ETSI TR 103 854 V1.1.1 (2022-03)

LEA support services;
Interfaces for Lawful Disclosure of vehicle-related data: scenarios, examples and recommendations

Reference
DTR/LI-00214

Keywords
interface, security, trust

ETSI

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

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

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

Contents

Intellectual Property Rights 4
Foreword 4
Modal verbs terminology 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definition of terms, symbols and abbreviations 5
3.1 Terms 5
3.2 Symbols 5
3.3 Abbreviations 6
4 Structure of the present document 6
5 Reference model 6
6 Examples of use cases 7
6.1 Overview 7
6.2 List of example use cases 7
6.2.1 Vehicle identification number to international mobile equipment identifier 7
6.2.2 International mobile equipment identifier to vehicle identification number 7
6.2.3 Vehicle identification number to international mobile subscriber identifier 8
6.2.4 International mobile subscriber identifier to vehicle identification number 8
6.2.5 Vehicle identification number to location 8
6.2.6 Vehicle identification number to vehicle data 8
7 Recommended approach for interfacing 9
7.1 Overview 9
7.2 Information fields 9
7.2.1 Request information 9
7.2.2 Response information 9
7.2.3 Format for request and response information 10
7.2.4 Data categories 10
7.3 Delivery protocols 11
7.3.1 Use of HTTP 11
7.3.2 Delivery security details 11
Annex A: Usage scenarios 12
A.1 Overview 12
A.2 Extended vehicle databases 12
A.3 European Production Order 12
A.4 Autonomous Vehicles 12
A.5 EU C-ITS WG6 12
A.6 Stolen vehicle recovery 13
A.7 Cross-border aspects 13
Annex B: Example of VIN-to-IMEI use case 14
Annex C: Change History 15
History 16

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 Report (TR) has been produced by ETSI Technical Committee Lawful Interception (LI).

Modal verbs terminology

In the present document "**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 describes an interface consisting of requests from a Law Enforcement Agency for vehicle-related data and the responses to those requests. The present document describes some usage scenarios and puts forward some examples for this interface. The present document includes a recommendation for the details of how the interface could work.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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] ETSI TR 103 767: "Lawful Interception (LI); Considerations about interfacing with providers of vehicle information".

[i.2] ETSI TS 123 003: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification (3GPP TS 23.003)".

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

[i.4] ETSI TS 103 280: "Lawful Interception (LI); Dictionary for common parameters".

[i.5] ISO 3779:2009: "Road vehicles - Vehicle identification number (VIN) - Content and structure".

[i.6] COM/2018/225 final: "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters".

[i.7] SAE J853-2009: "Vehicle Identification Numbers".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

C-ITS	Cooperative Intelligent Transport Systems
ExVe	Extended Vehicle
GPS	Global Positioning System
HTTP	Hyper Text Transfer Protocol
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
OEM	Original Equipment Manufacturer
PEI	Permanent Equipment Identifier
RPS	Response Processing System
SAE	Society of Automotive Engineers
VIN	Vehicle Identification Number
XML	eXtensible Markup Language

4 Structure of the present document

The present document includes:

- Reference model and description of basic responsibilities (clause 5).
- List of examples of use cases (clause 6).
- Recommendation for how the interface should be implemented (clause 7).
- Usage scenarios (annex A).
- Example data structures (annex B).

5 Reference model

Figure 5.1 shows the reference model for the present document.

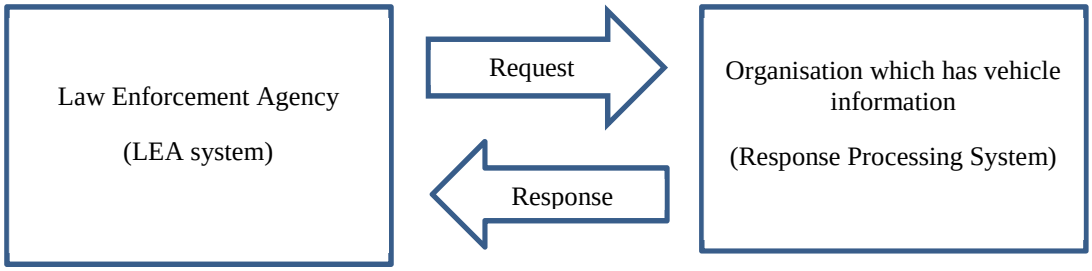

Figure 5.1: Reference model

The Law Enforcement Agency (LEA) is responsible for creating a lawful request. The LEA system delivers the request to a Response Processing System (RPS). The legal obligation on RPS (for example, what has to be delivered, what has to be retained) is considered independently of the delivery interface and is out of scope of the present document.

