



Talking Traffic TLEX I2V Deployment Documentation v1.4.0

Table of contents

1	Versioning.....	4
2	Referenced documents	6
3	Introduction.....	7
4	Overview	8
5	Cluster 1 connectivity	9
5.1	Intelligent TLC	9
5.1.1	Initiation	9
5.1.2	Connection	9
5.1.3	Data exchange	9
5.1.4	Security	9
5.2	VLOG TLC.....	10
5.2.1	Initiation	10
5.2.2	Connection	10
5.2.3	Data exchange	10
5.2.4	Security	10
6	Cluster 2 connectivity	11
6.1	Initiation	11
6.2	Connecting	11
6.3	Data exchange	11
6.4	Security	12
7	Data exchange	13
7.1	Messages from “cluster 1” to “cluster 2”	13
7.2	Messages from “cluster 2” to “cluster 1”	13
8	Testing	14

9	Authentication and authorization	15
10	Technical deployment details	16
10.1	Overview	16
10.1.1	TCPStreaming sessions.....	17
10.1.2	VLOG sessions	18
10.1.3	Domains	20
10.1.4	Session logs	20
10.2	Payload types.....	21
10.2.1	TCPStreaming protocol mappings	22
10.2.2	Payload type related standards.....	23
10.3	Time synchronisation.....	24
10.4	Load	25
10.4.1	Rate and size indication	25
10.4.2	Session rate and throughput limits	28
10.4.3	Back pressure policies	29
10.4.4	Load balancing	30
10.5	Payload policies	31

1 Versioning

This document is using a versioning scheme that indicates the version of the deployment and tracks the revisions of this document. This version scheme is <specification version major>.<specification version minor>.<document revision>. The first two version numbers (major and minor) indicate the version of the deployment and only change when there is technical change in the described deployment. Major version is only bumped when there is compatibility breaking change. Minor version is bumped on trivial, non breaking changes of the deployment. The last version number indicates the revision of this document.

Version	Date	Author	Changes
1.0.0	14 Dec 2016	L. Rijneveld	Initial release
1.1.1	13 Mar 2017	L. Rijneveld	Back-pressure thresholds CAM and SPAT increased from 200ms to 1000ms
1.2.0	25 Jul 2017	L. Rijneveld	Update for TLEX release 1.1 Added VLOG TLC connectivity TLEX-TLC-SYSTEM-VLOG Interface introduced
1.2.2	29 Sep 2017	L. Rijneveld	Update for TLEX release 1.2 TLEX-TLC-SYSTEM-VLOG Interface version changed to 1.1.0
1.2.4	14 Mar 2018	L. Rijneveld	Update for TLEX release 1.3 TLEX-TLC-SYSTEM-VLOG Interface version changed to 1.2.0
1.2.5	18 Apr 2018	L. Rijneveld	Update for TLEX release 1.4 TLEX-TLC-SYSTEM-VLOG Interface version changed to 1.3.0
1.2.6	05 Sep 2018	L. Rijneveld	Update for TLEX release 1.6 Added payload type IVI
1.2.7	22 Nov 2018	L. Rijneveld	Update for TLEX release 1.7 TLEX-TLC-SYSTEM-VLOG Interface version changed to 1.4.0
1.2.8	18 Jul 2019	L. Rijneveld	Update for TLEX release 1.8 Added payload policy chapter

Version	Date	Author	Changes
1.2.9	03 Oct 2019	L. Rijnveld	Update for TLEX release 1.9 Added "Monitor" session type TLEX-MONITOR-SYSTEM Interface introduced TLEX-MONITOR-ADMIN Interface introduced
1.3.0	23 Mar 2020	L. Rijnveld	Introduced new version scheme Moved interface specific specifications into interface documentation Improved layout and formatting
1.4.0	24 Apr 2020	L. Rijnveld	Added explicit information about the limitation of the amount of TLCs per session in chapter 10.4.4

