ETSI TR 103 767 V1.1.1 (2020-11)

Lawful Interception (LI);
Considerations about interfacing with providers of vehicle information

Reference
DTR/LI-00188

Keywords
interface, retained data

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

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.

Executive summary

ETSI TC LI has a significant experience developing international standards for interfaces to Law Enforcement to meet legal obligations to share data. The present document highlights the benefits to both parties of working in a standardized way. The present document is of relevance for organizations holding vehicle related data, as it can help to work on clear, secure, efficient and consistent interface standards.

1 Scope

The present document provides a high-level description of a process for interfacing between law enforcement and providers of vehicle information. The present document is not a legal document and does not state when or whether such an interface should be used. Instead, the present document highlights that (whenever there is a lawful requirement to deliver information) it is beneficial to use an automated, secure, efficient interface.

The present document investigates to what extent the existing TC LI specifications can be used for such an interface. The present document does not specify any details of such an interface; the interface design would need to be done in conjunction with a cross-section of the relevant industries.

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 TS 103 707: "Lawful Interception (LI); Handover for messaging services over HTTP/XML".

[i.2] ETSI TS 102 657: "Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data".

[i.3] ETSI TS 103 120: "Lawful Interception (LI); Interface for warrant information".

[i.4] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".

[i.5] ETSI TS 102 232-2: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for messaging services".

[i.6] ETSI TS 102 232-3: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services".

[i.7] ETSI TS 102 232-4: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services".

[i.8] ETSI TS 102 232-5: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services".

[i.9] ETSI TS 102 232-6: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services".

[i.10] ETSI TS 102 232-7: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services".

[i.11] ETSI TR 102 638: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Release 2".

[i.12] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

[i.13] ETSI TS 103 410-7: "SmartM2M; Extension to SAREF; Part 7: Automotive Domain".

[i.14] ETSI EN 302 665: "Intelligent Transport Systems (ITS); Communications Architecture".

[i.15] ISO 20077: "Road Vehicles - Extended vehicle (ExVe) methodology".

[i.16] ISO 20078: "Road vehicles - Extended vehicle (ExVe) web services".

[i.17] ISO 21177: "Intelligent transport systems - ITS station security services for secure session establishment and authentication between trusted devices".

[i.18] ISO 27000: "Information security management systems (ISMS)".

[i.19] 5GAA XWG5 200029: "5GAA Technical Report Tele-Operated Driving (ToD)".

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:

5GAA	5G Automotive Association
ACEA	European Automobile Manufacturers Association
CLEPA	Comité de Liaison des fabricants d'Equipements et de Pièces Automobiles (European Association of Automotive Suppliers)
DG GROW	European Commission's Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
ETSI TC ITS	European Telecommunications Standards Institute; Technical Committee; Intelligent Transport Systems
GSMA	Global System for Mobile Communications
ISMS	Information Security Management System
LEA	Law Enforcement Agency
LI	Lawful Interception
OTT	Over The Top
TLS	Transport Layer Security
UNECE.WP29	United Nations Economic Commission for Europe; World Forum for the harmonisation of vehicle regulations

4 Context

4.1 Overview

The present document is applicable to situations in which a lawful request for information is sent from Law Enforcement to organizations which hold vehicle data. The present document discusses standardizing an interface for the request and delivery of information in these situations.

4.2 Reference model

Figure 4.1 shows the reference model for the present document.

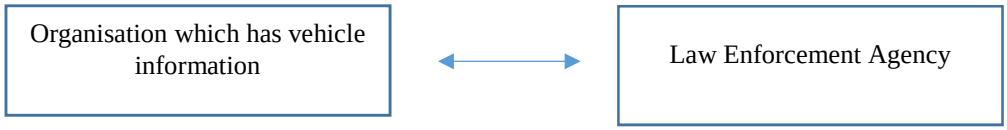

Figure 4.1: Reference model

The present document does not consider interfacing directly to vehicles.

4.3 Existing interface standards

ETSI TC LI has created interface standards for similar situations:

- ETSI TS 103 707 [i.1] is used by Over The Top (OTT) service providers to deliver information to Law Enforcement (more information is provided in clause 5.6).
- ETSI TS 102 657 [i.2] is used to request and deliver information from Communication Service Providers to Law Enforcement.
- ETSI TS 103 120 [i.3] is used as a consistent format for sending requests for information from Law Enforcement.