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 Examples of use cases

6.1 Overview

This clause contains a list of use cases which are intended to provide some useful illustrations. This is not an exhaustive list and there is no implication that these use cases are lawful or required in any particular jurisdiction (that is a legislative matter which is out of scope).

6.2 List of example use cases

6.2.1 Vehicle identification number to international mobile equipment identifier

This use case is called VIN-to-IMEI. In this use case, the LEA knows a Vehicle Identification Number (VIN) and requests the IMEI(s). An illustration is given in annex B.

Other variants of this use case could include other equipment identifiers beyond an IMEI, specifically including PEI.

For the VIN-to-IMEI use case:

- The request includes the VIN, as a string (checked to be compliant with the relevant standard, e.g. ISO 3779 [i.5] and SAE J853-2009 [i.7]).
- The response contains zero, one or more IMEI(s) (in the format defined in 3GPP TS 23.003 [i.2]) associated with the supplied VIN, or an error code.

NOTE 1: As with all use cases, the request and response would also contain the core parameters listed in clause 7.

NOTE 2: VIN-to-IMEI could be considered a canonical use case in that it is a simple, common example which is still complex enough to illustrate key concepts and challenges. It shows how to deliver benefits which are listed in ETSI TR 103 767 [i.1] (clarity, efficiency, auditability, security, privacy).

NOTE 3: This use case is only applicable to vehicles with manufacturer-issued VINs (which may exclude some vehicles from before 1985).

6.2.2 International mobile equipment identifier to vehicle identification number

This use case is called IMEI-to-VIN and is the reverse of VIN-to-IMEI, i.e. an IMEI is known and the VIN is requested.

Other variants of this use case could include other Equipment Identifiers beyond an IMEI, specifically including the Permanent Equipment Identifier (PEI).

6.2.3 Vehicle identification number to international mobile subscriber identifier

This use case is called VIN-to-IMSI. In this use case, the LEA knows a Vehicle Identification Number (VIN) and requests the IMSI(s).

Other variants of this use case could include other subscriber identifiers beyond an IMSI.

NOTE 1: There may be more than one IMSI associated with a given VIN.

The VIN-to-IMSI association could be made in a variety of ways (by the manufacturer, by a third party, at a dealer, or by the customer themselves). The present document does not comment on how or where any such association is made. The use case applies to the situation in which an RPS holds this mapping, and an LEA has lawful justification to request the data.

NOTE 2: This category could also include VIN-to-ICCID.

6.2.4 International mobile subscriber identifier to vehicle identification number

This use case is called IMSI-to-VIN and is the reverse of VIN-to-IMSI.

Other variants of this use case could include other subscriber identifiers beyond an IMSI.

6.2.5 Vehicle identification number to location

This use case is called VIN-to-Location and shows the basic relation from a VIN to a location of a vehicle. The following considerations are made:

- The location is typically identified by providing latitude and longitude, though other clear, unambiguous formats may be considered. The location provided should have a timestamp for the time that the location was observed.
- The location could include the source of location (e.g. from a network or cell site, from a GPS, user-input).
- The request for a location would need to contain a specific time or time range. The interface would support requests for very recent locations. The latency of data reaching the databases (i.e. how up-to-date the databases are) would depend on the design of the systems involved and is out of scope of the interface.
- Depending on the implementation and purpose of the location processing, the location is retrieved based on certain operational events of the vehicle, as requested by a lawful request.
- The RPS would be responsible for responding to the request. This might take place by looking in existing databases (such as extended vehicle databases or neutral servers, as per ISO's Extended Vehicle concept defined in ISO 20078-1 [i.3]). Alternatively, the relevant information might need to be retrieved by the RPS from the vehicle.

