ETSI TS 103 976 V1.1.1 (2024-02)

TECHNICAL SPECIFICATION

LEA support services; Interface for Lawful Disclosure of vehicle-related data

Reference

DTS/LI-00239

Keywords

automotive, lawful disclosure, security

ETSI

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

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

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

Important notice

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

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

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

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

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

Notice of disclaimer & limitation of liability

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

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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Lawful Interception (LI).

Modal verbs terminology

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

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

1 Scope

The present document defines an interface between two parties to make lawful requests for data relating to vehicles, and to respond to those requests where appropriate. The usage of the interface does not jeopardize the safety and security of the vehicles involved and takes into account the boundaries of the responsibilities of the parties involved.

2 References

2.1 Normative references

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

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

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

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

[1] ISO 20077-1:2017: "Road Vehicles -- Extended vehicle (ExVe) methodology -- Part 1: General information".

[2] ISO 20077-2:2018: "Road Vehicles -- Extended vehicle (ExVe) methodology -- Part 2: Methodology for designing the extended vehicle".

[3] ISO 20078-1:2021: "Road vehicles -- Extended vehicle (ExVe) web services -- Part 1: Content and definitions".

[4] ISO 20078-2:2021: "Road vehicles -- Extended vehicle (ExVe) web services -- Part 2: Access".

[5] ISO 20078-3:2021: "Road vehicles -- Extended vehicle (ExVe) web services -- Part 3: Security".

[6] ETSI TS 103 120: "Lawful Interception (LI); Interface for warrant information".

[7] ETSI TS 103 280: "Lawful Interception (LI); Dictionary for common parameters".

[8] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[9] IETF RFC 6125: "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)".

2.2 Informative references

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

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

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

[i.1] OWASP Cheat Sheet Series: "Transport Layer Protection Cheat Sheet".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

Law Enforcement Agency (LEA): organization authorized by a lawful authorization based on a national law to request data and to receive the results

Request Processing System (RPS): system within an organization which holds vehicle-related data where there is a lawful reason for it to respond to requests for information

3.2 Symbols

Void.

3.3 Abbreviations

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

EUI	Extended Unique Identifier
GNSS	Global Navigation Satellite System
GPSI	Generic Public Subscription Identifier
HTTPS	Hyper Text Transfer Protocol Secure
ICCID	Integrated Circuit Card IDentification
ID	IDentifier
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
LEA	Law Enforcement Agency
MAC	Media Access Control
MSISDN	Mobile Subscriber Integrated Services Digital Network
NAI	Network Access Identifier
PEI	Permanent Equipment Identifier
RPS	Request Processing System
SUPI	SUbscription Permanent Identifier
VIN	Vehicle Identification Number

4 Basic information

4.1 Contents

The present document includes:

- Reference model (clause 5).
- Definition of message flow and protocol (clause 6).
- Supported questions (clause 7).
- Security requirements (Annex A).

4.2 Basic points

The present document is designed to be used in conjunction with other vehicles industry interfaces. The present document references other existing techniques where appropriate.

The present document does not discuss legal or policy matters and does not imply that any request is lawful in any jurisdiction. It is a prerequisite (to using the interface in the present document) that the request is lawful. The legal obligations (for example, what has to be delivered, what has to be retained) are considered independently of the delivery interface and are out of scope of the present document.

The present document looks at requesting data but does not consider a request to affect the vehicle itself in any way. All the requests in the present document are designed to be answered without affecting the vehicle in any way.

The present document is based on a request to a database or central store of data (the Request Processing System, see clause 5). The interface in the present document is not intended to be used for the Law Enforcement Agency to make a connection directly to a vehicle. It is possible that the Request Processing System might make a connection to a vehicle (without affecting the security or safety of the vehicle, and without alerting the owner, driver or any unauthorized party) as part of responding to the request but such a connection is not mandated or considered by the present document.

Some data may be created or stored in different types of organization (such as a vehicle manufacturer, a dealer or organization related to an aftermarket device or service). It is not necessarily the case that all the requests in the present document are appropriate to be sent to all types of RPS organization.