2 Referenced documents

ID	Reference	Version	Date
[1]	RFP Talking Traffic 1.1 Beter Benutten	1.1	01 Jul 2016
[2]	EN_30263702v010302 (CAM berichten)	010302	
[3]	EN_30263703v010202 (DENM berichten)	010202	
[4]	J2735_201603 (SPAT en MAP berichten)	201603	
[5]	V-log protocol en definities v3 0 1	3.0.1	01 Nov 2017
[6]	Deliverable F – iTLC Architecture v1.2	1.2	27 Jan 2016
[7]	Intersection Topology Format (ITF) PROFILE	2.1	22 Mar 2018
[8]	MapData (MAP) PROFILE	1.2	29 Jun 2017
[9]	SPAT PROFILE	2.0	16 Nov 2017
[10]	TLEX-TLC-SYSTEM Interface	1.0.1	23 Mar 2020
[11]	TLEX-TLC-SYSTEM-VLOG Interface	1.4.1	23 Mar 2020
[12]	TLEX-BROKER-SYSTEM Interface	1.1.1	23 Mar 2020
[13]	TLEX-TLC-ADMIN Interface	1.2.1	23 Mar 2020
[14]	TLEX-BROKER-ADMIN Interface	1.1.1	23 Mar 2020
[15]	TLEX-MONITOR-SYSTEM Interface	1.0.1	23 Mar 2020
[16]	TLEX-MONITOR-ADMIN Interface	1.0.1	23 Mar 2020

3 Introduction

This document describes the deployment details of the TLEX I2V platform as “iVRI overnamepunt” for Talking Traffic.

4 Overview

This document describes the deployment specific details of the TLEX I2V platform as “iVRI overnamepunt” to facilitate the Intelligent Traffic Light Controller (iTLC) communication between “cluster 1” and “cluster 2” as described in document [1].

The sole purpose of the platform is to route real time data between both “clusters”:

- From “cluster 1” to “cluster 2” this involves passing through TLC originated SPAT, MAP, DENM, IVI and SSM messages.
- From “cluster 2” to “cluster 1” this involves passing through TLC destined CAM and SRM messages.

Additionally the platform is also capable of transmitting MAP and SPAT messages for “legacy” TLCs by converting VLOG 3.0 ASCII streams.

5 Cluster 1 connectivity

5.1 Intelligent TLC

5.1.1 Initiation

Intelligent TLCs will initiate connections with TLEX.

Both the Intelligent TLC and TLEX can end the connection. Both the TLC and TLEX must end the connection if no data is received for a period of 5 seconds.

Intelligent TLCs are responsible for re-establishing the connection with TLEX.

5.1.2 Connection

Intelligent TLCs will connect using the TLEX-TLC-SYSTEM Interface as described in document [10].

5.1.3 Data exchange

As soon as the connection has been established, the Intelligent TLC sends SPAT, MAP, DENM, IVI and SSM messages to TLEX.

- SPAT messages are sent upon change of content, with a maximum rate of 10 SPAT messages per second.
- MAP messages are sent upon connection and upon change of content, with a maximum rate of 1 MAP message per hour. Although partial MAP messages are possible in the ETSI specification; MAP messages sent to TLEX should always be complete.
- DENM messages are sent event driven, with a maximum rate of 1 DENM message per minute.
- IVI messages are sent event driven, with a maximum rate of 1 IVI message per second.
- SSM messages are sent as response to a received SRM message.

CAM and SRM messages received by TLEX from “cluster 2” will be sent to the Intelligent TLC.

- CAM messages will be sent to the Intelligent TLC when the CAM message is received from one of the “cluster 2” systems and was designated by the “cluster 2” system for the specific Intelligent TLC.
- SRM messages will be sent to the Intelligent TLC when the SRM message is received from one of the “cluster 2” systems and was designated by the “cluster 2” system for the specific Intelligent TLC.

5.1.4 Security

The connection between the Intelligent TLC and TLEX is secured using TLS, as this is in accordance with the choices made in the “iTLC Architecture” (see document [6]). TLS client authentication will not be used. There will be no custom PKI infrastructure used.

It is possible to connect without TLS in cases where the connection security can be guaranteed on a lower level.

