Council of the European Union

Brussels, 16 February 2023
(OR. en)

6050/23

LIMITE

COPEN 27
JAI 114
DATAPROTECT 28
TELECOM 29
ENFOPOL 49
CYBER 22
EUROJUST 1

NOTE

From:	Presidency
To:	Delegations
Subject:	Law Enforcement Operational Needs for Lawful Access to Communications (LEON) - Presentation by the Swedish Police and the Swedish Security Service

Delegations will in the Annex find the document Law Enforcement – Operational Needs for Lawful Access to Communications (LEON). LEON is the outcome of work undertaken by Swedish law enforcement agencies, in close co-operation with law enforcement representatives in EU Member States, North America and Australia. The aim is to identify and describe the law enforcement needs for lawful access to communications content, content related data and subscriber information.

Swedish law enforcement agencies have presented LEON in a number of international contexts, including at EU level. LEON has received broad support in the international law enforcement community.

As discussed at the informal meeting of JHA-Council on 26-27 January 2023, the Presidency recognises the need for a broad discussion on EU-action to enhancing and improving the access to data, electronic evidence and information for law enforcement purposes and judicial purposes. The Presidency will follow-up the conclusions of the informal JHA-Council in particular in the Standing Committee on Operational Cooperation on Internal Security. Lawful access to communications is obviously an essential issue in the context of discussing the need for access to data, electronic evidence and information for law enforcement purposes and judicial purposes. The Presidency believes that LEON is a well-structured contribution that describes the needs of law enforcement agencies for lawful access to communications.

LEON may also be used by Member States as guidelines for reviewing or updating national legislation and for technical discussions within standardisation bodies.

Law Enforcement – Operational Needs for Lawful Access to Communications (9 June 2022)

Contents

Introduction

Criminals, like anyone else, use communications in pursuit of their objectives. They take advantage of opportunities offered by communications systems both to avoid detection and to commit offences.

Lawful access to these communications is vital in the investigation of serious crime and the prosecution of offenders.

In 1993, representatives from various Law Enforcement Agencies (LEAs) in Europe, North America and Australia met to consider the impact on Lawful Interception (LI) of developments taking place in the communications industry. The representatives of these democracies paid particular attention to the need for sophisticated LI facilities within mobile networks. At the request of the communications industry, consideration was given to the development of a draft set of common requirements that could be considered by manufacturers in the development of new communications systems.

The requirements (International User Requirements: IUR) were agreed by the LEAs in 1994, presented to the European Council of Ministers and were then adopted as the European Council Resolution 96/C329/01 of 17 January 1995 on the Lawful Interception of Telecommunications. This Resolution was published in the Official Journal of the European Communities No.C329, 4.11.1996, p1. Some countries decided to align their national legislation with the requirements.

In Europe the European Council Resolution 96/C329/01 of 17 January 1995 was also brought in to the European standards body (ETSI) and the 3rd Generation Partnership Project (3GPP) to ensure LI by design.

In due course the United States of America, Canada and Australia recognised the IUR. They took account of the IUR in their national policies and recommended that it be used as a basis for discussion with the communications industry, standards bodies and others.

As a result of these activities LI by design occurred in many jurisdictions, both in Europe and elsewhere.

In the light of a rapidly changing environment in the telecom sector during the first two decades of the 21st century the IUR needs to be reviewed. Terms have to be aligned or generalised to maintain the LEAs capabilities of lawful interception. The IUR was reviewed in 2001 and the results were presented in the EU (Enfopol 55).

Nevertheless, in terms of lawful access the functional needs of LEAs (in this document referred to as Law Enforcement Operational Needs, LEON) will in essence remain consistent independent of any existing or emerging (communication) technology as they relate to public safety and the criminal justice process. Lawful access is essential in the context of investigations where core needs are not altered in conjunction with the rapid evolution of technology. Lawful access will remain an important measure to fight any kind of threats to public safety and serious crime in democratic societies as people require from their governments for the provision of safety and security for everyone's life.

The LEON remains subject to the implementation of national legislation and regulation.

Scope

General

Subject to national legislation, all kinds of communications may be subject to lawful access in relation to enquiries. This document relates to the operational needs of LEAs with respect to communications networks and services. This document does not address a specific national law or recommend technical specifications or solutions. It is a set of guidelines for policy makers and for technical discussions, preferably in international standardisation bodies such as ETSI and 3GPP.

