Muñoz, A., Urueña, M., Aparicio, R. & Rodríguez de los Santos, G. (2015). Digital Wiretap Warrant: Improving the security of ETSI Lawful Interception. *Digital Investigation*, 14, pp. 1-16.

DOI: 10.1016/j.diin.2015.04.005

Digital Wiretap Warrant: Improving the security of ETSI Lawful Interception

Alfonso Muñoz, Manuel Urueña*, Raquel Aparicio, Gerson Rodríguez de los Santos

Universidad Carlos III de Madrid, Avda. Universidad 30, 28911 Leganés, Spain

Lawful Interception (LI) of data communications is an essential tool for Law Enforcement Agencies (LEA) in order to investigate criminal activities carried out or coordinated by means of Internet. However, the ability to secretly monitor the activities of citizens also has a great impact on civil rights. Therefore, democratic societies must prevent abuse and ensure that LI is only employed in specific cases with justifiable grounds or a probable cause. Nowadays, in many countries each interception must be authorized by a wiretap warrant, usually issued by a judge. However, this wiretap warrant is merely an administrative document that should be checked by the network or service operator before enabling the monitoring of its customers, whose communications are later handed over to a LEA in plaintext. This paper proposes the idea of employing a Digital Wiretap Warrant (DWW), which further protects the civil liberties, security and privacy of LI by ensuring that monitoring devices can only be enabled with a valid DWW, and by encrypting the captured data so only the authorized LEA is able to decrypt those communications. Moreover, in the proposed DWW framework all digital evidence is securely time-stamped and signed, thus guaranteeing that it has not been tampered with, and that a proper chain of custody has been met. In particular this paper proposes how to apply the DWW concept to the lawful interception framework defined by the ETSI LI Technical Committee, and evaluates how the additional security mechanisms could impact the performance and storage costs of a LI platform.

Keywords: Digital Wiretap Warrant (DWW) - Lawful Interception (LI) - ETSI LI Technical Committee - Civil rights - Security - Privacy - Digital evidence - Chain of custody

Introduction

The advances of Information and Communication Technologies (ICT) have facilitated worldwide cooperation, communication and data sharing across the Internet. In addition to its enormous benefits, like any other broad-spectrum technology, data communications can be also employed for illegal purposes: human trafficking, organized crime, illegal drug trade, child pornography, terrorism, etc.

* Corresponding author.

E-mail addresses: ammunoz@it.uc3m.es (A. Mu˜noz), muruenya@it.uc3m.es (M. Urue˜na), raparici@pa.uc3m.es (R. Aparicio), gsantos@it.uc3m.es (G. Rodríguez de los Santos).

Therefore, governments, and in particular their law enforcement and intelligence agencies, have to employ new tools to identify criminals and prosecute illegal acts when they occur, or are coordinated, through electronic means. Although *Lawful Interception* (LI) of data communications seems to be necessary nowadays, and thus it has been included in the legal framework of modern democratic countries, this does not mean that these monitoring technologies should be deployed without considering a number of human rights issues, including the secrecy of correspondence and privacy of private life. In fact, there are a multitude of recent examples where similar monitoring technologies have been employed for mass surveillance, thwarting freedom of speech and oppressing dissidents (Reporters without borders, March 2011; Clayton et al.,

2006). But even consolidated democratic societies are not immune to the misuse of lawful interception technologies (Prevelakis and Spinellis, 2007; Risen and Lichtblau; Singel; Poulsen; Diffie and Landau, 2009).

Democratic societies must thus ensure that lawful interception of data communications is only employed in very specific cases, when less intrusive methods cannot be applied, and for the investigation of serious crimes that thwart critical human rights, like the right to life or the freedom from slavery that may override other human rights such as privacy and secrecy of communications. Nowadays this is achieved by a combination of legal and procedural mechanisms that depend on national legislations and thus vary very significantly among countries. Nevertheless, in many countries lawful interception must be explicitly authorized by a judge, who verifies that any wiretap request from a *Law Enforcement Agency* (LEA), such as the Police, is well founded, has justifiable grounds and/or a probable cause, and that the criminal offense being investigated is severe enough to justify the monitoring of all (or part) of the suspect's communications, and only during a certain period of time. The judge then issues a so-called *Wiretap Warrant* (WW), specifying the details and restrictions of the authorized monitoring. The LEA hands over the WW document to the telecommunication provider of the suspect, which should first verify it and then start monitoring the communications of its customer. This monitoring may be performed ad hoc, but it is usually done by means of dedicated LI equipment, which telecom providers are bound by law to deploy in order to operate in the country. The captured communications should be delivered only to the law enforcement agency that originally requested it. Finally, the LEA employs the captured communications for its investigations and, depending on the national legislation, the intercepted contents may be employed as evidence in a court of justice.