5.2 VLOG TLC

5.2.1 Initiation

TLEX will initiate the connection with VLOG TLCs. Upon registration of the TLC, it is possible to enable automatic connection establishment.

Both the TLC and TLEX can end the connection. TLEX will end the connection if no data is received for a period of 60 seconds.

TLEX is responsible to re-establishing the connection with the TLC.

5.2.2 Connection

VLOG TLCs will be connected using the TLEX-TLC-SYSTEM-VLOG Interface as described in document [11].

5.2.3 Data exchange

As soon as the connection has been established, TLEX will convert the registered ITF to MAP and sent it on behalf of the TLC. The TLC sends VLOG ASCII messages to TLEX. TLEX will convert the VLOG ASCII messages to SPAT messages and sent these on behalf of the TLC.

- SPAT messages are sent based on WPS (“Werkelijke Programma Status”) and FT (“Fasecyclus Timing”) VLOG messages, with a maximum rate of 10 SPAT messages per second.
- MAP messages are sent upon connection. Although partial MAP messages are possible in the ETSI specification; MAP messages sent to TLEX should always be complete.
- IVI, DENM and/or SSM messages are not sent.

CAM and SRM messages received by TLEX from “cluster 2” will **not** be sent to the TLC.

5.2.4 Security

The connection between the VLOG TLC and TLEX is not secured. With the exception to test scenarios, it is only permitted to connect VLOG based TLCs with TLEX using a VPN secured connection.

6 Cluster 2 connectivity

6.1 Initiation

Cluster 2 systems will initiate connections with TLEX.

Both the Cluster 2 system and TLEX can end the connection. Both the Cluster 2 system and TLEX must end the connection if no data is received for a period of 5 seconds. Cluster 2 systems are responsible for re-establishing the connection with TLEX.

6.2 Connecting

Cluster 2 systems will indicate the TLC scope of connections upon connection. This way it is possible to apply load balancing by utilising a pool of connections.

Cluster 2 systems will be connected using the TLEX-BROKER-SYSTEM Interface as described in document [12].

6.3 Data exchange


As soon as the connection has been established, TLEX will send SPAT, MAP, DENM, IVI and SSM messages to the Cluster 2 system.

- SPAT messages are sent upon reception of the message from one of the connected TLCs.
- MAP messages are sent upon reception of the message from one of the connected TLCs. Additionally, the last received MAP message for each TLC will be sent upon connection.
- DENM messages are sent upon reception of the message from one of the connected TLCs.
- IVI messages are sent upon reception of the message from one of the connected TLCs.
- SSM messages are sent upon reception of the message from one of the connected TLCs.

The messages will be delivered to the Cluster 2 system with a “TLC identifier”. This way the Cluster 2 system can identify from which TLC the message originated.

As soon as the connection has been established, Cluster 2 systems will send CAM and SRM to TLEX. Based on the “TLC identifier” of the message supplied by the Cluster 2 system, TLEX will forward messages to the specific TLCs if they are connected.

- CAM messages will be sent to TLEX with a maximum rate of 1 CAM message per vehicle per second and a maximum rate of 400 CAM messages per TLC per second. The Cluster 2 system is responsible for “selecting” the proper TLCs for reception of the CAM message. This selection is based on “geo fencing”, where a CAM message can only be sent when the vehicle related to the CAM message is within a, to be determined, radius of the TLC intersection(s). The TLC is responsible for CAM de-duplication in case multiple CAM messages are received from the same vehicle.
- SRM messages will be sent to TLEX. The Cluster 2 system is responsible for “selecting” the proper TLCs for reception of the SRM message.

 The maximum rate of 400 CAM messages per TLC per second is based on technical theoretical maximum and could be subject to change after evaluation.

 TLEX will **not** send CAM and SRM messages to VLOG based TLCs.

6.4 Security

The connection between the Cluster 2 systems and TLEX is secured using TLS, as this is in accordance with the choices made in the “iTLC Architecture” (see document [6]). TLS client authentication will not be used. There will be no custom PKI infrastructure used.

It is possible to connect without TLS in cases where the connection security can be guaranteed on a lower level.