EXAMPLE: Some organizations might not have any information about the vehicle that changed after the vehicle left the factory.

The present document does not put forward any requirement about whether the data in the RPS is up-to-date to any extent.

5 Reference model

Figure 5.1 shows the reference model for the present document.

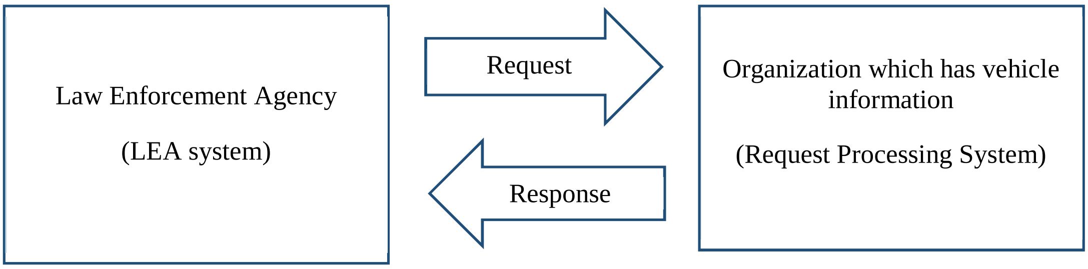
Law Enforcement Agency
(LEA system)
Request
Response
Organization which has vehicle information
(Request Processing System)

Figure 5.1: Reference model

The Law Enforcement Agency (LEA) is responsible for creating a lawful request. The LEA system delivers the request to a Request Processing System (RPS).

This architecture is designed to address use cases that can be met by transactional requests/responses. The present document does not attempt to describe use cases that require an ongoing live stream of data from an RPS (such as voice or video).

The request sent by the LEA needs to be clear. A request is clear if it is explicit to an RPS whether any particular record (held by an RPS) matches or does not match the request.

The RPS is responsible for the collection of the data within its organization and produces the data using its own capabilities and entirely under its control. The RPS identifies the data which matches the request, and only that data. The RPS is entitled to put in place a human review of the request and delivered material. The RPS packages the data, attaches relevant information (including a timestamp and the unambiguous reference to the issued request) and delivers it to the requesting LEA.

The term RPS is used to cover any organization which holds vehicle-related data where there is a lawful reason for it to respond to requests for information. It is not intended to include only manufacturers and may include any relevant commercial or government organization.

6 Definition of message flow and protocol

6.1 Summary

This clause defines a message flow and protocol based on ETSI TS 103 120 [6]. It is used to help meet the requirements given in Annex A.

6.2 Definition of message flow and protocol

6.2.1 Protocol

ETSI TS 103 120 [6] shall be used. JSON encoding (see ETSI TS 103 120 [6], clause 9.2.4) shall be used. XML encoding shall not be used.

The Simple Workflow Profile defined in ETSI TS 103 120 [6], clause H.2 shall be used.

6.2.2 Security

6.2.2.1 Transport confidentiality and integrity

Message exchanges shall be integrity and confidentiality protected by use of HTTPS, following ETSI TS 103 120 [6], clause 9.3.4.

TLS 1.3 (as defined in IETF RFC 8446 [8]) shall be used.

6.2.2.2 Authentication

Implementations shall perform mutual authentication using X.509 ("mTLS") certificates following IETF RFC 6125 [9] and ETSI TS 103 120 [6], clause 9.3.4. Implementations shall ensure that it is configurable which certificates are to be used.

6.2.2.3 Key generation, deployment and storage

The generation, distribution, storage of key material and certificates are out of scope of the present document.

Implementations are encouraged to support best practice e.g. the guidance given in OWASP TLS Cheat Sheet [i.1], section 2.6.

6.2.2.4 Integrity of responses

Implementations shall support signing responses following ETSI TS 103 120 [6], clause 9.2.3.

6.2.3 Destination information

There shall be a mechanism to establish the destination information as per ETSI TS 103 120 [6], clause 8.3.6 (specifically clause 8.3.6.2). This is not specified in the present document.

6.2.4 Errors

Transport errors shall be handled as per ETSI TS 103 120 [6], clauses 6.4.9 and 9.3.3.

