



Interface for Lawful Disclosure of vehicle-related data

Reference

RTS/LI-00295

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 the
[ETSI Search & Browse Standards](#) application.

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 on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

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

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

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

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

© ETSI 2025.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	7
3.3 Abbreviations	7
4 Basic information	7
4.1 Contents.....	7
4.2 Basic points	8
5 Reference model.....	8
6 Definition of message flow and protocol	9
6.1 Summary	9
6.2 Definition of message flow and protocol	9
6.2.1 Protocol.....	9
6.2.2 Security.....	9
6.2.2.1 Transport confidentiality and integrity.....	9
6.2.2.2 Authentication.....	9
6.2.2.3 Key generation, deployment and storage	9
6.2.2.4 Integrity of responses	10
6.2.3 Destination information	10
6.2.4 Errors	10
6.2.5 Format for request.....	10
6.2.6 Format for response	10
7 Details for the supported questions	11
7.1 Overview	11
7.2 VINtoCommsID request.....	12
7.2.1 Definition.....	12
7.2.2 Definition of request	12
7.2.3 Definition of response.....	12
7.3 CommsIDtoVIN request.....	13
7.3.1 Definition.....	13
7.3.2 Definition of request	13
7.3.3 Definition of response.....	14
7.4 VINtoLocation request	14
7.4.1 Definition.....	14
7.4.2 Definition of request	14
7.4.3 Definition of response.....	14
7.5 VINtoUniquePartNumber	15
7.5.1 Definition.....	15
7.5.2 Definition of request	15
7.5.3 Definition of response.....	16
7.6 UniquePartNumbertoVIN	16
7.6.1 Definition.....	16
7.6.2 Definition of request	16
7.6.2.1 UniquePartNumber	16
7.6.2.2 PartType	17
7.6.3 Definition of response.....	17

7.7	VINtoSubscribedServices	17
7.7.1	Definition	17
7.7.2	Definition of request	17
7.7.3	Definition of response	18
7.8	VINtoConnectedDevices	18
7.8.1	Definition	18
7.8.2	Definition of request	19
7.8.3	Definition of response	19
Annex A (normative):	Requirements for security, audit and assurance.....	20
Annex B (normative):	RequestValue Formats	21
Annex C (informative):	Example message exchange.....	22
C.1	Introduction	22
C.2	Example message flow	22
Annex D (informative):	Approach for supporting access to DSSAD data	23
D.1	Basic approach and scenarios	23
D.2	Scenario 1: Approach for requests to databases	23
D.3	Scenario 2: Approach for recovering data from a vehicle where there is connectivity to the vehicle ...	23
D.4	Scenario 3: Approach for recovery of data direct from vehicles	24
Annex E (informative):	Use of the present document in combination with the ISO 20078 series.....	25
E.1	Context	25
E.2	Owner consent and owner notification	25
E.3	Overview of data structures	25
E.4	Process and use of ISO containers	26
Annex F (informative):	Change history	27
History		28

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.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

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 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] [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 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] 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:

Authorized Organization (AO): any organization legally authorized to make requests and receive results

part number: identifier for a component of the vehicle

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

unique part number: part number from a numbering system that is designed to assign a unique number to each part (at least, unique within a known space e.g. country or manufacturer)

EXAMPLE: If a factory builds two copies of a particular part and assigns them the same part number, then it would not be a unique part number.

3.2 Symbols

Void.

3.3 Abbreviations

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

AO	Authorized Organization
DSSAD	Data Storage System for Automated Driving
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
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
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
TLS	Transport Layer Security
VIN	Vehicle Identification Number
VSS	Vehicle Signal Specification
XML	eXtensible Markup Language

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).

The present document makes extensive use of the messaging protocol defined in ETSI TS 103 120 [6], which contains most of the detailed technical definitions required by implementers.

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.

