SCIENTIFIC REVIEW PAPER

UDK: 007:004
Received: June 2020.

NATALIJA PARLOV[*], ŽELJKO SIČAJA[**], TIHOMIR KATULIĆ[***], RIKO LUSA[****]

Information security and the lawful interception of communications through telecom service providers infrastructure: advanced model system architecture

Abstract

Communication interception for national security purposes, as well as for purposes of conducting a criminal investigation, is an invaluable asset of law enforcement agencies. In technical terms, this field has seen rapid advances in the last decade, while available software programmes and platforms for lawful interception (LI) are now able to monitor a broad spectrum of communication channels. Lawful interception of communications invariably intersects with fundamental rights and freedoms of persons in the European Union and the Member States. The purpose of this paper, as part of the discussion on the framework of lawful interception, is to present a study of advanced lawful interception software with its functionalities and processes, compare it with the most common lawful interception models and analyse the software architecture defined by the European Telecommunications Standards Institute (ETSI) as a general standard. While this particular model of LI architecture has initially been designed to intercept voice communications, it can be successfully applied to intercept communications over Internet Protocol (IP) channels. Finally, the paper offers a comparative insight into different kinds of LI software and their capabilities in line with communication interception regulation.

Keywords: *lawful interception, LI, telecom service providers, information security, cybersecurity, national security*

[*] Natalija Parlov, M.A. APICURA & TÜV NORD, Zagreb; University of Zadar, Zadar, Croatia

[**] Željko Sičaja, M.A. APICURA & TÜV NORD, Zagreb; University of Zadar, Zadar, Croatia

[***] Tihomir Katulić, Assistant professor, LL.M., Ph.D. University of Zagreb, Faculty of Law, Zagreb, Croatia

[****] Riko Luša, M.Sc.EE. SedamIT, Zagreb; University of Zagreb, Faculty of Electrical Engineering and Computing, Zagreb, Croatia

1. OVERVIEW OF LAWFUL INTERCEPTION OF TELECOMMUNICATION SERVICES

Lawful interception (LI) is a process of collecting information from the communication network for criminal investigation purposes by law enforcement authority (LEA). It is impossible to imagine life today without communication services such as phone calls, instant messaging, or e-mails. The same services can, as such, be abused for criminal or terrorist activities. This exploitation can take different forms, such as exchanging e-mail, voice or SMS communications between criminal parties for organising illegal drug traffic, human trafficking, terrorist acts, etc. Voice over IP (VoIP) and instant messaging applications could also carry traffic susceptible to interception and should be analysed under a lawful interception process using any legal, technological possibilities to identify the investigative value to the authorities during a criminal investigation.

When dealing with digitalisation and software/platform requirements, information security systems are the main key in planning and management to provide for the integrity, availability and confidentiality of information (Ermana & Tanuwijaya, 2012). The development of information and communication technology has created a significant leap in improving business efficiency and accuracy and increasing its productivity. Moreover, IT assets – such as data, networks, hardware, and software – are now considered one of the resources and essential operators of successful business organisations in the twenty-first century (Itrada et al., 2014; Samota & Patel, 2017). The first step to achieve this is self-assessment of the reality of information security, known as gap-measurement (Al-Mayahi & Mansoor, 2012; Candiwan, 2014).

The process of gathering and evaluating information is increasingly susceptible to external influences and manipulations via information operations of state and non-state actors, particularly with the development of information technologies (Dokman & Malnar, 2019). Dynamic changes that characterise the modern security environment have been significantly driven and shaped by the rapid pace of technological development; its significant importance is found in the emergence and development of disruptive technologies that are changing the character of the security environment (Malnar & Olujić, 2019). With operating controls implemented, the system's technical controls should include logical access controls, such as identification, authentication, authorisation, accountability (including audit trails), cryptography, and the classification of assets and users (Whitman & Mattford, 2018). Information security systems are of great importance for business organisations as they become the primary key for planning and management in modern enterprises to ensure the safety, availability and confidentiality of information (Ermana & Tanuwijaya, 2012). Evaluating the information security compliance level in organisations with internationally recognised standards is growing in importance because it has become popular as a common basis for information security measurement (Ifinedo, 2014).

Keeping that in mind, strategic IT systems, such as advanced LI models, have to ensure compliance with comprehensive national legislation. Moreover, they must be built according to the industry best practices and security frameworks to ensure they fit into telecommunication information systems governance (e.g. ITU-T X.1051 series, ISO 27011 series). The new generation LI systems are built to fit into the proposed methodology goals for supporting infrastructure, utilising and managing resources most effectively, applying security policies, access control, and other security objectives. These systems are created in line with the European Technical Standards Institute (ETSI) standards for LI, making them compatible with existing infrastructure and ensuring future interoperability.

2. METHODOLOGY

Methodologies used in this paper are descriptive analysis, comparative analysis, macrostructural analysis and case study.

3. THE LEGAL FRAMEWORK IN CROATIA

In their struggle to prevent crime and especially acts of terrorism, law enforcement agencies (LEA) give great importance to their ability to catch and isolate related network traffic. Authorised interception of electronic communication is an essential tool for protecting national interests, especially national security and investigating serious crimes. In the Croatian legal system, the Electronic Communications Act (ECA) regulates the rights and obligations of operators of public communication networks.

The ECA provides the general framework of obligations for the public communication network operators concerning the facilitation of secret surveillance of electronic communications networks and services. Primarily, the Act demands that these operators ensure, finance and organise the function of secret surveillance of electronic communications networks and services as well as electronic communications lines to the operational and technical body competent for the surveillance of electronic communications under a special law regulating the field of national security (Article 108 of the ECA). This body also regulates the measures and standards of information security warranted by the ECA provisions for ensuring the function of secret surveillance of electronic communications networks and services.

The ECA also regulates that the obligations of operators of public communications networks and publicly available electronic communications services towards the competent body and other institutions and bodies authorised to perform secret surveillance of communications networks and services are regulated by laws regulating the legal framework of the system of national security and the Criminal Procedure Code. These provisions also limit individuals' rights and freedoms with regard to personal data protection rights in electronic communications.

Articles 109 and 110 define the obligations the operators of public communications networks and publicly available electronic communications have in retaining electronic communications data to enable conducting of the investigation, discovery and criminal prosecution of criminal offences.