6.2.5 Format for request

The technical details of the request shall be given as an LDTaskObject as defined in ETSI TS 103 120 [6], clause 8.3. The details of a request are given in clause 7 of the present document.

The request shall follow ETSI TS 103 120 [6], clause H.2, with the following additional clarifications. The LDTask Object supplied as part of the request shall have the Type field of the RequestDetails set to one of the values specified in the TS103976RequestType dictionary specified in Table 6.2.5-1 below.

Table 6.2.5-1: TS103976RequestType dictionary

Dictionary Owner	Dictionary Name
ETSI	TS103976RequestType.
Defined DictionaryEntries	
Value	**Meaning**
VINtoCommsID	VINtoCommsID request, as defined in clause 7.2.
CommsIDtoVIN	CommsIDtoVIN request, as defined in clause 7.3.
VINtoLocation	VINtoLocation request, as defined in clause 7.4.

The details that are specific to each of the supported questions are given in clause 7.

6.2.6 Format for response

Responses shall be given as a Delivery object as defined in ETSI TS 103 120 [6], clause 10, with JSON-encoded contents as described in Table 6.2.6-1 below. The details of a response are given in clause 7 of the present document.

Table 6.2.6-1: ResultRecords

Field	Format	Description	Mandatory/ Conditional/ Optional
VINtoCommsIDRecord	See clause 7.2.3	Used to provide results to a VINtoCommsID request (see clause 7.2).	Conditional
CommsIDtoVINRecord	See clause 7.3.3	Used to provide results to a CommsIDtoVIN request (see clause 7.3).	Conditional
VINtoLocationRecord	See clause 7.4.3	Used to provide results to a VINtoLocation request (see clause 7.4).	Conditional

7 Details for the supported questions

7.1 Overview

Clause 7 gives a list of questions which are supported by the present document. Clause 7 gives the details that are specific to each of the supported questions.

The present document follows the terminology of the ISO 20077 and ISO 20078 series ([1], [2], [3], [4] and [5]) as follows:

- The term supported question (in the present document) has the same meaning as the term *Use Case* in the ISO 20077 and ISO 20078 series ([1], [2], [3], [4] and [5]).

- The concept of Use Case Scenarios (from the ISO 20077 and 20078 series [1] to [5]) is useful in describing the overall operational outcome that is desired. The present document does not include Use Case Scenarios, though it is noted that ISO 20077-2 [2] provides a process for determining the Use Cases (supported questions) to be used to support a particular Use Case Scenario.

7.2 VINtoCommsID request

7.2.1 Definition

This request provides the communications identifier(s) associated with a given Vehicle Identification Number (VIN).

NOTE 1: This question is only applicable to vehicles with manufacturer-issued VINs.

NOTE 2: It is sometimes easy to change the IMSI(s) present in a particular vehicle. It is important to take this into account.

7.2.2 Definition of request

The LDTask object RequestValues field shall contain a single RequestValue (see ETSI TS 103 120 [6], clause 8.3.5.3) populated as described in Table 7.2.2-1 below.

Table 7.2.2-1: RequestValue for VINtoCommsID request

Field	Format
FormatType	Given as VIN (defined in ETSI TS 103 280 [7]).
Value	VIN of interest, following the format defined in ETSI TS 103 280 [7].

7.2.3 Definition of response

The response shall provide all communications identifiers which the RPS knows are installed in the vehicle with the given VIN.

NOTE: The appropriate regulation determines the meaning of the term *installed* but for clarity, this request is not about a device (e.g. phone) which is routinely (e.g. daily) disconnected from the vehicle and taken with the driver. The appropriate regulation also determines which of the identifiers in Table 7.2.3-2 may be returned (see Annex A).

Successful responses shall set the Manifest Specification field (see ETSI TS 103 120 [6], clause 10.2.2) to "TS103976" and provide the response in JSON format within the JSONData field (see ETSI TS 103 120 [6], clause 10).

The response shall contain zero or more instances of VINtoCommsIDRecord as defined in Table 7.2.3-1 below.