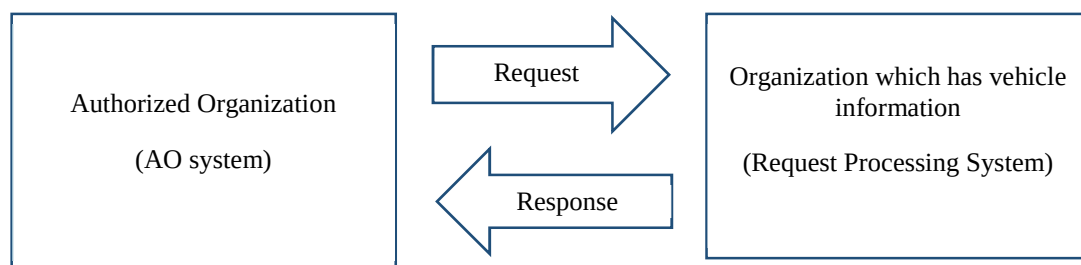


Figure 5-1: Reference model

The Authorized Organization (AO) is responsible for creating a lawful request. The AO 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 AO 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 AO.

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 present document provides a JSON schema for the vehicle-related response structures defined in clause 7, via the Forge (<https://forge.etsi.org/rep/li/schemas-definitions/-/tree/main/103976>). The JSON schema for the messaging protocol used by the present document is given by ETSI TS 103 120 [6], clause 9.2.4.

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

NOTE: Implementers should be aware that most of the protocol details and schema definitions required for the messaging protocol described in the present document are found in ETSI TS 103 120 [6] and ETSI TS 103 280 [7]. The present document sets out how the structures and messages defined in ETSI TS 103 120 [6] are used to ask and respond to the questions described in clause 7.

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 vehicle-specific details of a request are given in clause 7 of the present document, while the description of the usage and structure of the LDTaskObject, including semantics and required fields, is given in ETSI TS 103 120 [6], clause 8.3.

The request shall follow ETSI TS 103 120 [6], clause H.2, with the following additional clarifications. The LDTaskObject 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.
VINtoUniquePartNumber	VINtoUniquePartNumber request, as defined in clause 7.5.
UniquePartNumberttoVIN	UniquePartNumberttoVIN request, as defined in clause 7.6.
VINtoSubscribedServices	VINtoSubscribedServices request, as defined in clause 7.7.

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

To request confirmation of record existence the IsDataAvailable Task flag shall be set.

The AO shall set the flag TS103976ISOFormat in the request to indicate that it accepts that the RPS may use ISO containers to respond to the request (further details given in Annex D). An RPS may choose to work only using ISO containers; in that case, the RPS shall respond with an error if it receives a request where the TS103976ISOFormat flag is not set or is not present. If the TS103976ISOFormat flag is set, the RPS may choose to respond with an ISO-format response (see clause 6.2.6).

Table 6.2.5-2: TS103976HandoverFormat Dictionary

Dictionary Owner	Dictionary Name
ETSI	TS103976HandoverFormat.
Defined DictionaryEntries	
Value	Meaning
TS103976ISOFormat	The AO accepts that the RPS may use ISO containers to respond to the request.

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.

Table 6.2.6-1: ResultRecords

Field	Format	Description	M/ C/ O
VINtoCommsIDRecord	See clause 7.2.3	Used to provide results to a VINtoCommsID request (see clause 7.2).	C
CommsIDtoVINRecord	See clause 7.3.3	Used to provide results to a CommsIDtoVIN request (see clause 7.3).	C
VINtoLocationRecord	See clause 7.4.3	Used to provide results to a VINtoLocation request (see clause 7.4).	C
VINtoUniquePartNumberRecords	See clause 7.5.3	Used to provide results to a VINtoUniquePartNumber request (see clause 7.5).	C
UniquePartNumberttoVINRecords	See clause 7.6.3	Used to provide results to a UniquePartNumberttoVIN request (see clause 7.6).	C
VINtoSubscribedServicesRecords	See clause 7.7.3	Used to provide results to a VINtoSubscribedServices request (see clause 7.7).	C
ISOFormatResults	JSON compliant with ISO 20078-2 [4] and see details below.	May be used (as an alternative to the above structures) to provide results to a request only when the TS103976ISOFormat flag was set.	C

The details of a response are given in clause 7 of the present document. The JSON schema for the structure described in table 6.2.6-1 is provided as part of the present document (see clause 6.2.1). The JSON schema for the Delivery object and associated messages is provided by ETSI TS 103 120 [6], clause 9.2.4, while the details and usage of the relevant messages and structures are given in ETSI TS 103 120 [6], clauses 5, 6 and 10.

If the request was for confirmation of record existence (e.g. the IsDataAvailable Task flag was set in the LDTaskObject of the request), the response shall be given as a Delivery object as defined in ETSI TS 103 120 [6], clause 10, with a DataExistence Delivery format.