Article 110 defines the categories of retained data, such as the data necessary to trace and identify the source of communication, data necessary to identify the destination of the communication, data necessary to identify the date, time and duration of communication, data necessary to identify the type of communication, data necessary to identify users' communication equipment or what purports to be their equipment and the data necessary to identify the location of mobile communication equipment. The operators must also retain data relating to unsuccessful call attempts, whereby there is no obligation to retain data relating to unconnected calls. Article 110 also prohibits the retention of data by operators that may reveal the contents of the communication.

Article 339 of the Criminal Procedure Code regulates the procedure of enabling surveillance of electronic communications from the operators of public communications

networks and publicly available electronic communications in cases when there is reason to suspect that the owner or the user of electronic communication equipment has committed a criminal act punishable by imprisonment of five or more years.

Further clarification of the position and roles of the operational and technical body are regulated by Article 18 of the Security and Intelligence System Act. It defines the establishment of the Operational and Technical Centre for Telecommunications Surveillance (OTC) for activating and managing the measures of secret surveillance of telecommunications services, activities and traffic.

Additionally, the purpose of the OTC is to enable the operational-technical coordination between legal and natural persons operating public telecommunication networks and providing public telecommunications services and access services in the Republic of Croatia, and the bodies authorised to apply the measures of secret surveillance of telecommunications pursuant to the relevant Croatian legal framework.

The OTC is authorised to supervise the work of telecommunications service providers in the fulfilment of the obligations these providers have according to applicable laws and to enable security and intelligence agencies and monitoring bodies to conduct the activation and management of the measures of secret surveillance of telecommunications services, activities and traffic employing appropriate technical interface.

The information and data collected through a lawful interception are very useful to law enforcement agencies for criminal prosecutions or for protecting national security. According to Kopal (2001), the most commonly used criminal analytics techniques are crime analysis, investigative analysis, operations analysis and intelligence analysis. Thanks to careful analysis, it has been possible to reconstruct relationships between the members of organised crime, highlighting the roles they hold and the strategies used for territorial control (Frazzica, 2016).

The most important state subsystems with the highest level of direct liability for the implementation of national security and national interests are the foreign policy subsystem, intelligence subsystem, military subsystem and economic subsystem. Therefore, the instruments for the implementation of national security and national interests from each of these areas require particular attention. (Tatalović and Bilandžić, 2005, p. 74-75; Tatalović, 2011). The national security system implies a synthesis of all subsystems in society. Although it is common ground, it needs to be emphasised that not all subsystems share the same liability for implementing national security and national interests. (Maljak, Parlov and Sičaja, 2017).

Provisions such as these attest that in the modern legal framework, the interception of traditional telephone calls is well regulated by laws and procedures in most countries, supplemented by network components that participate in signalling and carrying traffic within a telecom network. The providers of telecommunication services are legally required (e.g. in the EU Member States as defined by Council Resolution, 1996) to assist LEAs in their endeavours by enabling electronic interfaces to monitor the traffic of individual subscribers. In this example, each EU Member State applies the requirements to their national laws and in line with national policies.

Essentially, these requirements define that LEAs have access to the communication information of the interception subject, being either a person or persons specified in a lawful authorisation, whose telecommunications are to be intercepted. This information can be entire

communication transmitted to or from the telephone number or any service identifier that the subject uses and call-associated data generated to process the call.

Other collected information, as stated in the referenced document, are all call signalling, including signalling emitted by the subject, called party number of outgoing connections, calling party number for incoming connections, the timestamp of connection beginning, end and duration, actual destination and geographic location information for mobile subscribers. Moreover, security requirements are being implemented to satisfy the interception order, like the design and implementation of safeguards to prevent misuse or improper use and safeguard classified information about how many interceptions have been performed and how they are carried out.

These requirements also give rise to challenges for the network operators (NWO) or service providers (SP) related to compliance, delivery, extraction, safety and cost.

4. CHALLENGES

The SPs are challenged continuously to comply with the requirement as their network is continually evolving. We have seen the change from traditional public switched telephone networks with related signalling such as SS7 to IP Multimedia Services (IMS) based on Session Initiation Protocol (SIP). Besides, internet access is seeing upgrades in technologies and access speeds with current capabilities, as shown in Table 1 and reported by the European Court of Auditors (2018) for broadband access networks depicted in Figure 1. In 2019 we saw the introduction of 5G Mobile access technologies implementation, increasing the download and upload speeds of mobile subscribers even further. The said will pose a challenge on both the SP and LEA on how to cope with the substantial increase of the subscriber traffic and ensure reliable intercepted data delivery.

Voice delivery has not changed much over the years. Still, constant change in network architecture, services and the development of new voice codecs, such as Enhanced Voice Services (EVS) codec, make voice delivery challenging on the latest network architectures for both operator and LEAs. Exploring different codecs used in telecommunications networks is not within the scope of this paper. It is, however, necessary to note that LEAs capability to decode the receiving data should also evolve in line with the technology or should utilise tools that will help them overcome these obstacles.

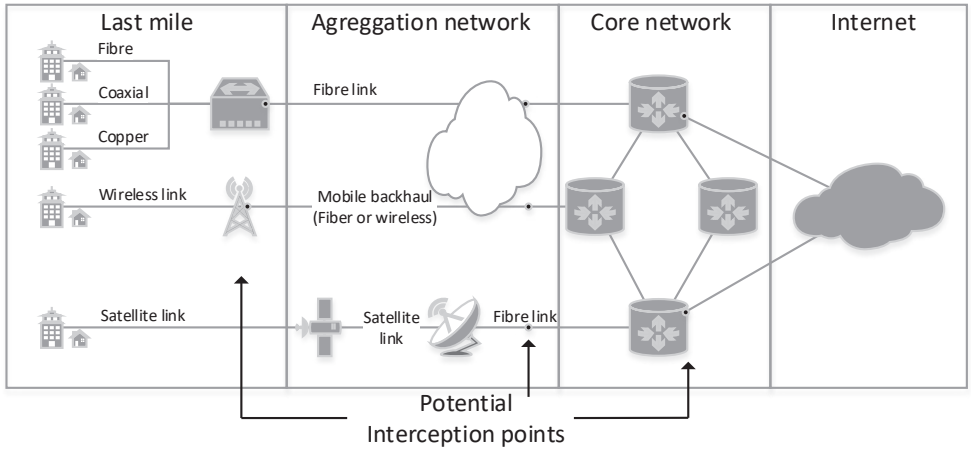
Table 1: Broadband infrastructure types and current commercial technology