7 Data exchange

The data exchange between “cluster 1” and “cluster 2” is based on ETSI, where TLEX as streaming platform should remain data agnostic. The data transfer is based on bi-directional stream of messages. There is no request/response pattern. Messages are streamed to both “sides” as long as there is connectivity.

For details regarding the streaming protocol see TLEX-TLC-SYSTEM Interface document [10] and TLEX-BROKER-SYSTEM Interface document [12].

7.1 Messages from “cluster 1” to “cluster 2”

The SPAT, MAP, SSM and DENM messages streamed from TLEX to “cluster 2” systems are described in ASN.1 notation in their respective ETSI documentation.

For SPAT messages see document [4] par. 5.13.

For MAP messages see document [4] par. 5.6.

For DENM messages see document [3] annex A.

For SSM messages see document [4] par. 5.15.

All messages will be encoded using the ASN.1 UPER encoding.

7.2 Messages from “cluster 2” to “cluster 1”

The CAM and SRM messages streamed from TLEX to “cluster 1” systems are described in ASN.1 notation in their respective ETSI documentation.

For CAM messages see document [2] annex A.

For SRM messages see document [4] par 5.14.

All messages will be encoded using the ASN.1 UPER encoding.

8 Testing

All “cluster 1” and “cluster 2” technology vendors will have access to their private test domain within TLEX in order to support the development of “cluster 1” and “cluster 2” systems.

Within TLEX, data is always streamed within the context of a specific logical domain. Technology vendors will be able to establish both “cluster 1” and “cluster 2” connections within their respective test domain so that they can test their systems.

This way, Cluster 1 technology vendors are able to develop and utilise a Cluster 2 “stub” in order to perform (automated) tests in regards to their Cluster 1 system implementation.

This way, Cluster 2 technology vendors are able to develop and utilise a Cluster 1 “stub” in order to perform (automated) tests in regards to their Cluster 2 system implementation.

Further details regarding the administrative operations using the TLEX API can be found in the TLEX-TLC-ADMIN Interface document [13] and TLEX-BROKER-ADMIN Interface document [14].

9 Authentication and authorization

Organizations and systems are granted access to TLEX using an authorization token. The authorization model allows organizations to manage the tokens for usage in their systems.

This allows technology vendors to generate the required authorization tokens within their test domains to facilitate testing.

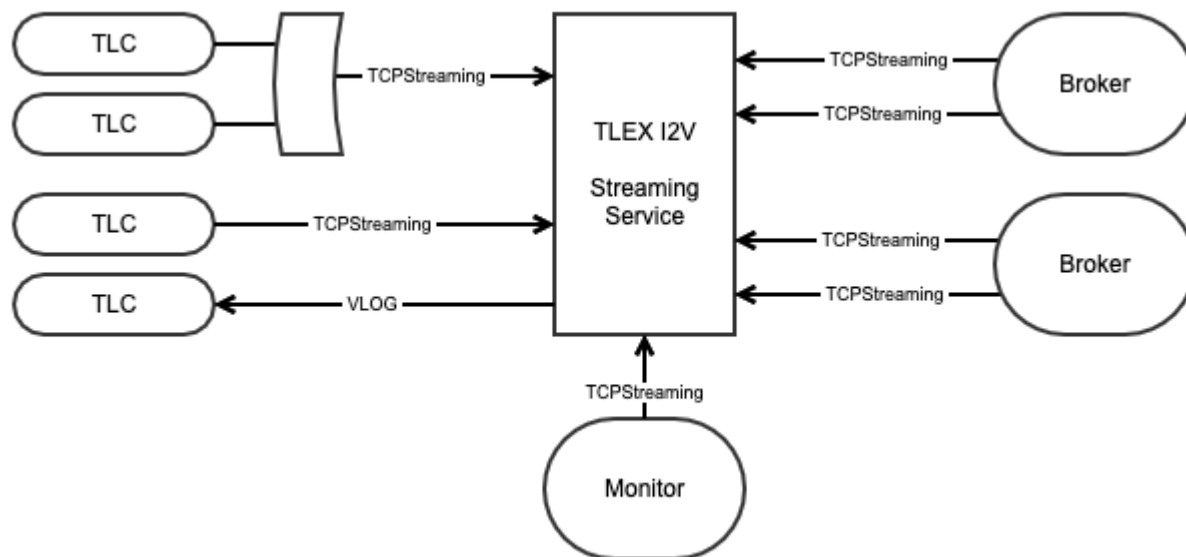
For the production domain this allows the operational governing entities for TLCs (Road Authorities) to register TLCs and manage authorization tokens.