The present document is not proposing that the above standards should be used directly by organizations holding vehicle information. The key point is that ETSI TC LI has a track record of creating interfaces which deliver the benefits listed in clause 5, i.e. that the benefits in clause 5 are realistic and achievable if the community wishes to work together.

5 Benefits of standardized interface

5.1 Clarity and accuracy

What does this mean? A clear interface is one where each parameter has a clear meaning and a clear encoding, so that the parties involved have a common understanding of what the parameter means and that there will be no confusion about values sent.

How is this achieved? Where possible, each parameter should have its own field which is strongly typed. Sometimes it is not possible for an interface to list every possible parameter - in which case it is possible to use common dictionaries or tagging to make sure that data is well-described. Large buckets of unspecified text or binary data should be avoided.

Why is it beneficial? The data being delivered over this interface is important and sometimes life-saving, so it is important that it cannot be confused or misunderstood. It helps develop trust and build relationships if all parties explain what the data is and have confidence that it will be understood. It is important that a request for information is clear so that the organization providing the information knows exactly what it is legal to provide.

What happens without it? It is very easy to get misunderstandings which can cause problems for all involved parties, e.g. court cases could be affected by creating a mistaken picture in legal proceedings. Often it can take a lot of time to explain unclear data e.g. a number of phone calls may be necessary to try to resolve unclear information, which is an inefficient use of time.

EXAMPLE: Whenever a time is sent over an interface, clarity is important in two ways. Firstly, it is important to know exactly what the time refers to, e.g. the time an event happened, or the time a message was sent describing that event. Secondly, it is important that the time is communicated accurately, which means clarity about time-zones, daylight saving time, AM/PM and whether it is written 9/1/2020 or 1/9/2020, for 1st September 2020.

5.2 Efficiency

What does this mean? An efficient interface reduces the manual effort involved in exchanging data. If there is a large amount of data to be delivered (It is not expected that this would be the case in general) then it is important that interfaces are efficient in terms of keeping data volumes as small as possible.

How is this achieved? It is necessary to ensure that the defined interface contains all the relevant information in a clear way (see clause 5.1) to reduce the need for human effort to follow up on requests or ask for more data or clarifications. If a large amount of data is involved, then it is necessary to ensure encodings are efficient (prefer binary encodings to text unless human-readability is an issue). It is necessary to ensure that interfaces are consistent globally (see clause 5.7) so that requests can be handled in an automated way with minimal human handling (though there should always be the facility for human oversight wherever needed).

Why is it beneficial? It improves manageability and maintainability of the interaction between vehicle telematics providers and LEAs.

EXAMPLE: Many telecommunications service providers use automated, standardized interfaces to interface to Law Enforcement because it is a more efficient way of handling that volume of traffic.

5.3 Cost

What does this mean? Reducing the costs of design, implementation, deployment, management, and on-going maintenance.

How is this achieved? Aim for one language for organizations holding vehicle data to communicate with international law enforcement, and vice versa.

Why is it beneficial? Consistent standards (see clause 5.7) avoid the need for niche development and allow components to be re-used or bought off-the-shelf. Standards create global marketplaces for systems which are cheaper than bespoke systems. Clear interfaces are more efficient (see clause 5.2) and reduce staffing costs.

EXAMPLE: Lawful Interception interfaces are standardized globally and the ETSI TSs 102 232 series of standards [i.4] to [i.10] has been implemented by many different vendors, creating a strong marketplace and level playing field.

5.4 Transparency and auditability

What does this mean? Having a published interface standard where everyone can see the formats for the requests and delivery of data, i.e. it is transparent what can or cannot be sent over the interface.

How is this achieved? It is necessary to make sure there is a unique numbering scheme so that every request has a unique number. This means that requests can be counted. Any important distinctions (different types of requests, e.g. those that need different levels of authorization) can be hard-wired into the standard, so that checks can be made that the right number of warrants/authorities were issued. Links can be included so that authorizations can be traced, to the extent that this is possible while respecting the privacy of the investigation.

Why is it beneficial? It gives everyone confidence that processes are being followed (i.e. the public and those supplying the data). It allows for accurate counting and reporting which is consistent across different organizations (different providers of data and different law enforcement agencies). It facilitates formal audit processes which are vital to maintaining public confidence in these systems.

5.5 Security and privacy protection

What does this mean? A secure interface protects the confidentiality and integrity of information on it and provides authentication assurance for the parties involved.

How is this achieved? The use of standard industry-best-practice secure protocols (e.g. TLS) using up-to-date algorithms and proper profiles can give assurance to confidentiality, integrity and authentication.