6.2.6 Vehicle identification number to vehicle data

This use case is called VIN-to-VehicleData and is a request for a set of vehicle-related data based on the vehicle's VIN. The request could be for specific categories of data (see clause 7.2.4). This use case also includes the possibility of defining a request for all the information from the RPS relating to the specified VIN. The present document does not state when or whether such a request would be lawful.

7 Recommended approach for interfacing

7.1 Overview

The approach is divided into the following clauses:

- Information fields, including schema details (clause 7.2).
- Transport protocol (clause 7.3).

An example is given in annex B.

7.2 Information fields

7.2.1 Request information

The following information would be present in a request (from the LEA):

a) Administrative details:

- Identifiers for organizations involved (LEA side and RPS side).
- A unique request number created by the LEA side (it is also possible to consider situations in which the request number is created by the RPS side, but extra care is then needed to ensure global uniqueness).
- Time the request message was prepared and ready to be sent.
- It should be possible to signal an urgency or priority of the request. The format for this field (and how it is used) is defined by national systems (this can be accommodated using a free text field for priority).

b) The details of a clear and unambiguous request:

- The type of the request being made (e.g. VIN-to-IMEI from clause 6.2.1).
- The criteria to be used for searching for information. This would depend on the request: for example, it would be a VIN for the VIN-to-IMEI use case from clause 6.2.1:
  - It includes the criteria to be used to identify the records that are being requested. This may need to include a time or time-range, depending on the request.
  - It could also include information describing which parts of the records should be sent, and which parts should not be sent. This might be based on the data categories listed in clause 7.2.4.

c) Supporting information:

- Documentation relating to the warrant or authorization where appropriate in line with national regulations. In some jurisdictions, this information is handled outside of this interface.

7.2.2 Response information

The following information would be present in a response (from the RPS):

a) Administrative details:

- Identifiers and unique request number (copied from the request).
- Time the response message was ready to send (not the same as the time of the request).

b) Response details:

- The information from the RPS which matched the clear and unambiguous request (see clause 7.2.1). The formats for the information in the response may vary (for example, between different types or makes of vehicle), therefore it is important to have both clarity about what the data means, but also flexibility of data structures - see clause 7.2.3.
- There should be clear handling of errors.

c) Supporting information:

- Nothing identified at present.

7.2.3 Format for request and response information

It is recommended that XML or JSON is used and that a schema is established for the data.

For the administrative details: it would be possible to write a clear and fixed schema for the relevant information (e.g. request number, date and time of request).

For the request parameters: for each of the common request types (e.g. the examples in clause 6) it would be possible to write a schema for the request information.

For the response parameters: it is likely there will be more variety of formats here. For simple common requests, it would be possible to write a clear schema (e.g. the IMEI for the VIN-to-IMEI example). For some query types, the responses might not always fit a single schema (might vary between different organizations). The following considerations might be relevant:

- Where appropriate each record would include the time of the observation, and potentially the location of the observation.
- A solution is for the RPS side to supply information in a schema they defined themselves, though it would be important that the schema was known and shared in advance or as part of the response.
- It would be possible to create a dictionary of common terms (which would include ETSI TS 103 280 [i.4] as a minimum). This could include other vehicle-related data such as VIN, speed, route, etc. Additionally, other standards from the vehicles industry should be included.
- It is recommended to consider the categories of data as described in clause 7.2.4. Where the data fits naturally into these categories, then this might help provide clarity.

7.2.4 Data categories

The present document identifies the following categories of response data. These may be used to help with requesting or formatting the delivery of data. There is no implication that all data will fall into one of these categories. Data should not be forced into structures or categories where it does not naturally fit, as this can cause aspects of the meaning of data to be lost.

The present document identifies the following categories of data, without implying that these data types should be stored or may be requested in any given situation:

- Identification: Identification numbers for vehicles or vehicle components.
- Location: Position at any given time.
- Routing: Planning of routes (may be different from actual routes taken).
- Driving: Driver's actions or the vehicle's assistance to the driver, including speed and information around autonomous vehicles. See clause 7.3.1 regarding live streaming of data.
- Component status: Status of individual parts of the vehicle, either user-controlled (doors, windows) or wear-and-tear and servicing. May also include fuel or battery status and expected driving range.