Further details regarding the administrative operations using the TLEX API can be found in the TLEX-TLC-ADMIN Interface document [13] and TLEX-BROKER-ADMIN Interface document [14].

10 Technical deployment details

10.1 Overview

The Streaming Service is designed to route TLC related data between multiple TLC's and multiple TLC data brokers. Data from a TLC is always sent to all connected brokers. Data from a broker is always sent to one specific TLC. The TLCs and the Brokers initiate the connection with the Streaming Service. When, for whatever reason, the session is terminated, the TLCs and/or Brokers have to reinitiate the connection.



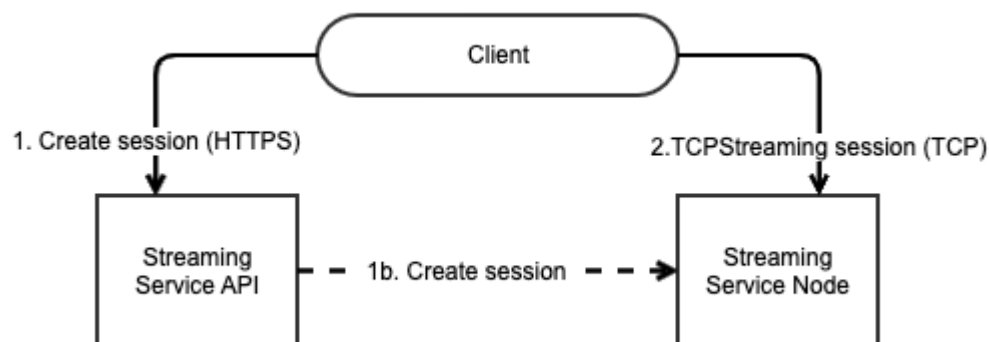
Arrows in diagrams illustrate the direction of connection establishment, not the flow of data.

The Streaming Service is build up from three components:

1. the REST API, primarily for creating streaming sessions;
2. the AutoConnect Session Manager for the management of Streaming Service initiated sessions;
3. the Streaming Service (nodes) for:
 - a. handling continuous streaming of payloads over TCP. One streaming session can stream several types of payload;
 - b. protocol/payload conversion if applicable.

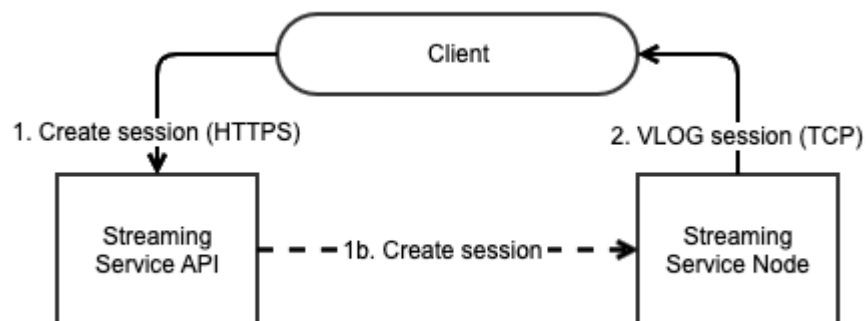
10.1.1 TCPStreaming sessions

In order to establish a connection for a streaming session a Client has to create the session using the Streaming Service API. The Streaming Service API will allocate a free Streaming Service Node for the streaming session and return the created session details, including the connection details, in the request's response.