Table 7.2.3-1: VINtoCommsIDRecord

Field	Format	Description	Mandatory/ Conditional/ Optional
CommsID	One of the identifier formats given in Table 7.2.3-2	Communications identifier known to be associated with the VIN.	Mandatory
AssociationTime	AssociationTime (see Table 7.2.3-3)	The latest time at which the RPS knew the communications identifier to be associated with the VIN (e.g. installation time), if known.	Conditional

Table 7.2.3-2: CommsID record

Field	Format	Description
IMEI	ETSI TS 103 280 [7], clause 6.8	IMEI associated with the VIN.
IMSI	ETSI TS 103 280 [7], clause 6.7	IMSI associated with the VIN.
ICCID	ETSI TS 103 280 [7], clause 6.54	ICCID associated with the VIN.
PEIIMEI	ETSI TS 103 280 [7], clause 6.42	PEI associated with the VIN.
SUPIIMSI	ETSI TS 103 280 [7], clause 6.39	SUPI associated with the VIN (in IMSI representation).
SUPINAI	ETSI TS 103 280 [7], clause 6.40	SUPI associated with the VIN (in NAI representation).
MSISDN	ETSI TS 103 280 [7], clause 6.6	MSISDN associated with the VIN (in InternationalE164 format).
GPSIMSISDN	ETSI TS 103 280 [7], clause 6.45	GPSI associated with the VIN (in MSISDN representation).
GPSINAI	ETSI TS 103 280 [7], clause 6.46	GPSI associated with the VIN (in NAI representation).
MACAddress	ETSI TS 103 280 [7], clause 6.25	MAC address associated with the VIN.
EUI64	ETSI TS 103 280 [7], clause 6.50	EUI64 identifier associated with the VIN.

Table 7.2.3-3: AssociationTime

Field	Format	Description
PointInTime	QualifiedDateTime (see ETSI TS 103 280 [7])	Point in time at which an association was known to be valid.
PeriodInTime	AssociationPeriod (see Table 7.2.3-4)	The start and (optionally) end time of a period for which an association was known to be valid.

Table 7.2.3-4: AssociationPeriod

Field	Format	Description	Mandatory/ Conditional / Optional
StartTime	QualifiedDateTime (see ETSI TS 103 280 [7])	Beginning of the period at which the association was known to be valid.	Mandatory
EndTime	QualifiedDateTime (see ETSI TS 103 280 [7])	End of the period at which the association was known to be valid. Shall be omitted if the association is ongoing.	Conditional

7.3 CommsIDtoVIN request

7.3.1 Definition

This request provides the VIN(s) associated with a given communications identifier.

7.3.2 Definition of request

The LDTask object RequestValues field shall contain a single RequestValue (see ETSI TS 103 120 [6], clause 8.3.5.3) populated as described in Table 7.3.2-1 below.

Table 7.3.2-1: RequestValue for CommsIDtoVIN request

Field	Format
FormatType	One item from Table 7.2.3-2.
Value	Communications identifier of interest, following the format defined in Table 7.2.3-2.

7.3.3 Definition of response

Successful responses shall set the Manifest Specification field (see ETSI TS 103 120 [6], clause 10.2.2) to "TS103976" and provide the response in JSON format within the JSONData field (see ETSI TS 103 120 [6], clause 10). The response shall contain zero or more instances of CommsIDtoVINRecord as shown in Table 7.3.3-1.

Table 7.3.3-1: CommsIDtoVINRecord

Field	Format	Description	Mandatory/ Conditional / Optional
VIN	ETSI TS 103 280 [7]	VIN associated with the specified communications identifier.	Mandatory

7.4 VINtoLocation request

7.4.1 Definition

This request gives the location(s) associated with a given VIN at a given time or time range.

7.4.2 Definition of request

The LDTask object RequestValues field shall contain a single RequestValue (see ETSI TS 103 120 [6], clause 8.3.5.3) populated as described in Table 7.4.2-1 below.

Table 7.4.2-1: RequestValue for VINtoLocation request

Field	Format
FormatType	Given as VIN, as defined in ETSI TS 103 280 [7]; see also clause 7.3 of the present document.
Value	VIN of interest, following the format defined in ETSI TS 103 280 [7].