In this document the term lawful access will be used instead of lawful interception since it also addresses some operational aspects closely associated to LI. These aspects include for example the provisioning of the Subject of Interest's (SoI) identification for LI. The SoI could not only be a person but also an object that is covered by the lawful authorisation. (Examples of objects can include but are not limited to: vehicles, smart sensors, navigation systems.)

The document does not address data retention requirements.

Applicable Services

This document applies to all communication services, independent of the network or platform they operate on and also independent of the type of access (e.g. mobile, wireless or fixed).

The term communication services in this document is technology neutral and is not limited to a fixed concept of telecommunication services used in the past. It includes communication services used today and those that may be used in the future.

Access to Communications

When talking about access to communications in this document the term communications technically comprises two parts. The first part is the content of a communication of a SoI (information exchanged between the communication partners like messages, voice, video etc.). The second part is the sum total of communications related data (e.g., the identifiers pertaining to the communication partners or time and date when the communication takes place, location information). LEA requirements for communications applies to both unless otherwise stated in this document.

General Observations

New Types of Communication and Networks

In the 2000s, there was increasing use of Internet for communication and a wealth of new communications services available. The fast and ongoing development of new communication technologies has resulted in tremendous challenges for LEAs when conducting lawful access.

Traditional telephone calls and Short Messaging Service (SMS) now represent a small fraction of the modern communications environment. Instead the use of new encrypted communication technologies via Internet, such as Internet-based voice and messaging services, are dominating the market. Generally these new types of communications services are developed without taking "Lawful access by design" into account.

In order to prevent, detect, investigate and prosecute criminal offences and Internet enabled criminal offences it is necessary to undertake lawful access also in the online environment, and in any number of otherwise connected networks. The SoI may even be a vehicle or smart device authorised for lawful access.

New types of mobile communication networks are causing new challenges through such factors as extreme bit rates, new types of connected devices, network virtualisation, anonymisation, pseudonymisation and use of artificial intelligence.

Encryption

While encryption technology is important to ensuring privacy and confidentiality of communications, encryption provides extreme challenges for LEAs despite the fact that the access to such data would be lawful. The communication and application industry are increasingly designing electronic devices and applications to encrypt communications and user data by default, resulting in more frequent use of end-to-end encryption.

"Digital life" and cyberspace presents considerable challenges consisting of certain vulnerabilities and the potential for exploitation for criminal purposes. Thus criminals can include readily available, off-the-shelf encryption solutions designed for legitimate purposes in their modus operandi.

Independently of the technological environment of the day, it is therefore essential to preserve the powers of competent authorities in the area of security and criminal justice through lawful access to carry out their tasks, as prescribed and authorised by law.

Lawful Access by Design and Privacy by Design

Traditional communication services were developed using lawful access by design and also with legal frameworks requiring service providers to implement solutions for lawful access. These requirements were also covering encrypted services where service providers are obligated to deliver the communication content “en clair”.

In conjunction with these developments, the level of public discussion and concern about protecting the privacy of communications increased. Consequently, new and emerging technologies have been developed ensuring capability for privacy protection often encrypted with no tools for lawful access implemented (sometimes referred to as privacy by design). In many cases these new communication technologies are not clearly covered by legal frameworks requiring lawful access.

Efforts are needed to ensure it is well understood by the industry and the public that the goals of ensuring lawful access by design and privacy by design are requirements that can be applied in common and can complement each other. A forum for developing technical solutions to meet the law enforcement operational needs could preferably be in the open international standardisation bodies such as ETSI and 3GPP.

Provider Obligations for Distributed Communications Services

The evolution of communication services, particularly distributed application software, reflects a paradigm change in the communications industry necessarily requiring a reconsideration of which actors playing an operative role in facilitating those communications should be considered “a provider” for lawful access purposes. Where once public switch traditional telephone companies could be considered the sole communications provider for lawful access purposes, today’s communications services are facilitated by and dependent upon an environment maintained by a number of providers.

These would include Internet access service providers, Internet-based communications service providers, communication device operating system providers, hosting providers, and communications device manufacturers. Role-based obligations for lawful access should be considered in legislation and regulation for all involved providers that facilitate those communications.

Global Market

The communication market has moved to global Internet-based communication services where providers can have billions of subscribers in many countries. These providers might not have a legal or physical entity in countries where they are offering their services. This does not eliminate the need for LEAs to have lawful access in the country where the service providers offer their service.