In cases where no records match the query criteria, the ResultRecords field shall be an empty JSON array with no other elements in the payload.

The entry ISOFormatResults may be used only when the TS103976ISOFormat flag was set in the request. The results are given in a format that is compliant with ISO 20078-2 [4] (see also Annex D). The RPS shall ensure that the AO can interpret the data delivered; a publicly-available standard (such as the Vehicle Signal Specification (VSS)) may be used to meet this requirement.

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 ISO 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 LDTaskObject 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], clause 6.57).
Value	VIN of interest, following the format defined in ETSI TS 103 280 [7], clause 6.57.

The LDTaskObject RequestDetails may also contain the StartTime and EndTime fields (see ETSI TS 103 120 [6], clause 8.3.5.1), indicating the range of times over which CommsID information is requested.

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. If StartTime and EndTime were not included in the request, the response indicates current associations. If StartTime and EndTime are both included in the request, the RPS shall provide the communications identifiers which the RPS knows were associated with the vehicle with the given VIN at some point or time interval during the period from the time contained in StartTime until the time contained in EndTime.

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	M/ C/ O
CommsID	One of the identifier formats given in table 7.2.3-2	Communications identifier known to be associated with the VIN.	M
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.	C

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).
GPSIMSIDN	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] clause 6.4)	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.

When the association time is reported, either the point in time field is used, or the period in time field is used, but not both.

Table 7.2.3-4: AssociationPeriod

Field	Format	Description	M/ C/O
StartTime	QualifiedDateTime (see ETSI TS 103 280 [7], clause 6.4)	Beginning of the period at which the association was known to be valid.	M
EndTime	QualifiedDateTime (see ETSI TS 103 280 [7], clause 6.4)	End of the period at which the association was known to be valid. Shall be omitted if the association is ongoing.	C

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 LDTaskObject 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.

The LDTaskObject RequestDetails may also contain the StartTime and EndTime fields (see ETSI TS 103 120 [6], clause 8.3.5.1), indicating the range of times over which VIN information is requested.

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	M/ C/O
VIN	ETSI TS 103 280 [7], clause 6.57	VIN associated with the specified communications identifier.	M
AssociationTime	AssociationTime (see table 7.2.3-3)	The latest time at which the RPS knew the VIN to be associated with the communications identifier (e.g. installation time), if known.	C

If StartTime and EndTime were not included in the request, the response indicates current associations. If StartTime and EndTime are both included in the request, the RPS shall provide the VINs which the RPS knows were associated with the CommsID at some point or time interval during the period from the time contained in StartTime until the time contained in EndTime.

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 LDTaskObject 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], clause 6.57; see also clause 7.3 of the present document.
Value	VIN of interest, following the format defined in ETSI TS 103 280 [7], clause 6.57.

The LDTaskObject RequestDetails object shall also contain the StartTime and EndTime fields (see ETSI TS 103 120 [6], clause 8.3.5.1), 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	M/ C/O
Location	One of the formats given in table 7.4.3-2	Location associated with the VIN.	M
TimeOfLocation	AssociationTime (see table 7.2.3-3)	When the location was known to be associated with the given VIN.	M
SourceOfLocation	One of the values given in table 7.4.3-3	Identifies the source of the location information (e.g. GNSS), if available.	O
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.	O

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.

7.5 VINtoUniquePartNumber

7.5.1 Definition

The request provides the Unique Part Numbers (see clause 3.1) associated with a given VIN, matching the specified Part Type if provided.

7.5.2 Definition of request

The LDTaskObject RequestValues field shall contain a RequestValue (see ETSI TS 103 120 [6], clause 8.3.5.3) populated as described in table 7.5.2-1 below.

Table 7.5.2-1: VIN RequestValue

Field	Format	Description	M/C/O
FormatType	FormatType (ETSI TS 103 120 [6], clause 8.3.5.4)	Set to indicate the VIN FormatType as defined in Annex B.	M
Value	LongString (ETSI TS 103 280 [7], clause 6.30)	The VIN of interest, following the VIN format given in ETSI TS 103 280 [7], clause 6.57.	M

Optionally, the LDTaskObject RequestValues field may also contain a RequestValue populated as described in table 7.5.2-2 below.

