Introduction

As per 3GPP standards, Lawful Intercept is defined as “laws of individual nations and regional institutions and licensing and operating conditions which define a need to intercept targeted communications traffic and related information in communications systems”. Lawful Interception in 5G networks will be different from past mobile wireless operations because factors like 5G networks are completely overhauled whereby the entire network core will be virtualized, including LI interfaces and capabilities, the sheer scale, transmission rates, and density of user devices as well as new devices themselves such as IoT, cars, video terminals, and embedded systems will present demands on monitoring facilities that are not experienced before. 5G standard bodies are heavily influenced by privacy-driven organizations like the IETF and non-traditional network equipment vendors with strong anti-government surveillance views, which can enable new levels of encryption and privacy.

Lawful Interception is one of the regulatory requirements operators must satisfy as a legal obligation towards the Law Enforcement Agencies (LEA) and Government Authorities in most countries where they are operating their businesses. Within 3GPP standards, it is defined as "laws of individual nations and regional institutions and sometimes licensing and operating conditions, which define a need to intercept targeted communications traffic and related information in communication systems". Lawful interception applies in accordance with applicable national or regional laws and technical regulations. It allows appropriate authorities to perform interception of communication traffic for a specific user(s) and includes activation, deactivation, interrogation, and invocation procedures.

A single user may be involved where interception is being performed by different LEAs. In such scenarios, it must be possible to maintain a strict separation of these interception measures. The LI function does not place requirements on how a system should be built but, rather, requires that provisions be made for legal authorities to be able to get the necessary information.

LI Requirements

- 5G network shall allow legal authorities to get the necessary information from the 5G networks via legal means according to specific security
requirements, without disruption of the normal mode of operations and without jeopardizing the privacy of communications not to be intercepted.

- It allows various authorized authorities to perform interception of communication traffic for a specific user(s), including activation, deactivation, interrogation procedures, etc.
- It must operate without being detected by the person whose information is being intercepted and other unauthorized persons.
- As LI has regional jurisdiction, national regulations may define specific requirements on how to handle the user’s location and an interception across boundaries.

5G Architecture for Lawful Intercept

The Service provider domain consists of 5G-RAN, 5G Core Network, and some additional functions like Administration function (ADMF) and Mediation & Delivery function (MDF), whereas the law enforcement domain includes law enforcement agency (LEA) and Law Enforcement Monitoring Facility (LEMF).

- LEA (Law Enforcement Agency): it is, in general, the one that submits the warrant to the service provider for the users’ interception.
- ADMF (Administration Function): it is responsible for the overall management/control plane of the L1 system. ADMF uses the L1_X1 interface towards the 5GC NFs (Network Functions) for managing the LI functionality.
- MDF (Mediation and Delivery Function): it delivers the interception reports to the Law enforcement monitoring facility.
- LEMF (Law enforcement monitoring facility): it is the entity receiving the interception reports.
- POI (Point of Interest): it is the functionality that detects the target communication, derives the intercept related information or communications.