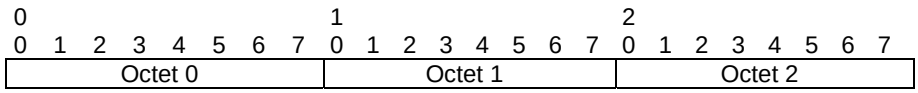

Figure 8: Format for the Octets

Table 15: 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 ITS-S is allowed to send out IVIM and to which the Service-specific parameter apply, using the DF Provider from CEN ISO/TS 19321 [7]. See also clause B.1.
4 to 5	Service-specific parameter	see Table 16. All containers for which no SSP Bit is defined in Table 16 are implicitly allowed to be sent by an ITS-S that has the ITS-AID of the IVI service listed in its Authorization Ticket.
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 behaviour 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 16.

Table 16: 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 14823-1 [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 14823-1 [i.3] road signs with traffic sign pictogram set to dangerWarning 0: The sending ITS-S is not authorized
4	2 (20h)	ISO/TS 14823-1 [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 14823-1 [i.3] road signs with traffic sign pictogram set to regulatory 0: The sending ITS-S is not authorized
4	3 (10h)	ISO/TS 14823-1 [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 14823-1 [i.3] road signs with traffic sign pictogram set to informative 0: The sending ITS-S is not authorized
4	4 (08h)	ISO/TS 14823-1 [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 14823-1 [i.3] road signs with public facilities pictogram 0: The sending ITS-S is not authorized
4	5 (04h)	ISO/TS 14823-1 [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 14823-1 [i.3] road signs with ambient and road conditions set to ambientCondition 0: The sending ITS-S is not authorized

Octet Position	Bit Position	IVIM data Item	Bit Value
4	6 (02h)	ISO/TS 14823-1 [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 14823-1 [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
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 indirect communication

The requirements for the indirect communication (e.g. usage of cellular network) shall be as in Table 17. The structure of the requirements is in accordance with ISO/TS 17423 [i.2].

Table 17: IVI service communication requirements for indirect communication 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
CSP_ExpFlowLifetime	n.a.	
Destination communication service parameters		
CSP_DestinationType	4: Unicast	
CSP_DestinationDomain	Global	
CSP_CommDistance	n.a.	
CSP_Directivity	n.a.	

Requirement	Value	Comment
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.	
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. It also supports managing entry or exit to restricted traffic areas accessible only via an access control barrier. The corresponding SREM is sent by an ITS-S to the traffic infrastructure environment (the ITS-S controlling the intersection or access barrier). In a signalized environment (e.g. intersection) the SREM is sent for requesting traffic light signal priority (public transport) or signal pre-emption (public safety). The service may not only be requested for the approaching signalized environment but also for a sequence of intersections along a defined traffic route. In response to the request the traffic infrastructure environment 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).