Table 7.5.2-2: Optional PartType RequestValue

Field	Format	Description	M/C/O
FormatType	FormatType (ETSI TS 103 120 [6], clause 8.3.5.4)	Set to indicate the PartType FormatType as defined in Annex B.	M
Value	LongString (ETSI TS 103 280 [7], clause 6.30)	Shall be given as one of the values in the PartType dictionary (see table 7.5.2-3), except that the value "Other" shall not be used.	M

Table 7.5.2-3: TS103976PartType Dictionary

Dictionary Owner	Dictionary Name
ETSI	TS103976PartType.
Defined DictionaryEntries	
Value	Meaning
Gearbox	Part that the RPS considers to be a gearbox.
Engine	Part that the RPS considers to be an engine.
Airbag	Part that the RPS considers to be an airbag.
Multimedia	Components of the vehicle used for providing information or entertainment capabilities, including an automotive head unit.
Other	Component not meeting any of the other entries of this list. This value shall not be used as part of a request.

7.5.3 Definition of response

The Response shall provide a list of VINtoUniquePartNumberRecords, one for each unique part number associated with that VIN. If the PartType was specified as part of the request, only records matching that PartType shall be returned.

If the value "Other" is used, then the field PartTypeFreeText shall be populated.

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 VINtoUniquePartNumberRecord as defined in table 7.5.3-1 below.

Table 7.5.3-1: VINtoUniquePartNumberRecord

Field	Format	Description	M/I/O
UniquePartNumber	ShortString (ETSI TS 103 280 [7], clause 6.29)	Part number of the component.	M
PartType	Shall be given as one of the values in the PartType dictionary (table 7.5.2-3)	Gives the Part Type of the part.	M
PartTypeFreeText	ShortString (ETSI TS 103 280 [7], clause 6.29)	Contains a free text description of the part. Shall be provided if the PartType is "Other".	C

7.6 UniquePartNumbertoVIN

7.6.1 Definition

The request is for the VIN(s) which is/are associated with a specified unique part number (and which match the PartType where it is present in the request).

7.6.2 Definition of request

7.6.2.1 UniquePartNumber

The LDTaskObject RequestValues field shall contain a RequestValue (see ETSI TS 103 120 [6], clause 8.3.5.3) populated as described in table 7.6.2-1 below.

Table 7.6.2-1: UniquePartNumber RequestValue

Field	Format	Description	M/I/O
FormatType	FormatType (ETSI TS 103 120 [6], clause 8.3.5.4)	Set to indicate the UniquePartNumber FormatType as defined in Annex B.	M
Value	LongString (ETSI TS 103 280 [7], clause 6.30)	Unique Part Number to be matched.	M

Results shall be returned only where the VIN is associated with a Unique Part Number that is a direct string match for the specified Unique Part Number. Characters shall not be interpreted as wildcards.

7.6.2.2 PartType

Optionally, the LDTaskObject RequestValues field may also contain a PartType RequestValue populated as described in table 7.5.2-2.

If the PartType is present, results shall only be returned where the relevant Part also matches the specified PartType.

7.6.3 Definition of response

The Response shall provide a list of UniquePartNumberttoVINRecords

NOTE: If all systems are functioning correctly, there would only be one VIN associated with a unique part number. However, the request may be used in situations where parts are being cloned or part numbers are not being handled correctly, so it is not considered a protocol error if there is more than one VIN associated with a specific unique part number.

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 PartNumberttoVINRecord as defined in table 7.6.3-1 below.

Table 7.6.3-1: UniquePartNumberttoVINRecord

Field	Format	Description	M/I/O
VIN	VIN (ETSI TS 103 280 [7], clause 6.57)	VIN of a vehicle containing a part which matches the request.	M

7.7 VINtoSubscribedServices

7.7.1 Definition

This request is relating to the subscribed services associated with the VIN. The request is asking about payments made to the RPS for services within a specified time range.

If a service was bought as part of the original purchase of the vehicle, then the purchase of the vehicle counts as a the RPS receiving a payment for the service i.e. if the original purchase date is within the specified time range, then the purchase of the vehicle shall be treated as a payment for the service and shall be included in the response.

7.7.2 Definition of request

The LDTaskObject RequestValues field shall contain a single RequestValue (see ETSI TS 103 120 [6], clause 8.3.5.3) populated as described in table 7.7.2-1 below.