Wired or wireless	Infrastructure	Indicative download speed	Indicative upload speed
Wired	Fibre	Up to 2.5 Gbps	Up to 1.2 Gbps
	Coaxial cable	300 Mbps up to 2 Gbps	Up to 50 Mbps
	Copper phone	5 Mbps up to 100 Mbps	Up to 10 Mbps
Wireless	Terrestrial wireless	60 Mbps	Up to 10 Mbps
	Satellite	Up to 20 Mbps	Up to 8 Mbps

Source: European Court of Auditors, 2018 [20]

The second challenge is extracting the data belonging to the target and ensuring that no other traffic belonging to non-targets is delivered. This task is made more complex as the SP network architecture is evolving into a structure that consists of a mix of technologies supporting the SPs evolution of provided services and accommodating new ones. The best example are MNOs with 2G, 3G, 4G access technologies of varying mix getting ready for the 5G introduction. In complex architectures, such as the ones depicted in Figure 3, the SP must ensure that intercepted data delivered to LEA is neither missing any communication data from the target nor including any of the non-targeted data, thus complying with data privacy laws.

Figure 1: Segments of a broadband access network



Source: Author's work, 2020

Compliance with the lawful interception requirements is a must for the SPs. Still, they must also ensure the safety of the intercepted data and that it is undetectable by the target in any communication scenario or that it does not interfere with its subscribers' services. In a continually evolving network environment, this is a serious challenge. The SPs are struggling to provide new services to their subscribers with minimum time to market and certify that they are tested for compliance, extending interception facilities. Auditing capabilities and network logging are thus important to ensure the data security and integrity are always maintained.

In order to be able to comply with these requirements, service providers are required to provide interfaces through which interception communication can be transmitted to a law enforcement monitoring facility (LEMF) in real-time. These interfaces are agreed upon between LEA and the SP, and so is the format of delivering communication data. Failure to maintain compliance would make operators susceptible to severe repercussions.

For this purpose, service providers install interception facilities to fulfil obligations defined by national laws and regulations, addressing the challenges stated above, and specialised vendors usually provide these facilities. Since laws and regulations define which subscribers are susceptible to lawful interception, there is a strict procedure on ensuring that the systems are not being misused. Technical requirements for lawful interception are defined by standards through standardisation bodies such as ETSI (European Telecommunication

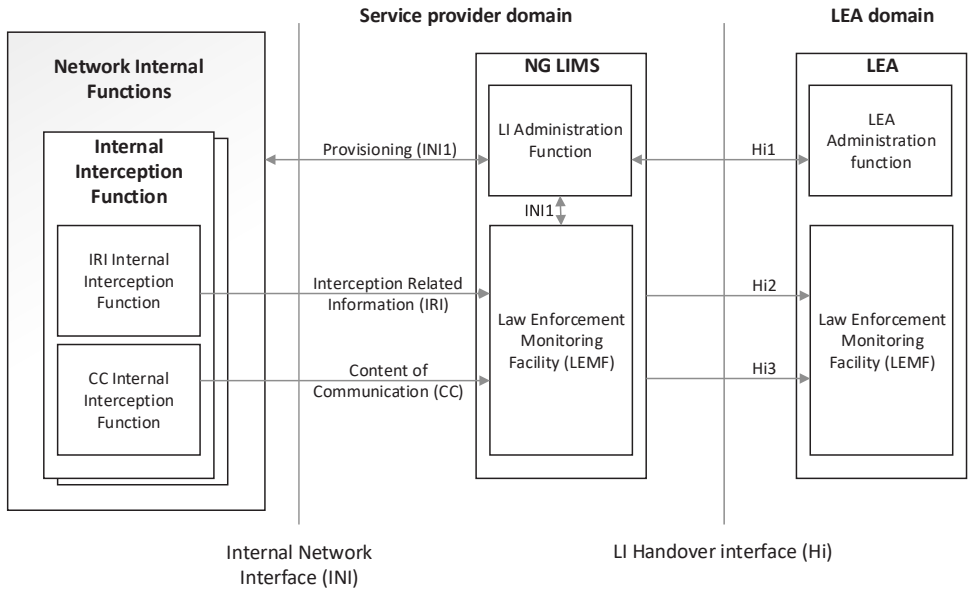
Standards Institute), 3GPP (3G Partnership Project) and others, ensuring maximum compatibility between different functional elements involved in the process of lawful interception. Interception facilities at the SPs should also have no impact on the performance and integrity of customer traffic. That is one of the major requirements that the SPs expect from providers of such solutions.

This case study will present the architecture for lawful interception and how mobile service providers face the above-referenced challenges referenced. The law and regulation of lawful interception are outside the scope of this paper. We will discuss potential solutions to operator challenges in more detail, referencing the next-generation lawful interception (NGLI) system Matison LIMS using the use case of implementing interception of communications in mobile networks.

5. ETSI ARCHITECTURE FOR LAWFUL INTERCEPTION

Lawful Interception Mediation system (LIMS) architecture is based on the reference model from ETSI and 3GPP standards and recommendations, using the same structure of modules and required interconnection interfaces. The same architecture is developed to conform to scalability for network growth in complexity and throughput while supporting all types of access technologies, circuit and packet networks, and enabling new technologies. The ETSI organisation proposed a basic reference model (ETSI TS 101 671 V3.14.1, 2016), and it is shown in Figure 2. The implementation of specific internal functions is described in ETSI TS 101 158 V1.3.1 (2014).

Figure 2: ETSI Reference model for lawful interception



Source: Authors' work, 2020

This reference model enables the use of specific mediation systems to help LEAs monitor traffic from different applications using preferred interception analysis tools and reduce dependency on network technology.

In recent 15 years, traditional telephone communication networks were being gradually supplemented and, in certain cases, replaced by modern technology running over internet protocol (IP). What is more important is that traditional communication services are replaced by IP based services such as VoIP and RCS, and data traffic has already gained large momentum. We see these changes in relation to lawful interception reflected in new lawful interception implementations on intercepted data delivery (ETSI TS 102 232-1 V3.1.1, 2012).

In this architecture, communication to the network operator or the SP is maintained through handover interfaces (Hi). More specifically, handover interface 1 (Hi1) is used for provision interception order through the administration function. Handover interface 2 (Hi2) supports the delivery of Intercept Related Information (IRI) to LEA, such as the destination of a call, duration of a call, source of a call etc. Handover interface 3 (Hi3) carries the call Content of Communication (CC) from the network to LEA.