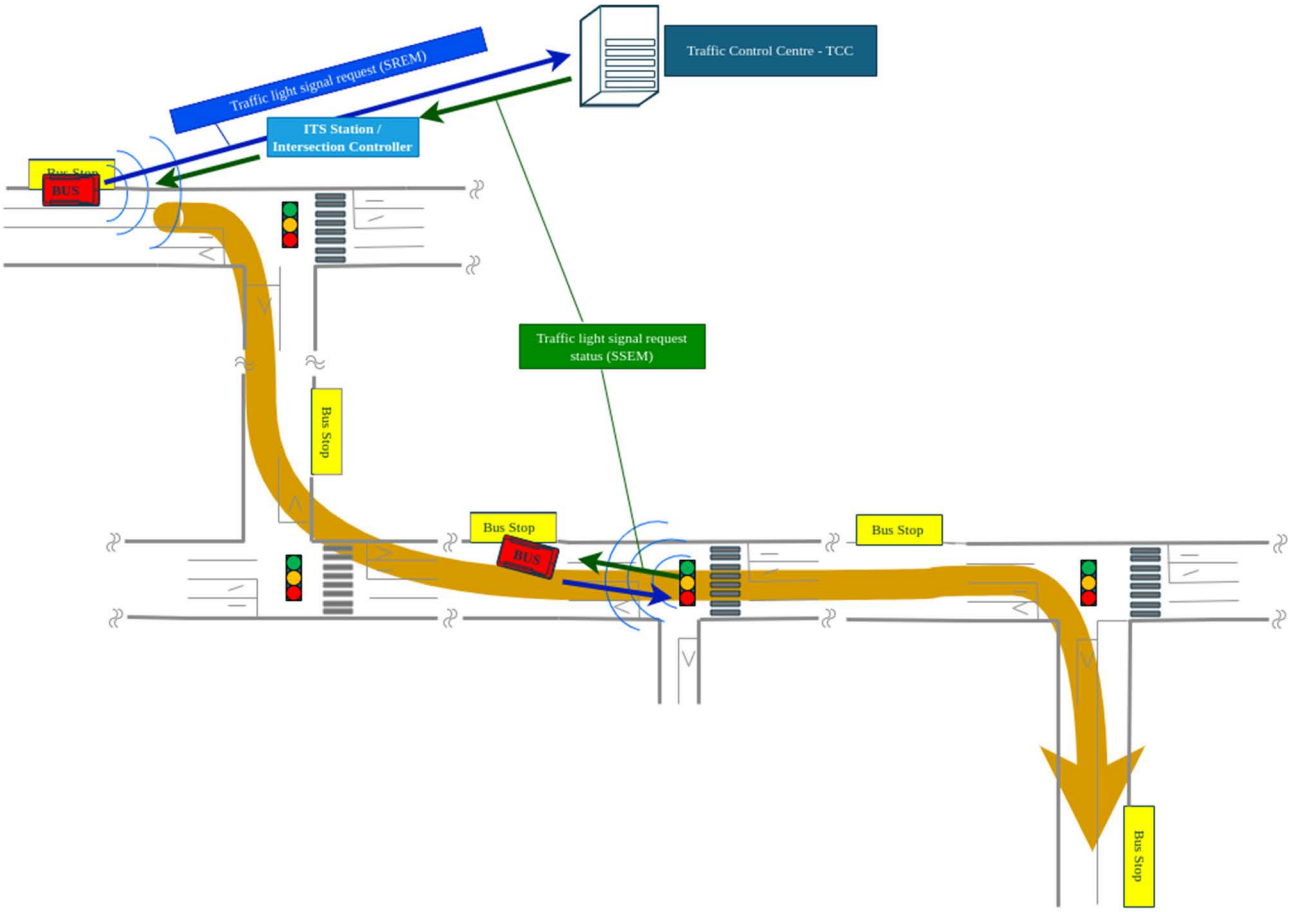

Figure 9: Traffic Light Control service example

Figure 9 gives an example of a bus requesting traffic light signal priority (using SREM) for the defined bus route from the Traffic Control Centre (TCC). The request is forwarded via the ITS-S Station controlling the intersection or by other communication facilities. Multiple requests, related to different intersections, are possible to transmit using one SREM only.

The SSEM reply is generated by the TCC and distributed via the forwarding ITS-S.

Depending on prioritization needs, a single request to the next signalized environment is also possible. Here the ITS-S controlling the intersection analyses the request and returns a SSEM.

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 Annex A.

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

The SSEM is transmitted as response to a previously received SREM to inform the requestor and adjacent traffic participants about the status of the request.

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 requirements

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 direct or indirect communication.

8.4.3.2 TLC service communication parameters for direct communication technologies

The requirements for the direct communication shall be as in Table 18. 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.

Table 18: TLC service communication profile for direct communication 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
	2 008	SSEM port number of the transport protocol
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.	

TLC Application Identifier for SREM and SSEM

The ITS-AIDs are allocated in ETSI TS 102 965 [i.18]:

- 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 is given in Table 19. 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 19: 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 10.

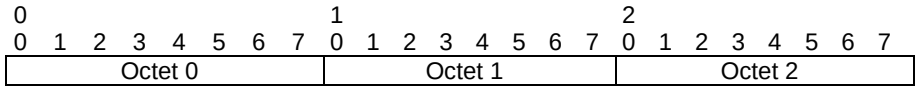

Figure 10: Format for the Octets

The SSP for the SREM shall correspond to the octet scheme of Table 20.