Maintaining Capability

It is obvious that legal frameworks cannot evolve at the same speed as technological evolution. Therefore lawful access must be independent of, and resistant to, technological changes.

The lawful access needs relating to traditional communications systems are equally applicable to any other communications technologies, including (but not limited to) email, Internet-based messaging platforms, social media, gaming communication networks, and all future communications technologies and platforms.

Law Enforcement Operational Needs (LEONs)

LEONs identified in this document refer to obtaining information pursuant to lawful authority. Throughout this document each operational need is presented first, followed by explanations/clarifications where applicable.

1. Access to Communications Content

[LEON 1] *Law enforcement agencies require access to the entirety of the communications content transmitted, or caused to be transmitted, to and from the identifier of the service used by the Subject of Interest.*

The entirety of the communication content means what is specified in the scope and timeframe of the lawful authority.

[LEON 1.1] *Law enforcement agencies also require access to content if it is stored by the service provider as part of the communication.*

The need explained in LEON 1.1 applies, for example, to stored communications content if generated or accessed during the authorised period even if it is stored in a sub party system such as third party cloud.

2. Access to Communications Related Data

[LEON 2] *Law enforcement agencies require access to the entirety of the communications related data generated or processed in support of the Communication Service related to the Subject of Interest. Communications related data includes but is not limited to:*

1) *signalling of service and access status and state information, including mid communication signalling and routing information,*
2) *addressing and identifier information for communication and communication events,*
3) *formats, media, and parameters of the communications,*
4) *source of information,*
5) *time stamping.*

The needs explained in LEON 2 apply to all communication services offered directly by the provider furnishing facilities or over another provider's facilities. This information may be included in the signalling associated with the communications or an accurate indication of the state/process of the communications.

Communications related data shall include all network and service identifiers used to generate, process, or route the SoI's communication service(s).

For example, identifiers should include both local and global identifiers for the communicating party(ies). Application-based communication services could include both the application-level service identifier and a network layer routing address (e.g. IP address) associated with routing to the identifier. Mobile networks could include both local temporary or concealed identifiers and the permanent identifier.

The LEON 2 1) states the need for information related to the management of the communication and underlying access. Examples of this information includes but is not limited to:

- Idle, active, on hold
- Logged in, logged off
- Attach, detach
- Start, end
- Rerouted, forwarded, diverged
- Send, delivered, read
- Attempted, established, successful, failed
- Cause (user, network, service)

The LEON 2 2) states the need for addressing and identifiers of the communicating entities events including rerouted or translated information. Examples of this information includes but is not limited to:

- Role (source, destination, intermediate, associated, initial, final, end user, server, mailbox, host, participant)

- Fixed, translated, temporary
- Network
- Service
- Hardware

The LEON 2 3) states the need for information on the characteristics of the communications. Examples of these characteristics includes but is not limited to:

- Bearer service
- Media
- Protocol
- QoS
- Parameters, qualifiers

The LEON 2 4) states the need for identification of the originator of the information provided. Examples of the types of originators include but is not limited to:

- Network based information
- Service based information
- User based information

The LEON 2 5) states the need for accurate timestamping of the communication and communication related data.

3. Access to Location Information

[LEON 3] *Law enforcement agencies require information on the most accurate and reliable location (geographical, physical or logical) derived from each source known to the service provider for a subscriber. Law enforcement agencies shall be able to determine the accuracy and quality of the provided location.*

[LEON 3.1] *Law enforcement agencies require the location be presented in a form that is easily interpreted.*

[LEON 3.2] *Law enforcement agencies require the location information to have a time stamp of the location(s) observation.*

It is important for LEAs to know both the accuracy of the location information received, as well as the method used to calculate the location. As an example, this information may contain a cell site id, secondary cell-id, cell sector information, timing advance, signal strength, real or predicted etc.

The type of information provided will depend on the service implementation, but should be as accurate as possible. If the service provider does not generate or process location information for the offered service, the provider must maintain access to available location information (e.g. underlying network or device). Due to location manipulation technologies such as spoofing, location information provided by the user's device (only) may not necessarily be considered reliable but will still be required.

If a communications provider uses multiple sources of location (e.g. Global Navigation Satellite Systems [GNSS], cellular, WiFi) the location information from each source shall be provided. The most accurate location information derived from each source shall be provided.