Table 7.7.2-1: RequestValue for VINtoSubscribedServices request

Field	Format	Description	M/I/O
FormatType	FormatType (ETSI TS 103 120 [6], clause 8.3.5.4)	Set to indicate the VIN FormatType as defined in Annex B.	M
Value	LongString (ETSI TS 103 280 [7], clause 6.30)	The VIN of interest, following the VIN format given in ETSI TS 103 280 [7], clause 6.57.	M

The LDTaskObject RequestValues shall contain StartTime and EndTime.

7.7.3 Definition of response

List of payments for paid-for services, where the RPS is receiving the payment for the service, which are associated with that VIN and where the payment was made during the specified time range.

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 VINtoSubscribedServicesRecord as defined in table 7.7.3-1 below.

Table 7.7.3-1: VINtoSubscribedServicesRecord

Field	Format	Description	M/I/O
NameOfService	LongString (see ETSI TS 103 280 [7], clause 6.30)	The RPS own description of the service.	M
PaymentDate	QualifiedDateTime (see ETSI TS 103 280 [7], clause 6.4)	The date of the payment for this service. Shall be present if known.	C
UserID	ShortString (see ETSI TS 103 280 [7], clause 6.29)	Free text field for an identifier that the RPS uses to identify the user. Shall be present if known.	C
SubscriptionID	ShortString (see ETSI TS 103 280 [7], clause 6.29)	Free text field for an identifier for this specific subscription (noting that one user may have multiple subscribed services). Shall be present if known.	C
CustomerName	ShortString (see ETSI TS 103 280 [7], clause 6.29)	Free text field for name as understood by RPS. Shall be present if known.	C
CustomerAddress	LongString (see ETSI TS 103 280 [7], clause 6.30)	Free text field for address as understood by RPS. Shall be present if known.	C
TypeOfPaymentMethod	TypeOfPayment (dictionary entry see table 7.7.3-2)	The payment type used most recently for this subscription. This field shall not contain any bank account numbers or credit card numbers. Shall be present if known.	C
TransactionIdentifier	ShortString (ETSI TS 103 280 [7], clause 6.29)	An identifier as known by the RPS for the specific transaction. This is not a credit card or bank account number: it is an identifier which is intended to be different for each different transaction. Shall be present if known.	C

Table 7.7.3-2: TypeOfPayment Dictionary

Dictionary Owner	Dictionary Name
ETSI	TS103976PartType.
Defined DictionaryEntries	
Value	Meaning
CreditCard	Payment made using credit card.
Other	Item not covered by other entries in this dictionary.

7.8 VINtoConnectedDevices

7.8.1 Definition

This request provides a list of devices that have connected to the vehicle within the given time range.

7.8.2 Definition of request

The LDTaskObject RequestValues field (see ETSI TS 103 120 [6] clause 8.3.5.3) shall contain a VIN RequestValue populated as described in table 7.8.2-1 below.

Table 7.8.2-1: VIN RequestValue for VINtoConnectedDevices request

Field	Format
FormatType	Given as VIN, as defined in ETSI TS 103 280 [7] clause 6.57; see also clause 7.3 of the present document.
Value	VIN of interest, following the format defined in ETSI TS 103 280 [7] clause 6.57.

The LDTaskObject RequestDetails (see ETSI TS 103 120 [6] clause 8.3.5.1) shall contain the StartTime and EndTime fields, specifying the range of times over which information is sought.

7.8.3 Definition of response

The response shall provide a list of any connections made to the vehicle that overlaps with the given time range and shall be provided using the VINtoConnectedDeviceRecord described in table 7.8.3-1. One record shall be made for each connection (i.e. if a device connected multiple times, then multiple records shall be included).

The time of the connection is given in the structure AssociationTime (defined in clause 7.2.3).

If the nature of the connection matches one of the ConnectionTypes in table 7.8.3-2 then the ConnectionType shall be provided.