The LDTask object RequestDetails object shall also contain a StartTime and EndTime field indicating the range of times over which location information is sought.

7.4.3 Definition of response

Successful responses shall set the Manifest Specification field (see ETSI TS 103 120 [6], clause 10.2.2) to "TS103976" and provide the response in JSON format within the JSONData field (see ETSI TS 103 120 [6], clause 10). The response shall contain zero or more instances of VINtoLocationRecord that match the query, populated as shown in Table 7.4.3-1.

Table 7.4.3-1: VINtoLocationRecord

Field	Format	Description	Mandatory/ Conditional / Optional
Location	One of the formats given in Table 7.4.3-2	Location associated with the VIN.	Mandatory
TimeOfLocation	AssociationTime (see Table 7.2.3-3)	When the location was known to be associated with the given VIN.	Mandatory
SourceOfLocation	One of the values given in Table 7.4.3-3	Identifies the source of the location information (e.g. GNSS), if available.	Optional
LocationRecordReason	LongString (see ETSI TS 103 280 [7], clause 6.30)	Gives a description of the event (as known to the RPS) that resulted in the location being recorded (e.g. vehicle was parked), if available.	Optional

Table 7.4.3-2: Location formats

Field	Format	Description
WGS84CoordinateDecimal	ETSI TS 103 280 [7], clause 6.33	Latitude and longitude following WGS84 in decimal degrees form.

Table 7.4.3-3: SourceOfLocation

Value	Meaning
GNSS	Location was obtained by a GNSS receiver.

Annex A (normative): Requirements for security, audit and assurance

The fundamental requirement is that the relevant legislation shall be observed at all times. In order to support this, the present document supports the core requirement that RPS and LEA shall ensure the integrity, authenticity and confidentiality of the interface in the present document. This is implemented via the following requirements.

The LEA and RPS shall ensure authenticity and integrity of the request and response messages:

- There shall be mutual authentication for the LEA and the RPS. Typically there are credentials (e.g. a certificate) stored securely on each side, used only for this purpose. Typically, the credentials are securely exchanged prior to the first use of the interface and there is also a mechanism to revoke or refresh credentials as needed. Authentication on the interface is performed organization-to-organization not person-to-person. Typically there is a point-of-contact within each organization who can be contacted if anyone wants to query what happened within the organization.

- When the RPS receives a request, the authentication and formatting shall be checked. The RPS shall reject any requests which do not have the correct formatting or authentication.

- In order to support legislation around audit, the present document supports situations where the RPS is required to store certain details of the request.

NOTE 1: This allows independent audit to correlate records at the RPS with LEA records and authorizations.

NOTE 2: Typically, this involves unique reference numbers but not sensitive details such as names or addresses.

- There is often a requirement to store details for when the requested information is used in court. The relevant national legislation may provide guidance about providing assurance of integrity (including non-repudiation) and continuity for material used in evidence from all parties who are allowed to be involved (i.e. to detect data being modified).

NOTE 3: Techniques such as hashing or signing are a way to provide assurance of integrity without storing sensitive details at the RPS.

There are also the following additional requirements:

- The RPS shall ensure that the system can meet legislation around owner (or user) consent (typically this means that the RPS shall be able to respond to a request without seeking or needing consent from the owner or user).

- The RPS shall ensure that the request is not detectible except to the people who are authorized to know about it (for example, it shall be possible to ensure that an LEA does not know about requests made by a different LEA). Care shall be taken about logging or error messages, to avoid situations where sensitive information is accidentally shared further than necessary.

- Messages shall have confidentiality protection (i.e. encryption). Typically this uses keys stored securely on each side which are used only for this purpose.

Annex B (informative): Change history

Status of Technical Specification ETSI TS 103 976 LEA support services; Interface for Lawful Disclosure of vehicle-related data		
TC LI approval date	**Version**	**Remarks**
February 2024	1.1.1	First publication of the TS after approval at ETSI TC LI#65 (6-8 February 2024, Saariselkä)

History

Document history		
V1.1.1	February 2024	Publication