4. Access to Information on the Subject of Interest

[LEON 4] *Based on a lawful enquiry and before implementation of the lawful access, law enforcement agencies require*:

1) *the Subject of Interest's distinctive identifier required for lawful access,*
2) *information on the services and features of the communications system used by the Subject of Interest and delivered by communication service providers.*

LEON 4 states the need for information which will support LEAs' requests for lawful access. Typical information required for lawful access can include but is not limited to:

- a technical identifier such as a:
    - service number,
    - equipment identifier,
    - base station number,
    - or email address;
- the full name of the person (or company) subscribing to the service;
- the residential address of the subscriber (or registered business address of a company);
- the postal address to which accounts are sent;
- credit card or other payment service details sufficient to identify the account;
- the directory name if applicable (note that this may differ from the subscriber's name);
- the directory address if applicable (note that this may differ from the residential or postal address).

LEON 4 also states the need for all information (e.g. identifiers, addresses and devices) associated to the SoI. Depending on the characteristics of the service provided multiple devices and/or multiple identities can be associated with a SoI.

5. Access to Encrypted Services

[LEON 5] *Law enforcement agencies require communication service providers to deliver lawfully accessed communications that are intelligible for law enforcement agencies notwithstanding that there are encrypted services offered (for example en clair).*

LEON 5 applies, for example, if communication service providers initiate or facilitate encryption for their communication service, LEAs require the communication service provider to deliver the communications unencrypted, maintaining the communication security. International state of the art standards shall be used where possible.

In architectures where encryption capabilities offered by a provider are distributed among more than one provider, the obligation for delivery of communications "en clair" shall be accounted for in the design of the system. This applies, for example, to home routing and private network routing.

6. Access to Communications from Roaming Subject of Interest

[LEON 6] *Law enforcement agencies require access to all communications of a service that a Subject of Interest is using even when the Subject of Interest is not a direct subscriber of that service provider.*

[LEON 6.1] *Law enforcement agencies require the lawful access capability for the Subject of Interest to be equivalent whether they directly or indirectly are a user of the service.*

[LEON 6.2] *Law enforcement agencies require the lawful access to be implemented in such a way that it is not detectable by the Subject of Interest's direct service provider.*

LEON 6 states the need for roaming users/subscribers. The LEON 6 applies to arrangements such as roaming on cellular networks and access to wireless LAN.

LEON 6.2 states the need that the home network shall not be aware of lawful access activities in the visited network.

7. Access to Diverted Communications

[LEON 7] *Law enforcement agencies require access to the communications even when the Subject of Interest's communications are diverted or transformed.*

LEON 7 states the need for communication to be available even when diversions take place within the domain of the service provider. These diversions may either be to a different destination (e.g. redirection of voice calls; forwarding of email) or transformed to a different communication format (e.g. uses of unified messaging).

8. Conditions for Authorised Access

[LEON 8] *Law enforcement agencies require that the communications be provided in a manner to exclude any communications that do not fall within the scope of the lawful access authorisation.*

LEON 8 is self-explanatory, but it should be noted that fulfilling the need in detail will depend on individual national jurisdictions.

9. Conditions for Point of Lawful Access

[LEON 9] *Law enforcement agencies require a physical point of lawful access within the nation/region of jurisdiction.*

LEON 9 states the need for a physical point of access for provisioning and a physical point of access for transmission of the intercepted communications to be performed in such a way that the confidentiality and integrity of the product are maintained.

10. Conditions for Real Time Capability

[LEON 10] *Law enforcement agencies require a real time, full time monitoring capability for the lawful access of communications.*

LEON 10 states the need for communications to be provided to the intercepting agency without undue delay (in real time or near real time). This will be dependent on the typical performance of the technology used and any special conditions imposed.

Provision of a real time and full time monitoring capability might require resilience and redundancy.

11. Security and Reliability

[LEON 11] *Law enforcement agencies require lawful access to be implemented so that neither the Subject of Interest nor any other unauthorised person or automated process is aware of any changes made to fulfil the lawful access order. In particular, the operation of the Subject of Interest's service must appear unchanged to the Subject of Interest.*

LEON 11 is self-explanatory, but it should be noted that communications services must be capable of performing lawful access without indicating this to SoI, other users, service provider staff, or automated process (e.g. Artificial Intelligence). When network virtualisation services are used the service provider must ensure that the aspect of security is maintained at least to the same level as for traditional non virtualised services.

[LEON 11.1] *Law enforcement agencies require the lawful access to be designed and implemented to preclude unauthorised or improper use and to safeguard the information related to the lawful access.*

LEON 11.1 is self-explanatory, but it should be noted that security considerations cover issues such as unauthorised access to facilities, site and personnel security.

