Lawful Interception and Data Retention in Telecommunication & Internet Networks in Greece

A. D. Panagopoulos, V.M. Stathopoulos, P.T. Trakadas, P.G. Babalis, and C.N. Capsalis

Hellenic Authority for the Information & Communication Security and Privacy (ADAE)
Ierou Lochou 3, Maroussi 151 24,
Athens, Greece

Legal Framework

- ADAE has been established by Article 1 of the law 3115/2003
- Paragraph 2 of the Article 19 of the Greek Constitution
- The objective of ADAE is to protect the Secrecy of Mailing, the Free Correspondence or Communication in any possible way as well as the Security of Networks and Information.
- The concept of Privacy encompasses the Control of Observing and Regulating the Terms and Processes of Waiving of Privacy Protection Rights as foreseen by the law.
- ADAE has Administrative Independency

Legal Framework

- ADAE's premises are in Athens,
- Functional offices can be in other cities of Greece.
- ADAE is responsible to submit its decisions to the Minister of Justice.
- At the end of every year, all the activities performed and the actions taken by ADAE are submitted to the President of the Greek Parliament, the Minister of Justice and the Greek Parliament.
- ADAE is subject to parliamentary examination, in ways and procedures that follow current parliamentary rules.

Organizational Structure

Administration of ADAE

- **President**
- **Vice-President**
- **Members (University Proffessors, Judges, Technical Directors)**
- **Office of Legal Adviser and Legal Services**

Division for the Assurance of Infrastructures and Privacy of Services and Internet Applications

- Department of Internet Applications
- Department of Added Value Services Assurance
- Department of Internet Infrastructures

Division for the Assurance of Infrastructures and Privacy of Telecommunication Services

- Department of Fixed Telephony / Wired Communications
- Department of Mobile Communications
- Department of Wireless Communications
- Department of Satellite Communications

Division for the Assurance of Privacy of Mail Services

- Department of Mail Services
- Department of Courier Services

Independent Department of Administrative and Financial services

Independent Department of International Collaborations and Public Relations

Independent Department for the Waiving of Privacy Protection

Telecommunication Regulatory Framework

Assurance of Privacy Protection during the Supply of Telecommunication Services through Networks of Mobile Communications

- **The clauses of this regulation concern all the mobile telecommunication services providers GSM-2G, GPRS, UMTS-3G**
- **Vulnerable points:**

Terminal equipment (cellular device, file of incoming and outgoing calls, SIM) Network Elements and Services (Base Stations, Mobile Switching Centers, Cryptographic Algorithms, Interconnection Points with Fixed Networks etc.).

Threats on the Mobile Communication Networks are the obtainment of access in the core network, denial of service of an interfered subscriber, attack on the SIM/USIM card, attack on the A5/f8/f9 algorithms, and man-in-the middle attacks.

Telecommunication Regulatory Framework

Assurance of Privacy Protection during the Supply of Telecommunication Services through Wired Networks

•Every Telecommunication Provider which provides or participates on the provision of Fixed Telecommunication Services (Telephony etc) through Wired/Fixed Networks.

• PSTN, ISDN, xDSL

• Vulnerable points:
Terminal equipment (telephone device, machine, etc.)
Network Elements and Services (TNI-Box Telephone Network Interface Box, outdoor switches-KV, switching centers, central switches and gateways).

Telecommunication Regulatory Framework

Assurance of Privacy Protection during the Supply of Telecommunication Services through Wireless Networks

- The clauses of this regulation concern all the wireless telecommunication services providers

- IEEE 802.11- Wi-Fi Networks (WLAN),
  Bluetooth-IEEE 802.15 (WPAN)
  IEEE 802.16-LMDS (WMAN)
  Satellite Networks (VSATs, DVB-S, DVB-S2)

- Vulnerable points:
  Terminal equipment
  Network Elements and Services (Access Points, servers, file of incoming and outgoing calls, hub station, satellite terminals, etc.)

Some threats on the Wireless and Satellite Communication Networks are attacks on the access points, satellite terminals, and on the cryptographic algorithms.

Telecommunication Regulatory Framework

These Regulations are based on the standard
BS 7799-2:2002
ISO/IEC 17799:2000
ITU-T X.1051 .