As depicted, the core element of the interception system is the Lawful Interception Mediation Function, which is used for:

- the collection of intercepted data from a network element such as soft switches, routers, probes,
- encoding this data into a data stream that LEMF can understand,
- the correlation and delivery of the data to one or more LEAs,
- managing security and authorisation,
- the protection of the data against unauthorised access or modification and
- logging function for auditing purposes.

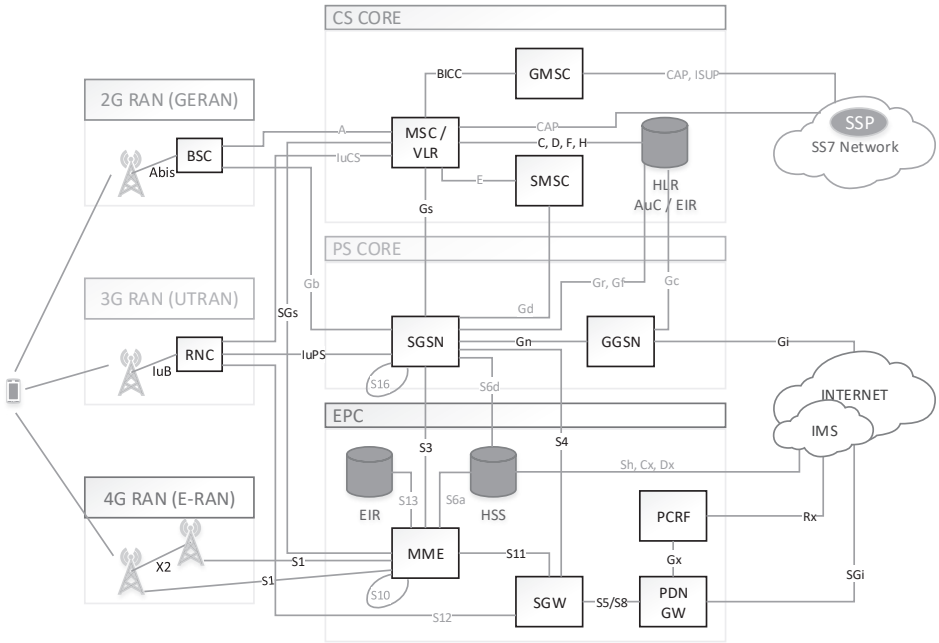
Through this mediation, the Network operators/Service providers (NWO/SP) could deliver voice, internet access, e-mail, Short Messaging Service (SMS)/Multimedia Messaging Service (MMS), Rich Communication Service (RCS) on any fixed or mobile access technology.

6. IMPLEMENTATION IN MOBILE SERVICE PROVIDERS AND ADVANCED MODEL CASE STUDY

A typical mobile network operator (MNO) is usually a service provider and an access network provider (AP). It provides services to subscribers like e-mail, VoIP, etc., through wireless technology like 3G or 4G. The following Figure 3 shows the most common architecture that these mobile NWO/SPs have implemented to provide voice and internet access, along with other services.

In section 4, we have listed the challenges the NWO/SPs face in fulfilling government requirements for lawful interception, but additional ones complicate lawful interception compliance.

Figure 3: Mobile network with 2G, 3G and 4G access technologies



Source: Authors' work, 2020

Throughput is continuously increasing, driven by the proliferation of streaming services. Mobile operators are thus constantly adapting their network, providing additional network elements and interconnecting links. These streaming services usually do not bring additional value to LEA, and it may be required to drop this traffic as it can saturate delivery.

It is not uncommon that a network consists of multi-vendor equipment, and such an environment might prove challenging for the delivery of the intercepted data. These different elements have to be connected to an interception mediation function, and operators must ensure that whenever there is a change in those elements, such as updating or upgrading, it will not affect the interception.

As depicted in Figure 3, each access technology utilises specialised network functions, and deploying new technology such as 5G will bring additional elements into operation like Access and Mobility Management Function (AMF) and Session Management Function (SMF) (5GPPP Architecture Working Group, 2019). Mobile operators are required to ensure the delivery of intercepted data for these technologies before it is placed into commercial operation, even though such rising network complexity is a challenge in itself. The same goes for introducing subscriber services through the implementation of IMS (3GPP TS 22.228, 2015) and VoLTE (GSMA IR.92, 2015).

Introducing a lawful interception solution for mobile operators, such as Matison LIMS (Matison, 2018), will help overcome these challenges. Essential for compliance with the regulation, these systems do not bring commercial value for mobile operators while still facing

the necessary issue of operating, administrating and maintaining such systems. It should be noted that due to these challenges, operators have to consider interception systems that would reduce their operating cost while also providing faster adaption to their changing network environment, ensuring full compliance with LI regulation.

6.1. The process of lawful interception

In the process of interception, national law describes which conditions and restrictions will be employed before interception is allowed. If LEA considers interception as a tool for help in investigating serious crime, LEA will ask the prosecuting judge or responsible body to authorise the use of interception. If this is granted, LEA will present authorisation to the NWO/SP through the administration interface Hi1 or procedure. After this process is authorised, IRI and CC are delivered to the LEMF.

Mobile operator may receive multiple lawful authorisations that will depend on subscribed services used by the interception subject. In addition, a single interception subject may be requested for interception by different LEAs for different investigations. The LIMS system should be able to separate these investigations and LEAs if required, and each of these investigations may contain various constraints on IRI and CC.

While providing the administration of interception and delivery of IRI and CC, mobile operators should ensure security and authenticate LEAs in their attempt to gain interception data. Two-way authentication is also used to ensure that data is coming from the NWO/SP specified in the lawful authorisation. The NWO/SP should also assure data integrity and confidentiality, so the data is not modified or intercepted by a third party.

