ETSI TR 104 195 Vm.t.e (2026-01-09 1900CET)

Lawful Interception (LI);
Study on LI for Encrypted Electronic Communications Services (ECS)

Should you need a step-by-step guide for drafting an ETSI deliverable, please consult the "Principles for Drafting ETSI Deliverables" document. Otherwise you may contact us at edithelp@etsi.org.

TECHNICAL REPORT

Reference
<Workitem>

Keywords
<keywords>

Contents

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

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.

Foreword

This Technical Report (TR) has been produced by {ETSI Technical Committee|ETSI Project|<other>} <long techbody> (<short techbody>).

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

Introduction

1 Scope

The present document contains a discussion about possible approaches for the LI architecture of number-based or number-independent (interpersonal) communications of electronic communications services (ECS), see Directive (EU) 2018/1972 establishing the European Electronic Communications Code (see [i.3]) and similar acts. The approaches are designed to realize forwarding copies of communications contents (CC) from a specific target, in accordance with the provisions of the legislation (i.e., so that it can be understood by law enforcement, as defined by the legislation), while maintaining the confidentiality level of the ECS. The approaches consider the protection and the strict control of usage of the proposed LI mechanism. The present document addresses considerations arising from the need for the ECS provider to support strong encryption and data protection measures while ensuring compliance with relevant legislation. The present document includes discussion points put forward by all participants representing a broad range of ideas and reflects all points of view by including feedback (pros and cons) from all stakeholders (see [i.1]).

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 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] The concluding report of EU Concluding Report of the High-Level Group

on Access to Data for Effective Law Enforcement of 15 November 2024

https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en#concluding-report

[i.2] Communication from the Council Presidency on Law Enforcement Operational Needs for Lawful Access to Communications (LEON), 6050/23 of 16 February 2023

https://data.consilium.europa.eu/doc/document/ST-6050-2023-INIT/en/pdf

[i.3] Electronic Communications Code Directive (Directive (EU) 2018/1972).

https://eur-lex.europa.eu/EN/legal-content/summary/european-electronic-communications-code.html

[i.4] ETSI TS 101 331: “Lawful Interception (LI); Requirements of Law Enforcement Agencies”.

[i.5] Paper 2021/321 “Abuse Resistant Law Enforcement Access Systems ARLEAS”.

https://eprint.iacr.org/2021/321

3 Definition of terms, symbols and abbreviations

3.1 Terms

For further study.

3.2 Symbols

For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

3.3 Abbreviations

For the purposes of the present document, the [following] abbreviations [given in ... and the following] apply:

ECS	Electronic Communications Services
ECSP	Electronic Communications Services Provider
LEA	Law Enforcement Agency
LI	Lawful Interception

4 Context

4.1 Summary

For further study.

4.2 Requirements

4.2.1 Explanation

The present document identifies LI requirements which are most relevant to encrypted communications. It is not intended to be a complete set of LI requirements.

The requirements are derived from the Law Enforcement Operational Needs document [i.2], existing standards (e.g., ETSI TS 101 331 [i.4]), legislation and academic documents (for example: Paper 2021/321 Abuse Resistant Law Enforcement Access Systems ARLEAS [i.5]).

The legal requirements for LI are defined by the relevant legislation, not by standards. The requirements in the present document are to be interpreted in accordance with applicable national policies.

The present document is considering a situation where a provider is lawfully required to perform LI and where a provider receives a lawful request. The present document is considering a situation where the provider is creating a service or managing a service (e.g., the provider provides an application) that provides encryption between parties and where the provider is required to facilitate the relevant parties in the LEA being able to see a copy of the data en clair (i.e., to have an understandable copy of the information as the communicating parties sent and received it).

4.2.2 Requirements

4.2.2.1 Basic requirements

Certain basic requirements remain unaffected by the security on the communication itself. The present document does not cover these requirements in detail. It is useful to mention them briefly to provide a core level of reassurance. The basic requirements specify that:

- RG 1: Each and every request is demonstrably and transparently lawful.
- RG 2: The request for LI is made over a secure and authenticated channel between LEA and ECSP and in internal LI systems of the ECSP.
- RG 3: The target of LI is accurately identified i.e.; the system is unable to be used for indiscriminate monitoring.
- RG 4: LI takes place against an approved target identifier. ~~The present document does not define how strongly a target identifier needs to be associated to a human~~. ~~However, relevant examples is that lawful interception may be based on identifiers such as IMSIs or e-mail addresses which might or might not be directly associated with a human.~~
- RG 5: The ECSP performs LI under the provider’s control and in accordance with the authorisation provided (this means that the identification and time limits in the authorisation are observed).

- RG 6: The results are handed over from ECSP to LEA to an authenticated endpoint using a secure connection.

- RG 7: Notification of the LI target takes place in line with legislation: LI systems have the ability to perform LI without the target's knowledge where required; LI systems have the ability to securely inform the target about the LI in line with legislation.