The Telecommunication Provider shall develop, implement, maintain and continually improve a documented telecommunication security policy that should contain at least:

Access Policy, Acceptable Use Policy, Personnel Security Policy Communications Data Processing Security Policy, Physical Security Policy , Protection of Telecommunication Network (Core, Access), Protection of the Internal Telecommunication Network, Organization Policy, User Ethics Policy, Security Incident Handling Policy, Third Party Agreements Policy, Back-up Security Policy.

Internet Regulatory Framework

Three more regulations referring to the assurance of Internet Communication Privacy. This is achieved by securing the internet infrastructure and the respective system and application services.

The scope of this regulation concerns every Internet Service Provider, Application Service Provider and Added Value Service Provider referred to them as Internet Providers.
Vulnerable Assets: any physical entity that participates in internet communication this communication, that is: the Terminal Equipments, the Network Elements (Routers, Switches or Gateways), the IT nodes and servers (Email servers, web servers etc) and their respective system or application Services.

Internet Regulatory Framework

Mainly, the internet provider shall develop, implement, maintain and continually improve a documented internet security policy that should contain at least the following sub-policies:

Access Policy: **that defines the access and authorization level that each user requires for accessing the provider's assets.**

Acceptable Use Policy: **that defines the allowed or the not allowed activities of each user.**

Perimeter Security Policy: **defines the appropriate mechanisms for protecting internet providers' assets from outside or inside attacks (firewalls, IDSs, e.t.c).**

Management and Installation of Telecommunication Infrastructure Policy : **that assures the communication privacy when changes or insertion of new communication infrastructure takes place.**

Back-up Security Policy **: describes all the required procedures that assure the recovery of communication infrastructure within a logical period of time after the occurrence of any damage.**

Internet Regulatory Framework

Security Incident Handling Policy **: defines a procedure for recording the incidents, notifying the relative organisations and examines all elements for identifying possible mistakes.**

Network Security Audit Policy: **mainly defines a team that uses special security audit software for scanning internet providers' assets for assuring their integrity confidentiality and availability.**

Risk Assessment Policy **: defines the procedure of identification, audit and evaluation of the vulnerable assets and vulnerable access points regarding the hardware and software infrastructure for minimizing the violation probability.**

Internet User Security Policy: **defines the rules and the security requirements for the usage of internet as a secure medium for the communication of sensitive information.**

Internet Regulatory Framework

User Ethics Policy: **defines a set of morality rules regarding the provider or and the user, for assuring the communication privacy**

Password Use Policy: **defines the creation, management and protection procedures regarding passwords usage**

Protection and Virus Deterrence Policy: **defines the deterrence, tracing and confront procedures from viruses.**

Application Service Provider Security Policy: **defines the set of warrants that the service provider requires to get from the application service provider in order to assure the users' communication privacy.**

Subcontractor Contract Policy: **defines the agreement framework, between a service provider and a subcontractor, for a project undertaking that requires access towards the service provider critical assets that is obliged to assure.**

Data Retention

A new directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available Electronic Communications Services or of Public Communications Networks.

- **data necessary to trace and identify the source of a communication**
- **data necessary to identify the destination of a communication**
- **data necessary to identify the date, time and duration of a communication**
- **data necessary to identify the type of communication**
- **data necessary to identify users' communication equipment or what purports to be their equipment**
- **data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.**

No data that are retained, reveal the content of the communication.

Data Retention

- Telecommunication and Internet Providers serve as the sources of data to be retained. They have the responsibility for the full act of Data Retention.
- The provider is responsible for the storage of the retained data, its Authenticity, Accuracy, Security, Prevention of loss during the retention period, and its delivery to the authorities.
- The provider is also responsible for data deletion at the end of the retention period.

Data Retention

- Upon receipt of a lawful warrant from the LEA requesting information about a specific target from the data retention repository, the provider will deliver without delay all retained information matching the warrant.

- The LEA can query the provider to the status of the request. LEA is any official authority, authorized by national law, which is allowed to request and receive information retained by a provider.