Why is it beneficial? Confidentiality is important for the protection of people's privacy, i.e. only the intended recipient (in Law Enforcement) can see the results. It is also important to the running of the investigation that only the appropriate people see the information. The integrity of the information is important to the correct running of justice, e.g. that the operation proceeds on the basis of accurate information, and that evidence can be relied-upon in court. It is important that confidence can be established in the identities of the parties involved. The provider of information needs confidence that they are talking to a genuine agency; the agency needs to ensure they are talking to the organization which genuinely holds the relevant information.

5.6 Confidence across the community

What does this mean? This item relates to all parties having a common understanding and common feeling that the right processes are being followed, and that the right data is being disclosed to people who will understand it and use it correctly.

How is this achieved? It is important to go through a process of creating an interface together, sharing the requirements and needs from all sides, so that everyone has an appreciation of everyone else's intentions, and that this appreciation is built into the final standard.

Why is it beneficial? Working together builds confidence that everyone wants to achieve a common goal. Suppliers and law enforcements can gain confidence through knowing that they are operating in the same way as other suppliers and law enforcement. Good standards enable the parties involved to be proud that they are working a way which is visibly and obviously correct (i.e. in line with all relevant legislation). If there are misunderstandings or problems, then they can be resolved quickly and by consensus. If people are challenged about their practices, they can point at a global standard and explain that they are working to meet legislation in a way which is clear, consistent and transparent.

EXAMPLE: In ETSI TC LI OTTs and LEAs work together as they recognize that they share a common goal in making standards which can be used (where there is a lawful requirement to do so) to exchange data in a way which is clear, transparent, auditable, secure, privacy-protecting, efficient and consistent across many countries and operators, see ETSI TS 103 120 [i.3]. ETSI TS 103 120 [i.3], and the process that was used to create it, could be a good example for working with vehicle providers.

5.7 Consistency

What does this mean? As far as is possible, the same interface standard is used across different countries and different providers of information.

How is this achieved? It is necessary to work together to create a common standard, which uses consistent terms wherever possible. In some contexts, it is clear that different organizations have different information and this should not be constrained - ETSI TC LI has experience of creating a flexible standard that is strict and strongly typed where possible but agile in other contexts (e.g. by allowing people to define their own mini-schema for certain components).

Why is it beneficial? It is cheaper and easier for the owners of vehicle data to design one system which works for many countries. It is easier and clearer for law enforcement to receive data from different providers in the same format. The possibilities for misunderstanding are reduced if everyone uses the same terms for the same concepts. This helps allow data to be compared regardless of its origin or routing (e.g. Wi-Fi or cellular).

What happens without it? Telematics data formats from different vehicle brands, or different models of the same brand, are different. Decoding becomes a big challenge. Efficiency and cost-effectiveness (see clauses 5.2 and 5.3) are reduced.

Annex A:
Existing standards and groups supporting vehicle telematics data

A.1 Standards for vehicle data

Table A.1 lists standards which support vehicle telematics data.

Table A.1: Standards which support vehicle data

Standard	Description
ETSI TR 102 638 [i.11]	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions
ETSI TS 102 940 [i.12]	Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
ETSI TS 103 410-7 [i.13]	SmartM2M; Extension to SAREF; Part 7: Automotive Domain
ETSI EN 302 665 [i.14]	Intelligent Transport Systems (ITS); Communications Architecture
ISO 20077 [i.15]	Road Vehicles - Extended vehicle (ExVe) methodology
ISO 20078 [i.16]	Road vehicles - Extended vehicle (ExVe) web services
ISO 21177 [i.17]	Intelligent transport systems - ITS station security services for secure session establishment and authentication between trusted devices
ISO 27000 [i.18]	Information Security Management Systems (ISMS)
5GAA XWG5 200029 [i.19]	5GAA Technical Report Tele-operated Driving (ToD)

A.2 Standards groups for vehicle data

The following standards groups are relevant to Telematics Data:

- ACEA.
- CAR 2 CAR communication consortium.
- CLEPA.
- European Commission DG GROW.
- ETSI TC ITS: Intelligent Transport Systems.
- GSMA.
- UNECE.WP29.
- 5GAA.

Annex B:
Change request history

Status of the present document: Considerations about interfacing with providers of vehicle information		
TC LI approval date	**Version**	**Remarks**
October 2020	1.1.1	First publication of the TR after approval by Remote Consensus following TC LI#55e (electronic meeting)

History

Document history		
V1.1.1	November 2020	Publication