- RG 8: The LI system of the ECSP manages situations where multiple LEAs have requested LI on the same target. This is done without letting ~~informing either~~ any other LEAs to detect such request and interception. (See also RT 1)

- RG 9: All communications of the LI target using the ECSP service are able to be intercepted in line with legislation.

4.2.2.2 Preventing abuse

The requirements in this category relate to preventing abuse at any point. The basic requirements (preventing unauthorised disclosure; secure transmission of data) are covered in clause 4.2.2.1.

The requirements in this category are specifically focussed on resisting unauthorised uses of LI systems (see also document LEON [i.2] clause 11.1):

- RA 1: LI systems are designed to avoid single points of failure internal to the ECSP, i.e., avoid giving any single staff member the ability to have unauthorised access. This could be achieved using mechanisms for separation of duties, access control and comprehensive audit/logging (securely stored and independently monitored) of all interception and attempted interception activities.

- RA 2: LI systems are designed to resist abuse from parties external to the provider. See also clause 4.2.2.4.

- RA 3: Indications of abuse are reported to the relevant authorities as required by applicable legislation.

- RA 4: The usage of the LI mechanism is subject to protection and strict control by the ESCP; it is not possible for it to be used for any other purposes than LI.

4.2.2.3 Oversight

The requirements in this category relate to allowing oversight from a wide variety of places e.g. LEA, provider, independent auditors, independent authorities, courts, judicial monitoring, parliament. It important to observe the legislative limits on this (e.g., need for confidentiality and for integrity of the interception).

- RO 1: Where required by legislation, specialist team members and auditors (with relevant security clearance) can check all relevant details, matching up records from provider and LEA to perform independent audit.

- RO 2: Where required by legislation, and when LI material is used in court, authorised parties can retrospectively perform checks, including checks that the correct authorisation and procedures were in place at the time of interception and can make checks on the material itself.

- RO 3: The details of the protocols used should be published (e.g., by using published standards and documents such LEON [i.2]) where it does not contravene other requirements.

4.2.2.4 Security of the communications service

The requirements in this category relate to maintaining the security of the underlying communications service i.e., sufficient, effective security is maintained for all accesses (including any LI accesses). The requirements specify that:

- RS 1: Intercepted Data and related meta data can only be accessed by those who are lawfully entitled to access them; the privacy of all users is maintained while meeting LI requirements.

- RS 2: The LI access does not use weaker protocols than those used for the non-LI parts of the service. Security of the LI system (including delivered data and meta data) should be at least at the same level as the underlying service.

- RS 3: The security of cryptographic algorithms and protocols used in any part of performing LI is not weaker than the security of cryptographic algorithms and protocols used in the underlying communications system.

EXAMPLE 1: If the protocol used by end-users to encrypt their communication has a formal security proof, then that proof holds also when LI is activated on that protocol.

EXAMPLE 2: The protocols used on the handover interfaces offers the same (or higher) cryptographic strength as the protocol by which the end-users protect their traffic.

-RS 4: The LI system is hardened using industry best-practice standards and techniques. It is set up and managed following appropriate cyber risk management standards and best practice. Such security management should be conducted regularly and updated appropriately.

-RS 5: The data and meta data collected by the LI system is protected from unauthorised access throughout collection, transmission and in any temporary storage (if used) until it is delivered to the Law Enforcement system.

NOTE: It is helpful to consider situations where the ECSP does not (for its normal business purposes) have en clair access to content. In these situations, it is helpful to demonstrate that LI can still take place (i.e. the LEA can see en clair content in line with lawful requirements) without compelling the Provider to have en clair access to any of its content (i.e. the Provider does not need to see the intercepted material en clair). In these circumstances, it would still be essential that the Provider has access to information necessary to perform all required audits.

4.2.2.5 Other security points

- RT 1: The target of the lawful interception does not have the ability to see that interception is taking place (except were described in RG 7). LI has to be undetectable to other users, to the target, to other LEAs and to unauthorized staff members. This means in particular that the quality of service (from the perspective of the target) is not noticeably different because of interception taking place.

- RT 2: Any user of ECS ~~who are in the communications~~, is not able to avoid lawful interception capabilities to be put in place by the ESCP. ~~the possibility of being lawfully interception being applied to the service. All ECSP services and any users are able to be subject to LI.~~

4.2.3 Continually improving the security of LI

New security requirements should be included wherever they improve LI security and do not make the overall requirement set impractical to build. The present document recommends against including mandatory requirements which cannot be met by any practical solution.

5 Key Issues

5.1 General

For further study – this clause will be used to present and discuss key issues.

6 Potential Solutions

6.1 General

For further study – this clause will be used to present a range of potential solutions.

7. Summary

For further study – this clause will be used to assess the potential solutions against the key issues in clause 5 and requirements in clause 4.2

Annex A:
Title of annex

Annex: Bibliography

-

Annex:
Change history

Date	Version	Information about changes
<Month year>	<#>	<Changes made are listed in this cell>

History

Document history		
<Version>	<Date>	<Milestone>

Latest changes made on 2025-06-19