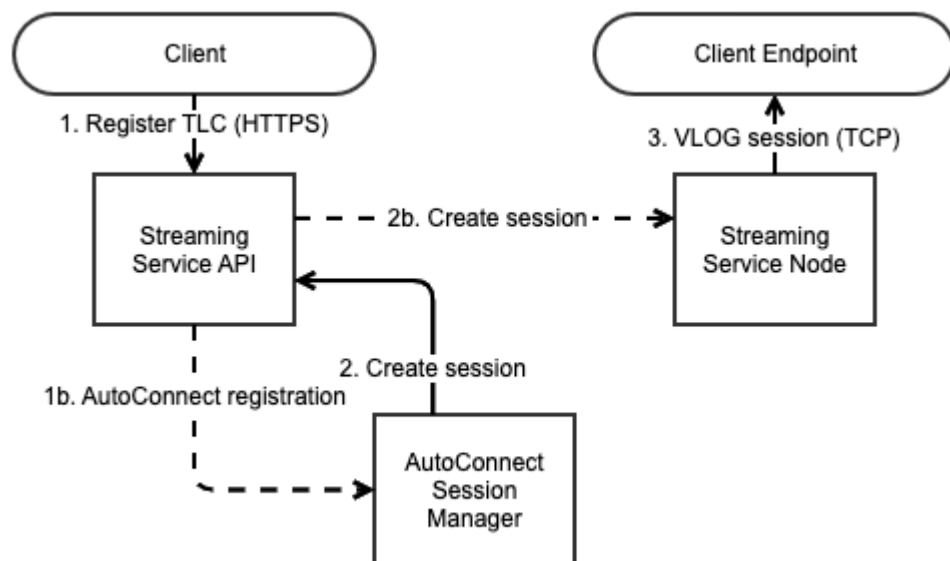
10.1.2 VLOG sessions

For streaming sessions that utilise a protocol, like VLOG, that requires the Streaming Service to initiate the connection, the Client is required to create the session with the specific host and port to which the Streaming Service should connect to.



10.1.2.1 VLOG AutoConnect

In order to facilitate the connection management in use cases where the device that will terminate the connection is not able to create it's session, the Streaming Service's AutoConnect Session Manager can manage the session creation.



10.1.3 Domains

In order to support testing and debugging the streaming sessions can be created for specific domain. The streaming sessions created in different domains are isolated from each other, making it possible for multiple parties to test and debug the streaming functionality simultaneously without the risk of interfering with each other.

10.1.4 Session logs

Besides creating new streaming sessions the Streaming Service API can also be used to request the session details of a previously created session and to request all created sessions.

10.2 Payload types

A streaming session can stream more than one type of payload. Although the Streaming Service itself does not interpret the payload while streaming between sessions, the different types of payload are pre-defined in order to:

1. inform the receiving end-point of the payload type so that the payload data can be interpreted correctly;
2. register streaming metrics per payload type;
3. calculate the "Session stale payloads" metric based on payload type specific TTL definitions;
4. enforce payload type specific back pressure policies.

The described TTL (Time-To-Live) of the payloads is mostly relevant for the parties receiving the payload. The Streaming Service uses this TTL only for determining the session metric "stale payload received".

Payload type	Stream direction	Payload format	TTL	TTL rationale
MAP	TLC -> Brokers	ASN.1 UPER encoded MAP	300 seconds	MAP is a semi-static message, it is important that it is delivered.
SPaT	TLC -> Brokers	ASN.1 UPER encoded SPaT	3 seconds	SPaT carries the current state of the traffic light, therefore it must be delivered on time.
DENM	TLC -> Brokers	ASN.1 UPER encoded DENM	60 seconds	A DENM has a timestamp and validity, it is acceptable if it is delivered later, and ignored if not valid anymore.
SSM	TLC -> Brokers	ASN.1 UPER encoded SSM	10 seconds	An SSM that is delivered too late will not be informative for the user.
IVI	TLC -> Brokers	ASN.1 UPER encoded IVI	60 seconds	An IVI has a timestamp and validity, it is acceptable if it is delivered later, and ignored if not valid anymore.
CAM	Brokers -> TLC	ASN.1 UPER encoded CAM	5 seconds	A bit older positions can still be used, the CAM itself contains a timestamp which rolls over after 64 seconds.
Secure CAM	Brokers -> TLC	ASN.1 UPER encoded CAM (with security envelop)		
SRM	Brokers -> TLC	ASN.1 UPER encoded SRM	10 seconds	An SRM that is delivered too late will not be able to provide priority in time.
Secure SRM	Brokers -> TLC	ASN.1 UPER encoded SRM (with security envelop)		