6.2. Implementing LIMS into the mobile operator network

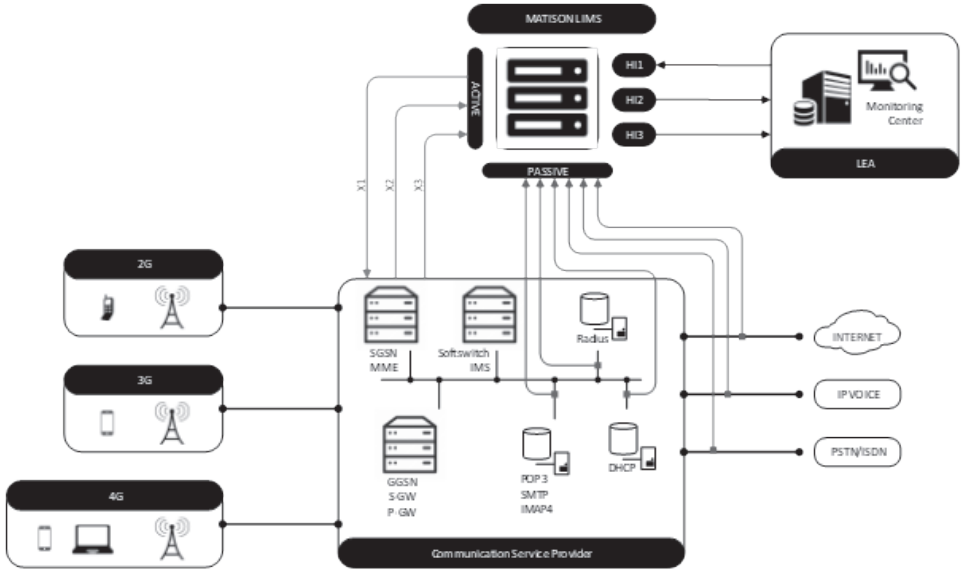
Figure 4 shows a generic implementation of a LIMS system inside a mobile operator network. There are typically two methods of how interception is being performed, depending on the capabilities of the NWO/SP and other factors. These methods are shown in the following sections and consists of either Internal Interception Function (IIF) or External Interception Function (EIF).

IIF enables LEA to directly receive IRI and CC from application servers through a mediation system and is the most straightforward way of receiving interception data. The advantage of this method is that it uses fewer points from which the target traffic data is extracted and delivered. The disadvantage is that it relies on the NWO infrastructure's capabilities and may provide bottlenecks or inadequate functionalities to support all interception requirements, as shown in Table 4, section 6.4. To be able to use IIF, network and application systems have to support secure data paths to a mediation platform.

On the other hand, EIF provides handling of intercepts on various scenarios where IIF cannot be used. For example, this is the case when network elements or application servers do not support LI implementations either due to the large volume of traffic or inherently by design, and modification of such systems to accommodate delivery and security mechanisms

required by LI cannot be provided. Depending on the deployed LIMS, the interception of the target under surveillance in such cases can be performed even on the highest capacity links. We will show in section 6.4 how the system can scale for some typical number of interceptions and what advantages the utilisation of next-generation LI systems can bring.

Figure 4: Matison LIMS in the mobile service provider



Source: Matison, 2020

One of the most common services that do not support IIF is the e-mail service. E-mail servers are not designed to deliver targeted IRI and content through specialised ports dedicated to secure interception transmission. Besides, it is not possible to guarantee that intercepted data will not be detected, as there are no mechanisms in place to assure that requirement. In this case, EIF is used, and passive interception is implemented (see Figure 4).

A typical implementation will consist of a taping device to duplicate the traffic and a probe to extract the required traffic coming to or going from the target. This device will utilise a mediation system to deliver IRI and CC to LEA. In the next generation LI system, it will be possible to control the probe and format CC according to any LEA requirements while ensuring the full security and integrity of data.

In case of lawful interception of mobile services running on 2G, 3G and 4G, implementation consists of active participation of the mediation system with network infrastructure using special interfaces called X1, X2 and X3. X1 is used by the Administration Function (ADMF) to send LI management commands to network elements. Network elements use X2 and X3 interfaces to send intercepted data structured as IRI and CC toward the mediation function, as shown in Figure 4. This intercepted data sent over X2 and X3 will be ultimately sent toward LEA through the handover interface Hi2 and Hi3, as shown in section 5.

The ETSI reference architecture is built to allow for service separation that the next-generation LI systems can utilise for scalability purposes.

6.3. Voice services

Intercepting voice services in mobile networks will require a mediation system to connect to switching servers and gateways, such as MSC-S, G-MSC-S, and MGW for legacy networks. Operators that have implemented IMS will need to interface mediation system with Call/Session Control Function (CSCF), Application Server (AS) and gateway to intercept IRI and CC from services such as Voice over LTE (VoLTE).

An alternative would be to use a passive solution and duplicate signalling and exchange call content at the central point in this architecture.

6.4. Data services

Both active and passive interception scenarios are available for intercepting data services, wherein the active scenario mediation system will connect with SGSN, MME and SGW/PGW, respectively. In order to use the passive solution, traffic duplication will be needed around SGW/PGW, where the probe will monitor and extract communication data from targets and deliver them to the mediation.

Other elements might also be interfaced depending on the implemented network services. For instance, e.g. if Wi-Fi is implemented, Packet Data Gateway (PDG) would be connected to a mediation system for traffic collection, and AAA server correlates data such as IP address and user identity.

The advantages of the next-generation LI system will be shown with the example of Matison LIMS as a representative of such systems. As noted in the sections above, the next-generation LI systems would utilise the reference LI architecture to build a distributed, scalable system capable of meeting today's demands from the NWO/SPs.

One of the major requirements was to make sure the NWO/SP could utilise existing hardware suppliers, which provide cost savings in the long term by reducing OPEX. Efficiency in operation comes from the service scalability, as it will enable pay as you grow a model that follows the NWO/SP network growth.

Legacy LI systems typically have a linear increase of cost as the NWO/SP grows, as shown in Figure 6. The main reason is that new LI systems will be deployed for each new service and expand the existing ones. By scaling with services, the next-generation LI systems will utilise their advanced architecture to optimally scale only functional parts that are needed, thus lowering the total cost of ownership (TCO) for the NWO/SPs.

An example is provided in Table 3. Voice packet sizes for typical implementations are stated in the following table (CISCO, 2016). For the sake of simplicity, we are referencing the G.729 codec. Standard VoLTE implementations will utilise more advanced codecs such as AMR or EVS.