Table 7.8.3-1: VINtoConnectedDevicesRecord

Field	Format	Description	M/C/O
ConnectionType	Given as one of the values in the TS103976ConnectionType Dictionary (table 7.8.3-2) or an RPS-provided Dictionary	Type of connection made by the device (present if the connection is for one of the purposes on the list in table 7.8.3-2).	C
DeviceIdentifiers	List of CommsID	Any known identifiers for the device as defined in table 7.2.3-2 if available.	C
ConnectionTime	AssociationTime (table 7.2.3-3)	Time of the connection using the AssociationTime structure described in clause 7.2.3.	M

Table 7.8.3-2: TS103976ConnectionType Dictionary

Dictionary Owner	Dictionary Name
ETSI	TS103976ConnectionType
Defined DictionaryEntries	
Value	Meaning
Infotainment	A device which is connected to the vehicle either via a cable (e.g. via USB) or wirelessly (e.g. via Bluetooth®) in order to allow features from the device (e.g. navigation, calls, music) to be displayed on the vehicle or accessed through the vehicle. Typically used when the device is in the vehicle.
RemoteAccess	A device which is connected to the vehicle (typically wirelessly) in order to access data from the vehicle or to remotely engage functions on the vehicle. Typically used when the device is not in the vehicle.
KeyPairing	Device is authorized to be used for gaining entry to the vehicle or to facilitate starting the vehicle, or both. This connection type is used to indicate that the device has the capability to assist with entry to the vehicle or starting the vehicle.
KeyUse	The use of a device to gain entry to the vehicle or to start the vehicle.
WLAN	Device that is using the car as a Wireless Local Area Network hot spot.

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 AO shall ensure the integrity, authenticity and confidentiality of the interface in the present document. This is implemented via the following requirements.

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

- There shall be mutual authentication for the AO 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 AO 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 detectable except to the people who are authorized to know about it (for example, it shall be possible to ensure that an AO does not know about requests made by a different AO). 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 (normative): RequestValue Formats

Annex B provides additional RequestValue Formats used by the present document in addition to those defined in ETSI TS 103 120 [6], Annex C. The FormatOwner of these RequestValues is "ETSI".

Table B-1: RequestValue Format Definitions

Format Name	Description	Format
VIN	Vehicle Identification Number.	Regular expression as per ETSI TS 103 280 [7], clause 6.57.
UniquePartNumber	Unique Part Number for a vehicle part.	ShortString (ETSI TS 103 280 [7], clause 6.29).
PartType	Part Type of a vehicle part.	Any of the values in the TS103976PartType dictionary except "Other".

Annex C (informative): Example message exchange

C.1 Introduction

Annex C provides an illustrative example of how a request for vehicle-related data is made according to the present document, as well as how the results are made available. It includes a description of how the present document makes use of the message and protocol elements defined in ETSI TS 103 120 [6].

The ETSI Forge contains a set of example files that are relevant to Annex C.

C.2 Example message flow

The message flow set out in clause 6.2 leverages ETSI TS 103 120 [6] as a messaging protocol. In this protocol, the initial request and the delivery of results occur in separate transactions. This is shown in figure C.2-1.

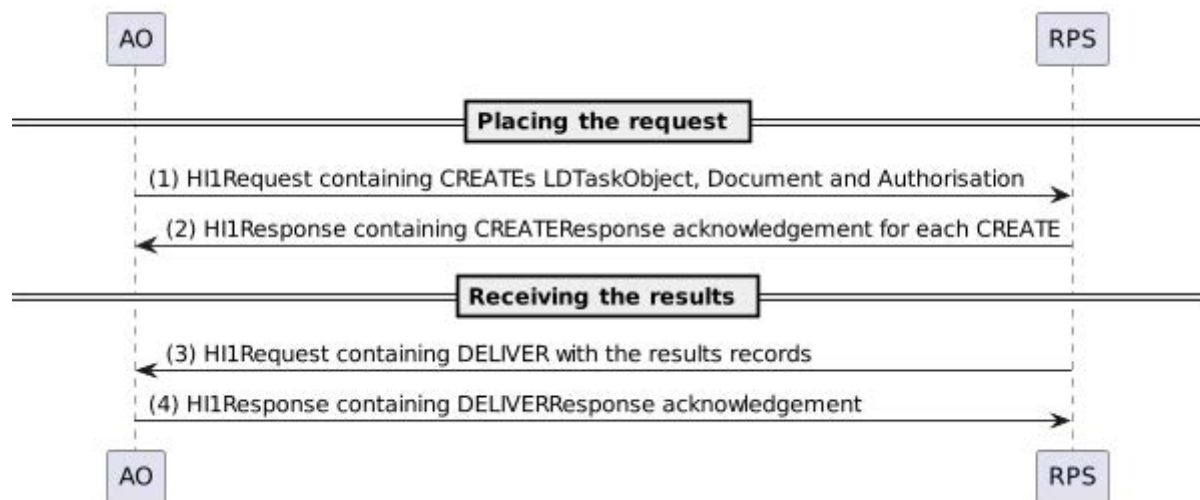


Figure C.2-1: Example message flow for requesting and receiving vehicle-related data

This separation makes the process asynchronous; that is, the request transaction can be completed, and then the results can be sent back when they are ready. This is important in order to provide for the possibility of human interaction and oversight at the RPS.