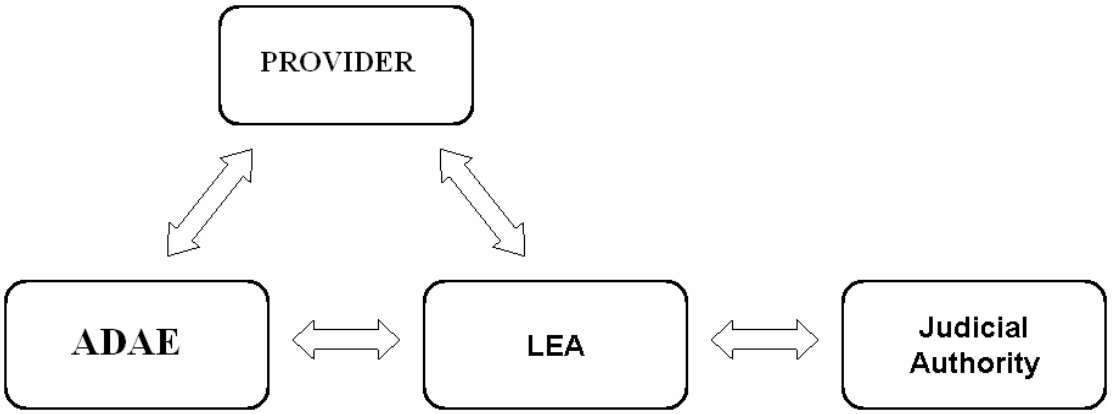
- LEA requests a warrant for the retrieval of retained data of a particular subscriber from the Judicial Authority. LEA requests the information retained about a specific target from the provider by supplying the appropriate warrant, digitally or manually signed by the Judicial Authority.

- Once the provider accepts and ADAE validates the request, the information is delivered to the LEA, which can use it for its investigative purposes and for submission as evidence in court.