Table 2: Voice over IP - bandwidth consumption per call

Codec Information				Bandwidth Calculations			
Codec & Bit Rate (Kbps)	**Codec Sample Size (Bytes)**	**Codec Sample Interval (ms)**	**Mean Opinion Score (MOS)**	**Voice Payload Size (Bytes)**	**Voice Payload Size (ms)**	**Packets Per Second (PPS)**	**Bandwidth Ethernet (Kbps)**
G.711 (64 Kbps)	80 Bytes	10 ms	4,1	160 Bytes	20 ms	50	87.2 Kbps
G.729 (8 Kbps)	10 Bytes	10 ms	3,92	20 Bytes	20 ms	50	31.2 Kbps
G.723.1 (6.3 Kbps)	24 Bytes	30 ms	3.9	24 Bytes	30 ms	33.3	21.9 Kbps
G.723.1 (5.3 Kbps)	20 Bytes	30 ms	3.8	20 Bytes	30 ms	33.3	20.8 Kbps

Source: CISCO, 2016 [10]

For example, the total bandwidth required for a G.729 call for a default 20 bytes payload can be calculated using the formula:

$$Bandwidth\ per\ call = \frac{voice\ packet\ size}{packets\ per\ second} \quad (1)$$

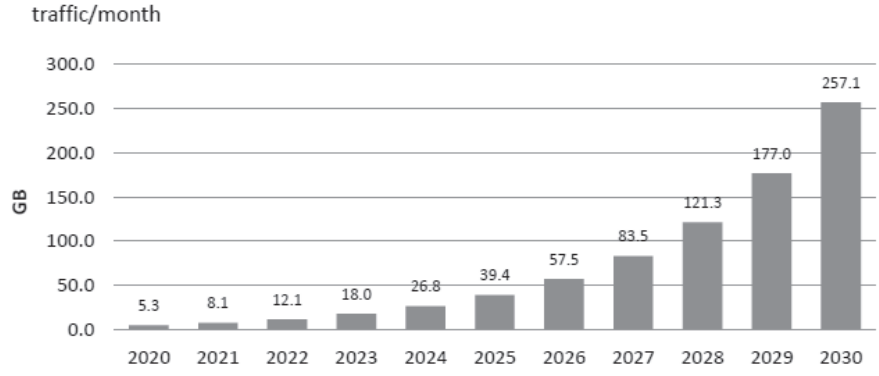
Where voice packet size and packets per second can be calculated as in the following:

$$voice\ packet\ size = (Eth\ header + IP/UDP/RTP\ header + payload) * 8bits \quad (2)$$

$$packets\ per\ second = \frac{codec\ bitrate}{payload} \quad (3)$$

For interception, along with voice traffic, average data rates per subscriber need to be included. For the EU, we can use average data consumption in 2020 per subscriber estimates (ITU-R M.2370-0, 2015) to calculate the required throughput needed for data interception.

Figure 5: Estimation of global mobile traffic per subscriber



Source: ITU-R, 2015 [22]

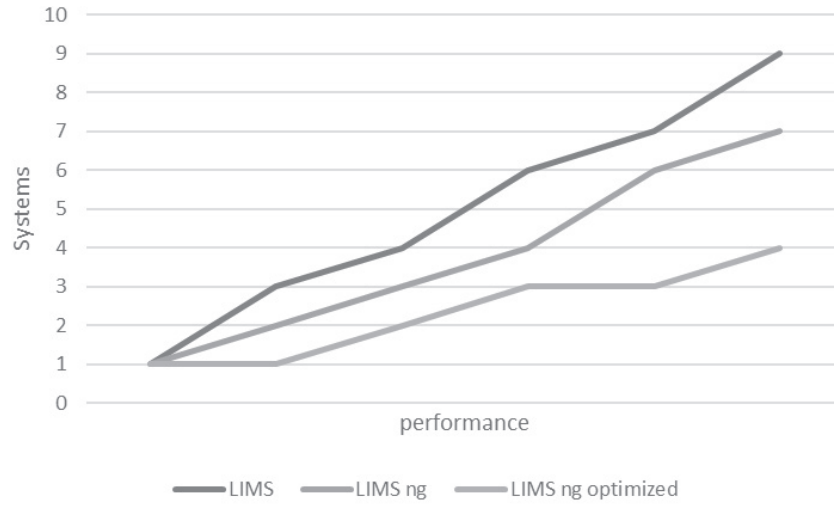
Table 3: Throughput required for target interceptions

Target interceptions	Voice (Mb/s)	Data (Mb/s)	Total (Mb/s)
1000	31.20	1,400.16	1,431.36
2000	62.40	2,800.32	2,862.72
3000	93.60	4,200.48	4,294.08
4000	124.80	5,600.64	5,725.44
5000	156.00	7,000.80	7,156.80
6000	187.20	8,400.95	8,588.15

Source: Authors' work, 2020

Figure 6 also shows how advanced filtering utilised in the next-generation LI systems can provide optimisations in a number of deployed LI mediations in the NWO/SP network, directly proportional to CAPEX and OPEX savings. For reference, we are using standard delivery mechanisms to LEA without irrelevant traffic drop that can provide even more benefits and 1G IP links are used for delivery. On standard commercial of the shelf (COTS) hardware, a direct impact on performance by 16% in a direct node vs node performance can be observed. However, if looking at the network level, with all intercepted services, we can observe up to 50% savings in the total cost of ownership (TCO).

Figure 6: Cost comparison of legacy vs the next-gen LI



Source: Authors' work, 2020

Table 4: Comparative table of LI systems

Description	**Next-generation LI**	**Legacy LI**
Active or Passive interception	Both	Separate systems
Converged LI system for fixed and mobile	Yes	No
Passive LI Probe throughput	Up to 100 G	Up to 10 G 100 G with External system
Legacy voice and IMS voice	Yes	Separate system
Mobile 2G, 3G, 4G support	Same system	Separate system
New access types (e.g. 5G)	Supported	Separate system
Fixed Broadband access	Any technology	Any technology, but usually separate systems
COTS HW	Yes	Yes for LIMS, No for probe
Secured access	Supported	Supported
Mediation of X3 /Hi3 interface	Supported	Not supported
Centralised target management	Yes	No
Advanced codec support	Yes	No
High Availability	Yes	Yes
Abstraction layer in collection and delivery	Yes	No
Advanced logging capability	Yes	No
Whitelisting	Yes	Yes
Statistics	Yes	Yes

Source: Authors' work, 2020

Table 4 shows a comparison of the next-generation LI system with legacy LI. Flexible architecture, the main advantage of such systems, provides different benefits to the NWO/SP. One of the major ones is cost-benefit. By utilising modular architecture and support of all major network types, operators take advantage of the service based optimisations and scalability of the platform. Scaling the system to accommodate growth in data throughput, the number of network elements, the number of targets, and simultaneous interception targets will enable operators to have direct and indirect benefits, such as utilising less infrastructure and simplifying operation and maintenance.