Implementers should be aware that because each transaction is initiated by a different side (the first by the AO, the second by the RPS), the Sender and Receiver identifiers are therefore reversed in the second transaction - messages (3) and (4) - compared with the first - messages (1) and (2).

Annex D (informative): Approach for supporting access to DSSAD data

D.1 Basic approach and scenarios

The approach for supporting access to DSSAD (Data Storage Systems for Automated Driving) data considers three scenarios:

- Scenario 1: Data is stored at a manufacturer database (see clause D.2).
- Scenario 2: Data is stored on a vehicle and the manufacturer has a network connection to the vehicle (see clause D.3).
- Scenario 3: Data is on a vehicle and the manufacturer has no connectivity to the vehicle (see clause D.4).

These approaches are designed to be in line with the ISO Extended Vehicles principles (ISO 20077-1 [1] and ISO 20077-2 [2]). This Annex is compatible with systems which are using a complementary ETSI/ISO approach (see Annex E).

This annex uses the term manufacturer to include the system that processes the request (RPS) and wider components of the system on the RPS side of the interface. This Annex identifies changes that would be necessary as a prerequisite to supporting the above scenarios.

D.2 Scenario 1: Approach for requests to databases

Description of the scenario: In this scenario, the relevant data is on the manufacturer's database.

Approach: The recommended approach is to use the interface defined in the present document for making a DSSAD request to the manufacturer.

Benefit: The present document ensures that there is a clear mechanism for authentication of parties involved and for securing data delivery. It provides a clear, consistent and easy-to-interpret data set. It facilitates the use automation where appropriate. This supports data access requirements from DSSAD.

Changes needed to the present document: This approach would be supported by adding a new request type (DSSADDataRequest) to clause 7 of the present document. The request and response details would be mapped directly from the relevant DSSAD documentation (the clear, strongly-typed fields from DSSAD are easy to map into JSON definitions). No additional constraints, parameters or definitions would be included as part of the mapping process.

D.3 Scenario 2: Approach for recovering data from a vehicle where there is connectivity to the vehicle

Description of the scenario: In this scenario, the relevant data is on the vehicle and the manufacturer has a network connection to the vehicle.

Approach: The recommended approach is for a request to be made to the manufacturer using the interface defined in the present document (i.e. the request is the same as Scenario 1). The manufacturer recovers the data from the vehicle (using the manufacturer's own secure techniques and processes) and then the manufacturer can respond to the request via the interface defined in the present document.

Benefit: This is a clear and simple way to achieve the same benefits described in clause D.2.

Changes needed to the present document: Same as clause D.2.

D.4 Scenario 3: Approach for recovery of data direct from vehicles

Description of the scenario: In this scenario, the relevant data is on the vehicle and the manufacturer does not have a network connection to the vehicle. A device is used to connect to the vehicle to recover data.

Caveat: Connectivity directly to a vehicle (e.g. how devices connect to the vehicle or how they recover data) is out of scope of the present document.

Approach: The present document contains a recommendation to support recovery of data from a vehicle. It is recommended that an authorisation token is used as part of the process of recovering data from a vehicle i.e. that data is not released by the vehicle until a valid authorisation token has been provided. It is recommended that the present document is used to request an authorisation token from the manufacturer and then for that token to be sent to the device that is connecting to the vehicle.

Benefit: This is a way to bring the benefits described in clause D.2 to this scenario. It gives assurance that each-and-every request has been authenticated and authorized and it helps prevent situations where devices (for connecting to a vehicle) are misused. Specifically, it helps reduce risks where devices have been lost, stolen or cloned.

Detail of the process: The recommended process for using an authorisation token is as follows:

- The AO makes a request for a token to the manufacturer over the interface defined in the present document.
- If appropriate, the manufacturer returns a token over the interface defined in the present document. The AO system sends the token to the device which will be used to access the vehicle.
- The token is presented by the device to the vehicle, which checks that the token supports the request for data.