[LEON 11.2] *According to national laws and regulations, communication service providers could be obliged to maintain an adequately protected record of activations of lawful access.*

LEON 11.2 is self-explanatory, but it should be noted that the same level of security applies to records of activation as to the lawful access facilities. The term activation also covers cessation and extensions.

[LEON 11.3] *Law enforcement agencies require communication service providers to protect information from unauthorised disclosure on which and how many lawful access authorisations are being or have been performed and not disclose information on how lawful access is carried out.*

LEON 11.3 is self-explanatory, but it should be noted that it applies to all communications providers.

[LEON 11.4] *Law enforcement agencies require the quality of service of the lawfully accessed communications as delivered to the law enforcement agency be no less than the quality of service provided to the Subject of Interest.*

LEON 11.4 is self-explanatory.

[LEON 11.5] *Law enforcement agencies require communication service providers to operate and maintain their lawful access facilities as an essential core function.*

LEON 11.5 is self-explanatory.

[LEON 11.6] *Law enforcement agencies require a service provider to disclose to the law enforcement agency the use of a process that is identified as artificial intelligence if such technology is used to perform lawful access.*

LEON 11.6 states the need for notification if, for example, artificial intelligence is used by the provider to identify the SoI. The identification of artificial intelligence and the consequences of the use of artificial intelligence are national issues.

LEON 11.6 also states the need for service providers to have a tool that will indicate if a non-authorised person uses artificial intelligence to detect lawful access activities.

12. Response Time

[LEON 12] *Law enforcement agencies require communication service providers to implement lawful access as quickly as possible.*

LEON 12 states the need for administrative facilities and technical designs which enable providers to implement lawful access efficiently. In urgent cases the lawful access has to be activated within minutes. This response requirements of LEAs will vary by country and by the type of communication service that is to be accessed.

13. Multiple and Simultaneous Lawful Access

[LEON 13] *Law enforcement agencies require communication service providers to make provision for implementing a number of simultaneous lawful access sessions.*

[LEON 13.1] *Law enforcement agencies require the capability to support multiple lawful access sessions for a single Subject of Interest's service.*

[LEON 13.2] *In the case of multiple lawful access sessions for a single Subject of Interest, communication service providers should take precautions to safeguard the identities of the monitoring agencies and the confidentiality of each investigation.*

LEON 13 states the need to support multiple simultaneous lawful access sessions for different SoI's. The maximum number of simultaneous lawful access sessions for a given subscriber population will be in accordance with national requirements.

LEON 13.1 states the need, for example, to allow simultaneous monitoring by more than one law enforcement agency.

14. Delivery

[LEON 14] *Law enforcement agencies require communication service providers to provide one or several lawful access interfaces from which the accessed communications can be transmitted to the law enforcement monitoring facility. These interfaces have to be commonly agreed on by the law enforcement agencies/lawful access authorities and the communication service providers. Other issues associated with these interfaces will be handled according to accepted practices in individual countries.*

LEON 14 is self-explanatory. It should be noted the need to provide information on the technical parameters of the transmission to the law enforcement monitoring facility is essential. The use of international state of the art standards is preferred.

[LEON 14.1] *Law enforcement agencies require lawfully accessed communications be provided in a way that allows for the accurate correlation of communications, related data and content.*

LEON 14.1 states the need for correlation. This may be intrinsic in some technologies where communications related data is delivered together with communications content. If this is the case the service provider should separate the communication related data from the content. However, where this is not the case a reliable method for correlation should be used. The correlation of different streams/channels of communications content is also required. International state of the art standards shall be used where possible.

[LEON 14.2] *Law enforcement agencies require that the format for transmitting the lawfully accessed communications to the law enforcement monitoring facility be a generally available format. This format will be agreed upon on an individual country basis.*

LEON 14.2 states the need for law enforcement to receive the communications in a publically available format. If the communication service provider utilises a proprietary encoding or compression technology on the communications they should provide the communications in a publically available standardised format.

International state of the art delivery standards shall be used where possible.

[LEON 14.3] *Law enforcement agencies require the transmission of the lawfully accessed communications to the law enforcement monitoring facility meet applicable security requirements.*

LEON 14.3 states the need for transmission of lawfully accessed communications to be performed in such a way that the confidentiality and integrity of the product are maintained. The product may be used as evidence for both defence and prosecution purposes; the confidentiality needs to be maintained both to meet privacy considerations and for investigative reasons.