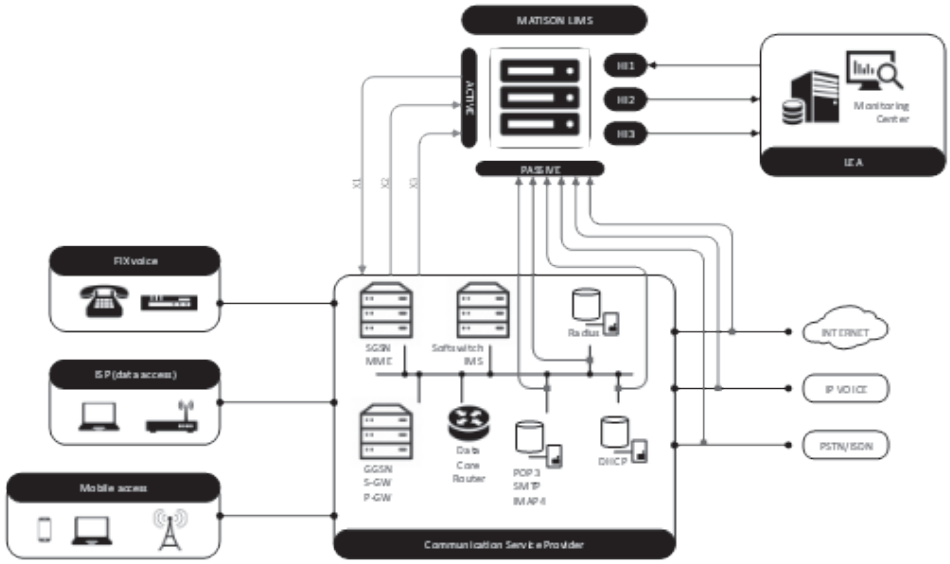
With advanced features such as X3/Hi3 mediation, codec support, layered collection and delivery abstraction, there is no interference with the SP network, and LEAs can reliably receive the intercepted data.

As a representative of the next-generation LI systems, Matison, through its Matison LIMS system, enables the telecommunication service providers (SP) compliance with regulatory requirements and the automatisation of operative tasks related to lawful interception (LI). With this approach, Matison LI is built to ensure a cost-effective interception solution for network deployments of varying complexity.

The Matison LIMS architecture is shown in and allows Matison LI to be utilised in any mobile, fixed, cable or internet service provider network scenario without compromising subscriber services' performance or reliability. It handles voice, fax, SMS, MMS, e-mail, voicemail, RCS, and internet access on a single platform. It addresses the growing need to support emerging services and access technologies such as 5G. Its service scalability and modular architecture ensure extension and adaptability to new services, technology, or changes in national legislation and regulatory requirements.

By utilising this system, interception is performed in real-time and enhances operational capabilities of intelligence organisations through non-intrusive all-software technology that easily integrates into any operator network and enables gathering and the analysis of evidence during criminal investigations.

Figure 7: Matison LIMS



Source: Matison, 2020

Using the next-generation LI system provides benefits over standard LI systems that span several categories and can be compared in Table 4.

The Administration and Mediation Functions are logical components of Matison LIMS in charge of target handling processes, configuration, auditing and data consistency checking. It receives target information over the HI1 interface. Two types of communication interfaces are available for setting the target: over REST API or on the Matison LIMS GUI (Web Portal for Administration). Target information is forwarded to NE or Probe and Mediation Function for correlation over the X1 interface. For elements where target ID changes (e.g. DHCP/ Radius server map MAC address/username to target ID), additional actions are triggered to update that mapping.

Besides, Mattison LI employs user management and role-based security, where system-wide policy is defined together with secure logging. It is imperative to have highly controlled, secure access to the system, and this was built to enable clearance access to every part of the system.

To scale with the NWO network, the administration function can take the form of a separate system. The said will enable additional functionalities required by the NWO/SP, such as LI consolidation.

7. CONCLUSION

As information technology, in general, continues to rapidly change and advance, the same goes for electronic communications. As we have witnessed over the last two decades, the case of mobile network technology proves this by generations of this technology being introduced in less time than it took to establish the previous.

The availability of mobile connectivity, especially internet access, has allowed for the proliferation of new communication services. For these services, operators are also obliged towards their users to keep their data and communication secure, and these days, almost universally, providers of these services have to conform to national or international legislation to secure and encrypt communication and data.

Prediction of future data usage shows an exponential increase. With improvements to communication technology, encryption of communication channels is applying the latest cryptography developments to enable widespread and efficient end-to-end encryption. The technology used in modern LI systems is advancing in the same significant leaps, adapting to avoid the obstacles imposed by new services and law enforcement organisations have to follow the dynamics of the market.

National security faces critical challenges now more than ever as the digital service market is booming and a multitude of new communication services spring up all over cyberspace. Both LEAs and NWO/SPs have an essential role in the process of ensuring that threats are discovered, localised and adequately processed. Telecom operators are obliged to conform to local legislation. While modern privacy legislation does significantly improve the position of individuals concerning their rights and freedoms, this development might impede business opportunities and prevent service providers from offering new services to their customers. LEAs decide what information are required to perform their duties, and their ability to decode the information might be impeded by advancing technology in communication services. The improvement in the chain of lawful interception from both angles will ensure that the NWO/SPs deploy new services faster, without interference in the process of LI. Hence, LEAs will be able to inspect the information received and will not limit NWO/SP capabilities.

There are new solutions on the market built to withstand the changes in communication technology through new architectural design and to adapt to new services and access technologies. Both LEAs and NWO/SPs should rethink their current strategies and see new solutions to ensure compatibility with future services and technology and enable flexibility in operative tasks of performing interceptions.