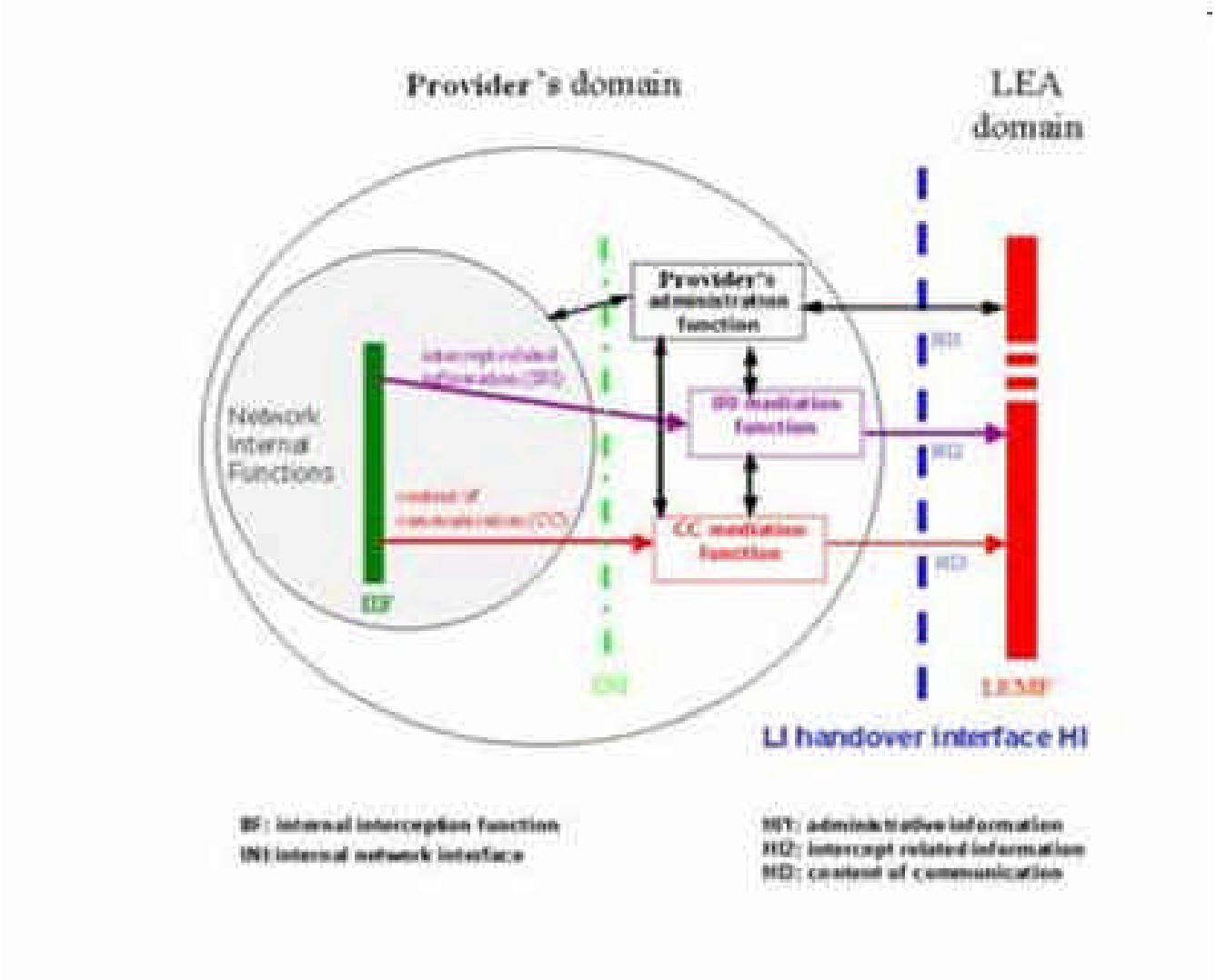
Data Retention

•LEA requests a warrant for the retrieval of retained data of a particular subscriber from the Judicial Authority. LEA requests the information retained about a specific target from the provider by supplying the appropriate warrant, digitally or manually signed by the Judicial Authority.

•LEAs and the Providers are directly audited by ADAE for the above procedure.



Lawful Interception



Lawful Interception

- LI system contains the network internal functions, the internal network interface (INI), the administration function and the mediation functions for IRI and CC.

- Network Internal Functions contain the internal functions of the network (e.g. switching, routing, handling of the communication process). Within the network internal function the results of interception (IRI, CC) are generated in the IIF.

- The internal interception functions (IIF) provide the content of communication (CC) and the intercept related information (IRI), respectively, at the internal network interface INI.

- Within the provider's administration centre, the LI related tasks, as received via interface HI1, are translated into man machine commands for the provider's equipment.

Lawful Interception-CS

There have been done meetings in ADAE premises between mobile and fixed telephony providers and many issues of the three interfaces prescribed in ETSI 201671 have been agreed like:

- HI1 specification (manually),
- IRI continue records,
- Mono/Stereo mode, Call Identifier (CID),
- Network Identifier (NID),
- CC Link Identifier (CCLID),
- Call Identity Number (CIN)
- Definition of interception Start, Date & time indication.

Lawful Interception Identifier (LIID) has not been identified yet.

For each LEA the LIID value is unique. 25 alphanumeric characters (octets) are reserved for the LIID in ETSI standard.

Lawful Interception-CS

•The Type of Interconnection (leased lines, through public switched telecommunication network, etc) between the Providers and the LEAs and the security measures for HI2 and HI3 interfaces have not been agreed yet.

•Security requirements at the interface ports HI2 and HI3 should been discussed and addressed issues like Authentication, Confidentiality and Integrity.

Lawful Interception-PS

ETSI TS 102 232 is a generic standard which describes HI parts, ETSI TS 102 234 concerns with internet access by applying to the total IP traffic while ETSI TS 102 233 is referred to e-mail services.

There are some key requirements that should be fulfilled by the involved parts when implementing any LI architecture.

- **LI must be undetectable by the intercept subject. Solutions such as wiretapping the customer premise equipment (CPE) or diverting the call to a conference unit is not acceptable because the intercept subject can detect the LI. Tapping should be enforced on equipment that is within the domain of trust of the Internet Service Provider (ISP) and must be performed along the normal path of the data.**
- **Multiple LEAs intercepting the same subject must not be aware of each other.**
- **Security mechanisms should be enforced in order to avoid unauthorized personnel from performing wiretaps.**
- **The information identifying intercepts must be correlated with the corresponding content of intercepts.**
- **Information towards the LEAs must support the same reliability as the original delivery of the packets to customers.**

Lawful Interception-PS

Interception Mediation should carry out the following functions:

- **Collection of intercepted data from various switches routers probes etc. in the network**
- **Formatting the data into standardized representations**
- **Delivery of the data to one or more LEAs.**
- **Ensuring that a given LEA is authorized to accept the delivered data protection of all delivered information against unauthorized access and modification through rigorous network security.**
- **Delivery of the interception information in a timely manner, with appropriate time stamps to synchronize network events against content delivered.**

Conclusions

- **Technical Divisions of ADAE are presented.**

- **ADAE's technical regulations and their basic points regarding the required by ADAE Security Policies are discussed.**

- **The vulnerable components of each and the security threats are given.**

- **The recently released Data Retention Directive is also addressed.**

- **A small introduction in Lawful Interception Implementation and its Open Issues have finally been discussed .**