Table 20: Octet scheme for TLC Request service (SREM) SSPs

Octet #	Description	Value
0	SSP version control	3
1-6	Service-specific parameter	See Table 21

The service-specific parameter for SREM shall be as defined in Table 21.

Table 21: 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

Octet Position	Bit Position	SREM data Item	Bit Value
2	1 (40h)	Requestor role (motorcycle) {SREM.srm.requestor.type.role. motorcycle}	0: certificate not allowed to sign 1: certificate allowed to sign
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
3	3 (10h)	Requestor role (tram) {SREM.srm.requestor.type.role. tram}	0: certificate not allowed to sign 1: certificate allowed to sign
3	4 (08h)	OcitRequestorDescriptionContainer {SREM.srm.requestor.ocit}	0: certificate not allowed to sign 1: certificate allowed to sign
4 to 6		Provider identification extension {SREM.srm.requestor.serviceProvider Id}	Identification of the Service Provider for which the ITS-S is allowed to send out SREM and to which the Service-specific parameter apply, using the DF Provider See also clause B.1
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 22.

Table 22: 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 indirect communication

The communication requirements for the indirect communication (e.g. usage of cellular network) in accordance with ISO/TS 17423 [i.2] shall be as in Table 23.

Table 23: TLC service communication profile for indirect communication 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
	2 008	SSEM port number of the transport protocol
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.	

9 GNSS Positioning Correction (GPC) service

9.1 GPC service overview

The GPC service uses positioning correction message for GNSS as defined in ISO/TS 19091 [i.11]. 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 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 manoeuvres (e.g. for safe execution of manoeuvres across a conflict area of an intersection).

9.4.3.2 GPC service communication requirements for direct communication technologies

The requirements for the direct communication shall be as in Table 24. 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.

Table 24: GPC service communication requirements for direct communication 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
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.	

Requirement	Value	Comment
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

The ITS-AID of the GPC service is allocated ETSI TS 102 965 [i.18].

GPC service security parameters

For security against misuse of keys it is necessary to change the pseudonym identity regularly. The default time is given in Table 25. 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 25: 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 11.

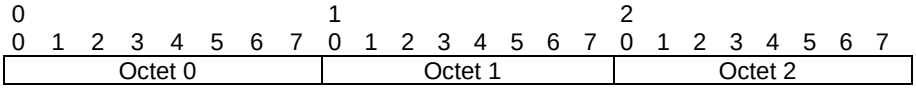

Figure 11: Format for the Octets

The SSP for the GPC service shall correspond to the octet scheme of Table 26.

Table 26: 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 indirect communication

The requirements for the indirect communication (e.g. usage of cellular network) in accordance with ISO/TS 17423 [i.2] shall be as in Table 27.

Table 27: GPC service communication requirements for indirect communication 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
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.	

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 centres (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, etc.) 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 Decentralized Environmental Notification (DEN) service. 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 centre).
- Forwarding of DENM generated by the backbone ITS infrastructure (e.g. TCC) to other ITS stations (e.g. via ITS-G5, LTE-V2X and/or NR-V2X, WLAN, UDP-IP, TCP-IP data services).

- Forwarding of DENM received from other ITS stations to the backbone ITS infrastructure (e.g. TCC).

NOTE: DEN service and DENM are specified in ETSI TS 103 831 [i.17].

10.3 CA service on ITS infrastructure devices

Infrastructure ITS devices shall be able to transmit CAMs and provide the Common Awareness (CA) service. Due to the role of the infrastructure device additional applications may run using the CA basic service:

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

NOTE: CA service and CAM are defined in ETSI TS 103 900 [i.16].

11 Communication Profiles

Void.