10.2.1 TCPStreaming protocol mappings

The TLEX-TLC-SYSTEM Interface (see document [10]) and TLEX-BROKER-SYSTEM Interface (see document [12]) use the TCPStreaming protocol. The following table illustrates the payload type identification byte used within the Talking Traffic project.

Payload type byte	Payload type
0x00	MAP
0x01	SPAT
0x02	DENM
0x03	SSM
0x04	IVI
0x10	CAM
0x11	Secure CAM
0x12	SRM
0x13	Secure SRM

10.2.2 Payload type related standards

Subject	Standard	Version	Comment
CAM	EN 302 637-2	v1.3.2	Cooperative Awareness Message
DENM	EN 302 637-3	v1.2.2	Decentralized Environmental Notification
IVI	ISO TS 19321	v1	In-Vehicle Information
CDD	TS 102 894-2	v1.2.1	Common Data Dictionary for all messages
Geonetworking	EN 302 636-4-1	v1.2.1	For 802.11p networks
BTP	TS 103 248	v1.0.1	For 802.11p networks
Security	TS 103 097	v1.2.5	Security envelope and certificate format
MAP, SPaT, SRM, SSM	TS 103 301	V1.1.1	ETSI header including protocol version for TS 19091
MAP, SPaT, SRM, SSM	TS 19091	v0910	Based on SAE J2735

10.3 Time synchronisation


It is important that all connected systems have their times properly synced to a reliable clock source. A big clock difference between the systems would be problematic for determining the age of the payload. The Streaming Service will continuously measure the clock difference during a streaming session by sending a protocol specific time enquiry message every 15 seconds and will terminate sessions if the average clock difference (average over 1 minute period) exceeds the "clock difference threshold". This threshold will be set to 3 seconds. The Streaming Service requires at least 2 time synchronisation responses each minute; if less than 2 responses are received the session will also be disconnected.

10.4 Load


10.4.1 Rate and size indication

The described payload sizes are all based on ASN.1 Unaligned PER encoding.

The "broker" rate limits and throughput calculations are based on a maximum of 1300 connected TLCs.

 Streaming protocol overhead has not been included

10.4.1.1 Theoretical maximums

 The rate metrics used are based on theoretical maximums and will need to be evaluated against the actual rates expected in real life.

Name	Maximum rate	Average payload size	Maximum payload size	Size explanation	Maximum TLC rate	Maximum average TLC throughput	Maximum broker rate	Maximum average broker throughput
MAP	1/hour/TLC	4 KB	20 KB	Average based on 10 signal groups Maximum based on 50 signal groups	1/hour	4 KB/hour	1300/hour	5.08 MB/hour
SPaT	10/second/TLC	1 KB	5 KB	Average based on 10 signal groups Maximum based on 50 signal groups	10/second	10 KB/second	13000/second	12.7 MB/second
DENM	1/minute/TLC	200 B	300 B	Maximum based on 50% increase	1/minute	200 B/minute	1300/minute	253.91 KB/minute
SSM	60/hour/TLC	100 B	150 B	Based on CAM size	60/hour	5.86 KB/hour	78000/hour	7.44 MB/hour
IVI	1/second/TLC	250 B	500 B	Maximum based on increase of 100%	1/second	250 B/second	1300/second	317.38 KB/second
CAM	1/second/vehicle 400/second/TLC	100 B	150 B	Maximum based on 50% increase	400/second	39.06 KB/second	520000/second	49.59 MB/second
SRM	60/hour/TLC	100 B	150 B	Based on CAM size	60/hour	5.86 KB/hour	78000/hour	7.44 MB/hour

