This thematic section is intended to inform readers on the latest progress of standardization work items on Lawful Interception (LI) and Retained Data (RD) mainly focusing on European regional level (ETSI). The scope is to cover all relevant LI and RD aspects in terms of requirements, communication service providers architecture and network interfaces/protocols definition.

by Gerald McQuaid and Domenico Raffaele Cione

THE LI-INTERFACE FOR WARRANT INFORMATION

Gerald MCQUAID is Chairman of ETSI Technical Committee for Lawful Interception and attending ETSI TC CYBER and 3GPP SA3 LI since 2004. Member of the EU Data Retention Experts Group under the auspices of the European Commission.

Domenico Raffaele CIONE, Ericsson Strategic Product Manager for Regulatory Solutions, is active delegate in ETSI Technical Committees for Lawful Interception (LI) and Retained Data (RD) since 2003.

1. Background

Traditionally the ETSI standardization work was focused on IRI and CC data details (from CSP to LEA) by defining, updating and maintaining related data Handover Interfaces (HI-2 and HI-3) specifications (ref. [1], [2], [3] with related services parts). Furthermore, ETSI had defined a dedicated Handover Interface, named HI-1, at clause 5.3 of ref. [7], referred to be also crossing borders between countries based on corresponding international laws or agreements. HI-1 was defined as an interface between LEA and CSP to transport all kind of administrative information being used for the transmission of the request to establish or to remove the interception action from the LEA to the CSP and the acknowledgement message back to the LEA. This HI-1 port was extended to support manual transmission (e.g. document fax) for cases in which an automatic transmission between LEA and CSP was not possible for some reasons. Status reporting from CSP to LEA or LEMF was defined to cover all kind of alarms, reports or information related to the intercept function. Overview of HI-1 was provided by clause 5.1 of ref. [1].

HI-1 was not standardized at stage 3 level (e.g. detailing protocols, messages, parameters) and its standard implementation was limited to HI-1 Notification interface data from CSP to LEA, as specified by clauses 5.1, 7 and D.4 of ref. [1] and by Annex M of ref. [2] specifically for the 3GPP HI-1 Notification. Both these HI Notification implementations are supported by the ASN.1 Specification of the ETSI HI IP delivery mechanism as specified by clause A.2 of ref. [3].

2. Latest years standard evolution

Based on the experience of standardization in HI-2 and HI-3 that has provided industry with benefits in terms of interoperability, security and cost reduction, starting from 2013 almost all major European Government organizations present in ETSI TC LI have supported a new standard document to provide a completely new ***electronic interface*** for warrant information for the exchange of information relating to the establishment and management of Lawful Interception between two systems. The initial input materials were the requirements of the different Administrative European countries which were analyzed to identify the set of common requirements as base for the new HI standard specifications. Following the initial document definitions, also non-European organizations (from US and Australia among others) were actively involved by contributing with their requirements and implementation proposals resulting into a specification adoptable worldwide, hence not limited to the European countries context. The specification has been finalized in January 2016 with the publication of the ETSI TS 103 120 v1.1.1, ref. [4].

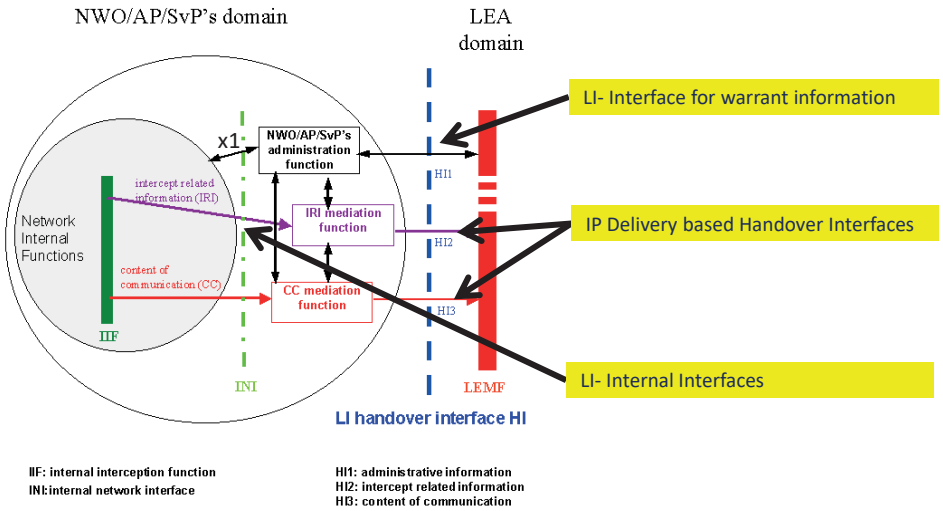

Fig. 1: *ETSI LI HI standards*

Usage of standardized HI-1 is applicable to several scenarios with LEA, CSP, Warrant Approval Authorities (single or multiple) and Central Authority. Figures 2a to 2d shows the main four architecture covered by this ETSI TS.