Changes needed to the present document: This approach would be supported by adding a new request type to clause 7 of the present document, called AuthorisationTokenRequest. The request parameters would be the VIN, an identifier for the tool which will be used to recover the data, a time period during which access is needed (e.g. a specified day), and a request type which specifies the data that is requested. The response would be an authorisation token (or error message).

NOTE: It is also possible to consider an approach where the requesting party recovers an encrypted copy of the data, which is sent (using the interface in the present document) to the manufacturer for them to decrypt.

Annex E (informative): Use of the present document in combination with the ISO 20078 series

E.1 Context

Annex E provides a description of a recommended technique for using the present document in combination with systems (for the RPS side of the interface) which are based on the ISO 20078 series standards [3], [4], [5].

It is recommended to have (at least) these two components on the RPS side of the interface:

- A function which handles the AO-related requirements (called the Support Function).
- The main database running in line with the ISO 20078 series standards [3], [4], [5].

It is recommended that:

- The request is made from the AO to the Support Function (which may choose to make manual checks as described in clause 5).
- The Support Function creates a connection to the main database using the ISO 20078 series standards [3], [4], [5].
- The Support Function sends the results back to the AO in the format received from the main database.

The normative details are given in clauses 6.2.5 and 6.2.6.

E.2 Owner consent and owner notification

Annex E is designed to cover situations where a request is made and the owner/keeper/driver of the vehicle is not asked for permission to share the data. Also Annex E is designed to cover situations where an owner is not notified about the request for data. It is out of scope of the present document to discuss whether owner consent or notification is needed. When following the advice in this Annex, particular care should be taken about the requirements in Annex A concerning owner consent or notification.

E.3 Overview of data structures

An overview of the structure of the data is as follows:

- For requests and responses: it is recommended to use details such as identifiers (for the AO and RPS), timestamps, authentication details and authorisation details as defined in the present document (see clause 6).
- For the request: it is recommended to create a mapping from the request types in the present document to containers (as defined in ISO 20078-2 [4]). More details are given in clause E.4.
- For the response: it is recommended that the AO support function uses the structure of the data as it is presented to the AO support function over the ISO 20078-2 [4] interface, in line with the normative details given in clause 6.2.6.

E.4 Process and use of ISO containers

The recommended approach is for the RPS to establish one container (as defined in ISO 20078-2 [4]) for each request type that might potentially be required. Where there are different variations of the same request type (e.g. if the requests can differ because they are requesting different subsets of the response data), then the different requests will be distinguished using the Request Subtype field (see ETSI TS 103 120 [6], clauses 8.3.5 and 8.4.4). It is recommended that the RPS establishes a container for each different request subtype.

The recommended process is as follows:

- When the RPS receives a request, the Support Function invokes the relevant container and uses this to access data via the ISO gateway.
- The response from the ISO-based system is directly included in the ETSI response as defined in clause 6.2.6.

Annex F (informative): Change history

Status of Technical Specification ETSI TS 103 976 Interface for Lawful Disclosure of vehicle-related data		
TC LI approval date	Version	Remarks
February 2024	V1.1.1	First publication of the TS after approval at ETSI TC LI#65 (6-8 February 2024, Saariselkä)
November 2024	V1.2.1	Included Change Requests agreed by ETSI TC LI#67 CR001, LI(24)P67022r1 (Cat F) Clarifications CR002, LI(24)P67023r2 (Cat F) Schema fixes CR003, LI(24)P66028r6 (Cat B) New questions CR004, LI(24)P67016r1 (Cat B) Clarification on use of StartTime and EndTime
February 2025	V1.3.1	Included Change Request agreed by ETSI TC LI#68 CR007, LI(25)P68037r3 (Cat B) Vehicle Records Record Request
June 2025	V1.4.1	Included Change Requests as agreed by ETSI TC LI#69 CR008, LI(25)P69007r1 (Cat B) DSSAD Annex CR009, LI(25)P69008r2 (Cat B) ISO changes CR010, LI(25)P69009r3 (Cat B) Connected devices CR011, LI(25)P69038r2 (Cat B) Change to Authorized Organization CR012, LI(25)P69032r1 (Cat B) Zero Response Clarification

History

Document history		
V1.1.1	February 2024	Publication
V1.2.1	January 2025	Publication
V1.3.1	May 2025	Publication
V1.4.1	August 2025	Publication