REFERENCES

1. 3GPP TS 22.228. (2015). Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS), Stage 1. 3GPP.
2. 5GPPP Architecture Working Group. (2019). View on 5G Architecture, White Paper. 5GPPP, 65-67.
3. Al-Mayahi, I., Mansoor, S. (2012). ISO 27001gap analysis – case study, *presented at the 2012 International Conference on Security and Management (SAM '12)*, Las Vegas, 2012.
4. Candiwan, C. (2014). Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia, *In Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014)*, pp. 50-58
5. CISCO. (13 April 2016). Voice Over IP - Per Call Bandwidth Consumption. Retrieved from Cisco: https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/7934-bwidth-consume.html. Accessed 3 March 2020.
6. Council Resolution. (1996). On the lawful interception of telecommunications, 96/C 329/01. *Official Journal of the European Communities*.
7. Criminal Procedure Act. (2008). *Official Gazette of the Republic of Croatia*, 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19, 126/19. Accessed 7 March 2020.
8. Dokman, T., Malnar, D. (2019). Conceptualisation of Information Operations in Modelling the Understanding of a Security Environment. *Annals of Disaster Risk Sciences*, 2(1-2). Retrieved from https://ojs.vvg.hr/index.php/adrs/article/view/20.
9. Electronic Communications Act. (2008). *Official Gazette of the Republic of Croatia*, 73/08, 90/11, 133/12, 80/13, 71/14, 72/17.
10. Ermana, F. H., Tanuwijaya, M. I. (2012). Security audit information system based on the ISO 27001 Standards, *PT. BPR Jatim (STIKOM)*, Surabaya
11. Ermana, F. H., Tanuwijaya, M. I. (2012). Security audit information system based on the ISO 27001 Standards, *PT. BPR Jatim* (STIKOM), Surabaya.
12. ETSI TS 101 158 V1.3.1. (2014). *Telecommunications security; Lawful Interception (LI); Requirements for network functions.* ETSI.
13. ETSI TS 101 671 V3.14.1. (2016). *Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic.* ETSI.
14. ETSI TS 102 232-1 V3.1.1. (2012). *Lawful Interception (LI); Handover interface and Service-Specific details (SSD) for IP delivery*; Part 1: Handover specification for IP delivery. ETSI.
15. ETSI TS 102 232-3 V3.5.1. (2017). *Lawful Interception (LI; Handover Interface and Service-Specific Details (SSD) for IP delivery*; Part 3: Service-specific details for internet access services. ETSI.
16. European Court of Auditors. (2018). Broadband in the EU Member States: despite progress, not all the Europe 2020 targets will be met. Special Report, No. 12, p. 11.
17. Frazzica, G. (2016). Proposal for a computer-assisted analysis of lawful interceptions of communication, *Global Crime*, 17:1, 79-98, DOI: 10.1080/17440572.2015.1114920
18. GSMA IR.92. (2015). IR.92 - IMS Profile for Voice and SMS v9. GSMA.
19. Ifinedo, P. (2014). Understanding information systems security policy compliance: an integration of the theory of planned behaviour and the protection motivation theory, *Computers & Security*, Vol. 31, No. 2011, pp. 83-95.

20. Itrada, A., Sultan, S., Al-Junaidi, M., Qaffaf, R., Mashal, F., Daas, F. (2014). Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a case study, *Jordan Journal of Mechanical and Industrial Engineering*, Vol. 8, No. 2, pp. 102-118.
21. ITU-R M.2370-0. (2015). IMT traffic estimates for the years 2020 to 2030. ITU-R.
22. Kopal, R. (2001). Pojmovnik kriminalističke analitike s prikazom metodologije analize telefonskih izlista. *Police and Security*, Number 1-6/2001, pp. 84-97.
23. Maljak, M., Parlov, N., Sičaja, Ž. (2017). Intelligence services as part of the national security system. *10th international scientific conference Crisis management days*, Book of papers. Velika Gorica: University of Applied Sciences Velika Gorica, pp. 154-165.
24. Malnar, D., Olujić, J. (2019). The Security Challenge of Disruptive Technologies. *Annals of Disaster Risk Sciences*, 2(1-2). Retrieved from https://ojs.vvg.hr/index.php/adrs/article/view/23. Accessed 10 March 2020.
25. Samota, K., Patel, J. (2017). Resent IT trends: A Review paper, *International journal of scientific research in multidisciplinary Studies*, Vol. 3, Issues 5, pp. 1-7.
26. SedamIT (2018). *Matison*, Zagreb. Retrieved from www.matison.eu. Accessed 6 March 2020.
27. Tatalović, S. (2011). Treba li Hrvatskoj nova strategija nacionalne sigurnosti?, *Političke analize*, Zagreb, FPZ, No. 6, Year 11, pp. 34-38.
28. Tatalović, S., Bilandžić, M. (2005). Osnove nacionalne sigurnosti. Zagreb: Ministry of the Interior.
29. The Security and Intelligence System Act. (2006). *Official Gazette of the Republic of Croatia*, 79/06.
30. Whitman, M. E., Mattford, H. J. (2018). Principles of Information Security. Sixth Edition. Mason: Cengage Learning.

Natalija Parlov, Željko Sičaja, Tihomir Katulić, Riko Lusa

Informacijska sigurnost i funkcija tajnog nadzora komunikacija putem infrastrukture davatelja telekomunikacijskih usluga: model napredne arhitekture sustava

Tajni nadzor komunikacija koji se rabi za potrebe nacionalne sigurnosti i u svrhu provođenja policijskih istražnih radnji vrijedno je tehničko sredstvo i koristan alat tijela policijskog, pravosudnog i sigurnosnog sustava. U tehničkim aspektima, ovo polje bilježi značajne pomake u posljednjem desetljeću gdje su dostupni softver i platforme za provođenje tajnog nadzora proširene mogućnostima nadzora širokog spektra različitih komunikacijskih kanala. Funkcija tajnog nadzora komunikacija u suštini predstavlja ograničenje temeljnih prava pojedinaca na području Europske unije i država članica. Svrha ovog rada kao priloga raspravi o mehanizmima tajnog nadzora jest izložiti osobine modela naprednog softvera razvijenog u svrhu tajnog nadzora, usporedba s najčešćim modelima tajnog nadzora i analiza softverske arhitekture definirane od strane Europskog instituta za telekomunikacijske norme (ETSI) kao dominantne norme u ovom području. Iako se ovaj model arhitekture tajnog nadzora razvio inicijalno za nadzor glasovnih komunikacija, može ga se uspješno primijeniti i za tajni nadzor komunikacija koje koriste internet protokol (IP). Konačno, članak pruža komparativni pregled različitog softvera tajnog nadzora u skladu s regulativom funkcije tajnog nadzora.