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/-/tree/release2_v2.3.1

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

Filename	SHA-256 cryptographic hash digest
SPATEM-PDU-Descriptions.asn	f41b051f9703e16d80fd45cec47b5359fd257a071cca4e18f2795b473ad5a144

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

Filename	SHA-256 cryptographic hash digest
MAPEM-PDU-Descriptions.asn	b5c0d28ae238d905bd2d0b54b74291ea9fbf5d4093ddf27b367ac4a99fe8f040

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

Filename	SHA-256 cryptographic hash digest
IVIM-PDU-Descriptions.asn	a8a4ea41c05554ccc414284c9f0336fa1d2e631aa5bc3516f67fb6b6c6df5d87

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

Filename	SHA-256 cryptographic hash digest
SREM-PDU-Descriptions.asn	8381a329ed5259679bacc1919b8de16976d057828217d04a10a3b6946aa59596
SSEM-PDU-Descriptions.asn	9b71acfcd8d193892da1f9bc9e3e238269366d030ac11fcaf48cfd0b9b230658

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

Filename	SHA-256 cryptographic hash digest
RTCMEM-PDU-Descriptions.asn	0786da745470771b599f9dead7b7141f16aead2e73c1234c6804b652264feac2

Table A.6: SHA-256 cryptographic hash digests ETSI-ITS-DSRC

Filename	SHA-256 cryptographic hash digest
DSRC.asn	c6c1de963ec43302da11aa491d8936d924e70a11f0d4732e23bcefde2e33339d

Table A.7: SHA-256 cryptographic hash digests ETSI-ITS-DSRC-REGION

Filename	SHA-256 cryptographic hash digest
DSRC-Region.asn	55b2592f630a0104a2d03db7faebd387c50a4345471969585faafa621b67c55a

Table A.8: SHA-256 cryptographic hash digests ETSI-ITS-DSRC-AddGrpC

Filename	SHA-256 cryptographic hash digest
DSRC-addGrp-C.asn	a5a97244c826797fc7dab4cf506a04fd1ec6a6369c31a9315b4d6ee5a4146da5

Annex B (informative): SSP coding of ServiceProviderId (DF Provider)

B.1 SSP coding examples of DF Provider

In Table 15 and Table 21 a 3 bytes field for the Identification of a Service Provider is specified. Here are examples how these 3 Bytes are generated.

As reference the relevant parts of the underlying ASN.1 definitions from the ETSI CDD [2], since the 3 bytes represent the UPER encoded value of DF Provider.

```
/**
 * This DF identifies an organization.
 *
 * @field countryCode: represents the country code that identifies the country of the national
registration
 *                     administrator for issuers.
 *
 * @field providerIdentifier: identifies the organization according to the national register for
 *                     issuers.
 *
 */
Provider ::= SEQUENCE {
    countryCode     CountryCode,
    providerIdentifier  IssuerIdentifier
}

/**
 * This DE represents the country code encoded using ITA-2 encoding.
 *
 */
CountryCode ::= BIT STRING(SIZE(10))

/**
 * This DE represent the identifier of an organization according to the applicable registry.
 *
 */
IssuerIdentifier ::= INTEGER(0 .. 16383)
```

First lookup the Country code, which will be a two-letter code according to ISO 3166-1 [i.20].

The codes in ISO 3166-1 [i.20] are available on the Online Browsing Platform https://www.iso.org/obp/ui/#search/code/.

Encoded with ITA2 encoding [i.21] these build the first 10 bits (5 bits per letter).

Together with the 14 bits from the Issue Identifier these build the 3 bytes (24 bits) of the SSP octets.

As quick help here the relevant ITA2 letter codings as example:

A	11000
B	10011
C	01110
D	10010
E	10000
F	10110
G	01011
H	00101
I	01100
J	11010
K	11110
L	01001
M	00111
N	00110
O	00011
P	01101
Q	11101
R	01010
S	10100
T	00001
U	11100
V	01111
W	11001
X	10111
Y	10101
Z	10001

SSP Octet coding examples:

Example	DE CountryCode	DE IssuerIdentifier	SSP Bytes (HEX)
Austria 1 (AT)	1100 0000 01	00 0000 0000 0001	C04001
Norway 2 (NO)	0011 0000 11	00 0000 0000 0010	30C002
Sweden 3 (SE)	1010 0100 00	00 0000 0000 0011	A40003

History

Version	Date	Status
V1.1.1	November 2016	Publication
V1.2.1	August 2018	Publication
V1.3.1	February 2020	Publication
V2.1.1	March 2021	Publication
V2.2.1	August 2024	Publication
V2.2.2	November 2024	Publication
V2.3.1	April 2026	Publication