[LEON 14.4] *Law enforcement agencies require communication service providers to ensure that lawfully accessed communications are only transmitted to the law enforcement monitoring facility consistent with the lawful access authorisation.*

LEON 14.4 is self-explanatory and applies to all communications providers.

[LEON 14.5] *Law enforcement agencies require communication service providers to be able to deliver a complete and single communication product per authorisation to the dedicated law enforcement agency.*

LEON 14.5 states the need that the communication service provider, when lawfully accessing the communications at more than one point of access within its network, shall avoid the delivery of duplicate copies of identical communication content and communication related data, but to deliver it as a single / coherent communication product to the Law Enforcement Monitoring Facility. This process should not degrade the quality of the product.

15. Other Assistance

[LEON 15] *Preparing and/or during the lawful access, law enforcement agencies may require information and/or assistance from the communication service providers to ensure that the communications acquired at the lawful access interface are those communications associated with the Subject of Interest's service.*

LEON 15 states the need to ensure the right communication is lawfully accessed. To meet this requirement it is necessary for the communication service provider to determine the permanent identifier for lawful access such as the equipment identifier in a fixed environment or service identifier in the mobile environment. The type of information and/or assistance required will vary according to the accepted practices in individual countries.

[LEON 15.1] *Law enforcement agencies require assistance from service provider to identify a Subject of Interest´s unique technical identifier, which can be used for lawful access.*

LEON 15.1 states the need for communication service providers to support the LEA to make the technical identification possible for example for an observed SoI.

[LEON 15.2] *Law enforcement agencies require assistance from service provider to make an accurate location determination directly by the Law enforcement agencies of a known Subject of Interest possible.*

LEON 15.2 states the need for communication service providers to support, implement and assist with technical solutions to make radio location determination of a SoI with a known identifier possible. For example this need is also present in life rescue situations, like missing people.

Under certain circumstances the communication service provider shall provide a solution to LEAs as an integral part of the communication service provider's network. International state of the art standards shall be used where possible.

Glossary

Communication	Any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system.
Communications Content	Any content of a communication exchanged between the communication partners such as messages, voice, video, pictures, etc.
Communications Related Data	This includes data on addressing, routing, signalling, switching, processing, transmitting, managing of a service, or other information that identifies or assists in the identification of the origin, destination, direction, date, time, duration, termination, or status of each communication generated, processed, transmitted, received controlled or attempted, by a user, service or network. Note: The term communications related data does not include the content of the communication. Note: Location information is a specific form of communication related data and is treated separately in portions of this document with specific requirements.
Communication Service	A service enabling communication between users. Users can be persons or objects like in machine-to-machine services.
Communication Service Provider	An entity providing Communications Service(s).
Home Routing	A functional architecture for providing a communication service to a roaming user while in a visited mobile network where the communication service is mainly processed and handled in the user's home network.
Lawful Access	The statutory-based action of obtaining information on the subject of interest, communications content, communications related data and location information by the law enforcement agency.
Lawful Access Interface	The connection and protocol for handing over of the lawfully accessed communications content, communications related data and location information from the service provider to the law enforcement agency.
Law Enforcement Monitoring Facility	A law enforcement agency facility designated as the destination for the delivery of lawfully accessed information.

Lawful Authorisation	Legal permission granted to a law enforcement agency under certain conditions to lawfully access specified communications. Typically this refers to an order or warrant issued by a legally authorised body.
Quality of Service	The quality specification of a communications connection, system, communications session, etc.. Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.
Reliability	The probability that a system or communication service will perform in a satisfactory manner for a given period of time when used under common specified operating conditions.
Roaming	The ability of subscribers of mobile communications services to communicate when they are located outside their designated home service area/home network.
Subject of Interest (SoI)	Identifier associated with a person or object described in the lawful authorisation from which the communications content, communications related data and location information are to be lawfully accessed.

Abbreviations

3GPP	3rd Generation Partnership Project
ETSI	European Telecommunication Standards
Institute EU	European Union
IUR	International User Requirements
GNSS	Global Navigation Satellite System
LAN	Local Area Network
LEA	Law Enforcement Agency
LEON	Law Enforcement Operational Needs
SoI	Subject of Interest
QoS	Quality of Service

Table of Amendments

Version	Date	Amd No	Description
1.0	9 June 2022		Agreed version 1.0