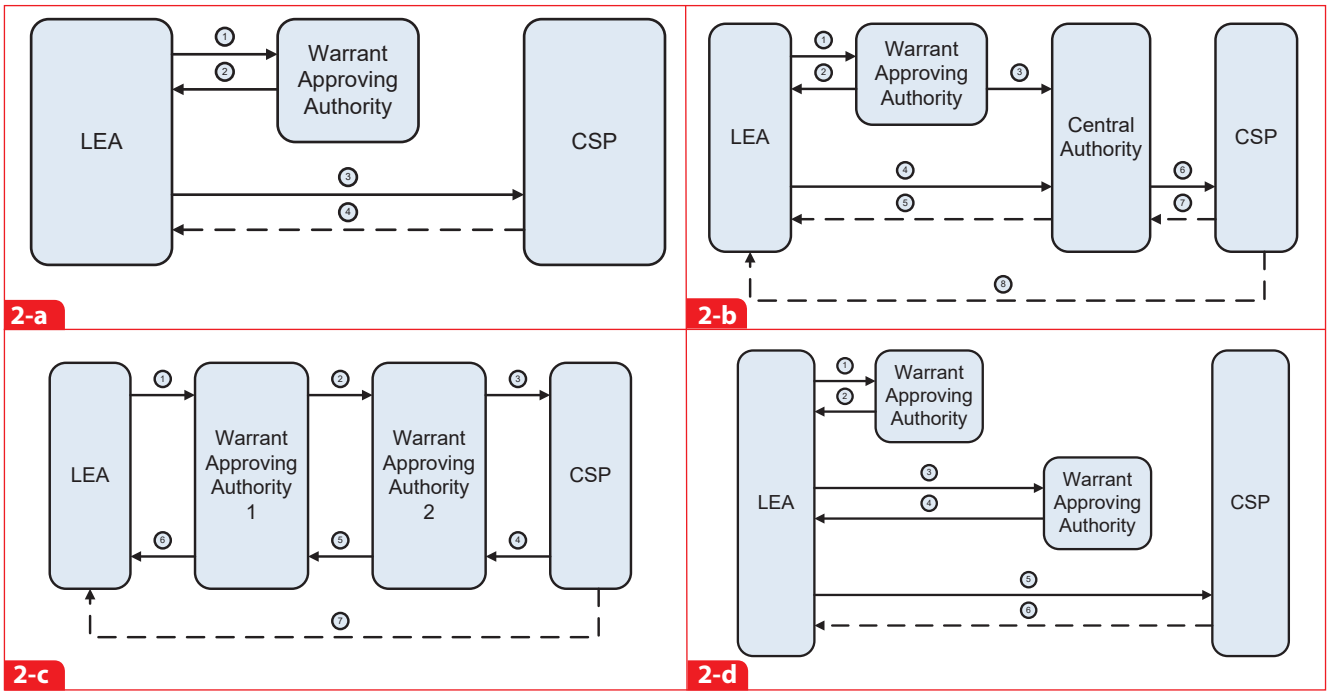

Fig. 2: *Example usage scenarios for exchange of warrant and tasking information*
2-a: *Simple architecture;* ***2-b:*** *Scenario including a Central Authority*
2-c: *Scenario with multiple Approving Authorities and "Serial" interaction;*
2-d: *Scenario with multiple Approving Authorities and "Parallel" interaction.*

4. TS 103 120 Specification

The standard document is intended to provide an interface and data structure of warrant leaving out the definition of the process for creating, approving and implementing a warrant as national matter. Specifically, the TS provides the definition of national profiles to specify the national logics and rules that are applied to warrant exchange. A National Profile is specified as informative example.

HI-1 is simply defined by means of Request and Response messages and each Message is made of a Header and a Payload component (Request Payload, Response Payload). The Message Header part is only intended to contain basic routing and identification information. The Message Payload consists of a collection of Actions (Action Requests, Action Responses) and only few basic actions have been identified, e.g. Get, Create, Update and List. Each Action was conceived to act on a specific Object which was defined as the relevant entity for Data Definitions. The basic set of standard Object types are defined for Authorization, Document, Notification and Task to manage the LI interception task associated to a target. ETSI target identifier formats and all possible error codes are all detailed within normative annexes.

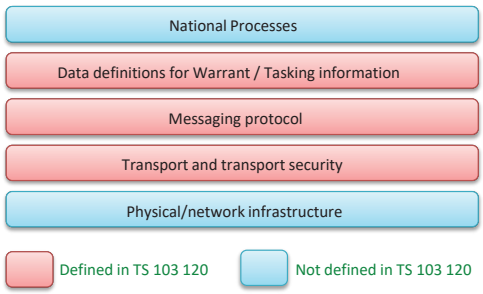

Fig. 3: *Conceptual structure of the standard*

Based on the defined data details, the specification provides LEA with the management of all the basic electronic procedures on warrants by allowing actions at different data levels (including also document exchange). The defined HI-1 interface is now being used as the new official standard HI-1 interface referred in all new LI specifications, i.e. the corresponding internal X1 interface (ref. [5]) and NFV LI Architecture (ref.[6]). Further analysis has started to consider its possible extension to new requirements, i.e. the possible coverage of the Retained Data HI management. Encoding and Transport mechanisms are specified in terms of XML schema and HTTP transport, but a nationally-defined transport alternative is allowed as national basis. ©

ABBREVIATIONS

CSP	Communication Service Provider
CC	Content of Communication
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
HI	Handover Interface
IRI	Intercept Related Information
NFV	Network Function Virtualisation
HTTP	HyperText Transfer Protocol
XML	eXtensible Markup Language

REFERENCES

[1] ETSI TS 101 671 Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic v3.14.1 (2016-03)
[2] ETSI TS 133 108 Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108 version 13.1.0 Release 13)
[3] ETSI TS 102 232-1 Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery v3.11.1 (2016-03)
[4] ETSI TS 103 120 Lawful Interception (LI); Interface for warrant information v1.1.1 (2016-01)
[5] draft ETSI TS 103 221-1 Lawful Interception (LI); Internal interface X1 v0.1.2 (2016-09)
[6] draft ETSI GS NFV-SEC 11 Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture
[7] ETSI TS 101 158 v1.3.1 (2014-02) Telecommunications security; Lawful Interception (LI); Requirements for network functions ◊