10.4.1.2 Expected

Name	Average TLC rate	Average payload size	Average TLC throughput	Average broker rate	Average broker throughput
MAP	1/day/TLC	4 KB	4 KB/day	1300/day	5.08 MB/day
SPaT	1/second/TLC	1 KB	1 KB/second	1300/second	1.27 MB/second
DENM	1/hour/TLC	200 B	200 B/hour	1300/hour	253.91 KB/hour
SSM	1/minute/TLC	100 B	100 B/minute	1300/minute	126,95 KB/minute
IVI	1/hour/TLC	250 B	250 B/hour	1300/second	317.38 KB/hour
CAM	100/second/TLC	100 B	9.77 KB/second	130000/second	12.40 MB/second
SRM	1/minute/TLC	100 B	100 B/minute	1300/minute	126,95 KB/minute

10.4.2 Session rate and throughput limits

In order to safe guard that sessions do not generate more load than anticipated the streaming sessions are rate and throughput limited regarding the that traffic is allowed to be transmitted. If one of the limits is exceeded the session will be terminated. The rate and throughput limits depend on the session mode (TLC or Broker) and TLC count (in case of a multiplex session).

Mode	Description	Limit/TLC	Rationale
TLC	Maximum payloads per second	12 payload/s	Mainly SPaT based, including some overhead for MAP, DENM, SSM, IVI and general headroom
	Maximum throughput per second	60 KB/s	Theoretical maximum is applied
Broker	Maximum payloads per second	120 payload/s	Mainly CAM based including some overhead for CAM, SRM and general headroom
	Maximum throughput per second	12 KB/s	Expected average is applied

When a session is created using the Streaming Service API the rate limits which apply for the created session will also be available in the response.

10.4.3 Back pressure policies

If payloads are not processed quickly enough by the receiving end, queues and buffers start to fill up within the Streaming Service. This phenomenon, commonly called "back pressure", occurs when congestion occurs somewhere in the processing chain. One of the indicators of "back pressure" is an increased (increasing) streaming latency (time between reception and transmission of a payload within the Streaming Service). In case of back pressure, the Streaming Service will lower the load on the receiving streaming session by applying a payload type specific "back pressure latency threshold". When a payload's streaming latency exceeds this threshold, the payload will be dropped. By temporary dropping a specific portion of the load before transmission the receiver has the opportunity to "catch up".

Payload type	Latency threshold
MAP	<none>
SPaT	1000 ms
DENM	<none>
SSM	<none>
IVI	<none>
CAM	1000 ms
Secure CAM	<none>
SRM	<none>
Secure SRM	<none>

10.4.4 Load balancing

It is possible to balance the streaming load over more than one connection. Since it is required to explicitly specify the TLCs while create a new streaming session, parties can setup multiple connections over which the total amount of TLCs is distributed. It is also possible to change the "TLC scope" of an already connected streaming session in cases where TLCs should be added or removed from a connected session. There are a few things to consider regarding the management of session TLC scopes:

- There will be an upper limit for the amount of TLCs per session to force the ability to load balance. The default upper limit is 250 TLCs per session;
- Adding TLCs to an active session could be refused due to lack of resources on the session's Streaming Service Node or the maximum TLCs per session limitation. If the TLC cannot be added to an other session a new session needs to be created, or the current session needs to be reestablished;
- Brokers can poll the API for new TLC registrations and add TLCs at any given time. In case of reestablishing sessions it is best to do this during daily designated maintenance windows (midnight);
- TLCs can never be in scope of more than one broker session of the same account and can never be in scope of more than one TLC session. When redistributing TLCs between connections the TLCs should first be removed from the original session before adding it to the new session. Redistribution of TLCs is best done during daily designated maintenance window since it will always cause a brief intermission of the moved TLC's payload stream.

10.5 Payload policies

It is possible to configure payload policies within the Streaming Service, that regulated whether messages can be received by certain accounts. The following payload types are dropped by default in the Talking Traffic production domain and can only be received if the receiving account has been explicitly whitelisted by the governing body.

Payload type
CAM
Secure CAM
SRM
Secure SRM