Therefore, the security of the whole process mainly resides on the paper-based wiretap warrant and thus on the trust that the telecom provider really validates the WW and abides to its rules and limits, such as keeping the captured information confidential. However, this wiretap warrant is merely an administrative document, meaning that the telecom provider, in collusion with the LEA or other third party, may monitor some of its customers without a valid WW, ignore the limits of an existing one, or just peek into the captured data of a valid LI, for instance to sell it to journalists. Furthermore, a corrupt member of the LEA may silently delete or tamper some digital evidence (e.g. changing the date or the location of a phone call) in order to incriminate an innocent person or to release a criminal. Obviously these are serious offences that are severely penalized in all legal frameworks, but still nowadays the proper implementation of lawful interception is only enforced by legal and administrative means, not technical ones.

In order to solve these problems, this paper proposes the so-called *Digital Wiretap Warrant (DWW)*, which is also issued by a judge to authorize, within certain limits, the monitoring of a particular suspect. However the DWW is also a digital document, and thus it can be an integral part of the lawful interception technical process. In particular, we propose that certified LI equipment cannot be enabled without a valid DWW (i.e. digitally signed by a judge), and that the captured communications must be securely time-stamped, signed and encrypted by the monitoring station itself, so that not even the telecom provider can peek at the data captured by the LI platform, but only the law enforcement agency that obtained the DWW from the judge. Moreover, a corrupt or overzealous LEA agent cannot secretly delete or tamper the seized digital evidence, since the new DWW-enabled LI process creates a secure chain of custody that can be followed back up to the monitoring station that captured the data. Furthermore, this paper specifies how the proposed DWW mechanism can be applied to the LI architecture defined by the LI Technical Committee of the European Telecommunications Standards Institute (ETSI).

Before starting to discuss the details of the DWW proposal, Section 2 reviews related work on lawful interception. Section 3 briefly summarizes ETSI LI standards and analyses their security limitations. Section 4 provides an overview of the proposed DWW-enabled LI process in the context of the considered ETSI LI limitations. Section 5 explains in detail the proposed DWW LI platform. Then, Section 6 analyses the security properties of the proposed DWW LI workflow, while Section 7 provides a brief discussion about the performance, cost and scalability of the DWW LI platform. Finally, Section 8 summarizes the main results of this work and concludes the paper.

Related work

Most fears about powerful surveillance programs were summed up by Diffie and Landau in (Diffie and Landau, 2009, 2007). From a more technical point of view, there is still a vivid debate (Electronic Frontier Foundation and 2014–04; Townsend) on whether building wiretapping capabilities into communications infrastructures is truly necessary or it creates new privacy risks (Riabov, May 2000). However, this has not stopped other LI standardization efforts or network vendors from including LI capabilities on their products (Baker et al., 2004), and LI technologies are widely used nowadays in modern democratic countries. The two major LI standards are CALEA (Communications Assistance for Law Enforcement Act), mainly employed in the USA, and ETSI LI, which is a European standard,[1] although it is also employed in several parts of the world, as it has also been adopted by other bodies like the 3rd Generation Partnership Project (3GPP). This paper is focused on the ESTI LI architecture, which is explained in next section.

In the last years several security researchers have reported potential attacks to LI systems (Cross, 2010), as well as some abuses by law enforcement or intelligence agencies. For instance the intercept target can launch denial of service (DoS) attacks (Sherr et al., 2009) that prevent the accurate collection of not only the call contents, but even the metadata recorded by the law enforcement agency. These problems motivate other researchers to propose improvements to lawful interception systems, or

[1] Notice though that, due to the different LI national legislations, it has not even been adopted in all European countries.

even completely different alternatives (Bellovin et al., 2013) for LI. In (Bates et al., 2012), Bates et al. proposed a more accountable CALEA wiretapping system that enables secure audits. The proposed system maintains an encrypted log of wiretap meta-data, and allows different access profiles to those wiretap records.

Regarding to actual cases of LI misuse, probably the most well-known one is the Vodafone Greece case (Prevelakis and Spinellis, 2007) in 2004–2005, where some unknown attackers leveraged the wiretap capabilities of mobile network switches to spy the communications of more than 100 mobile phones of high level officials, including the Greek Prime Minister and members of his government. Meanwhile in the United States, it was reported that the national security agency (NSA) illegally wiretapped US residents without a proper wiretap warrant (Risen and Lichtblau; Singel). And more recently, it has been reported that some analysts abused the vast NSA powers tools to spy their love interests or just other people they met (Poulsen).

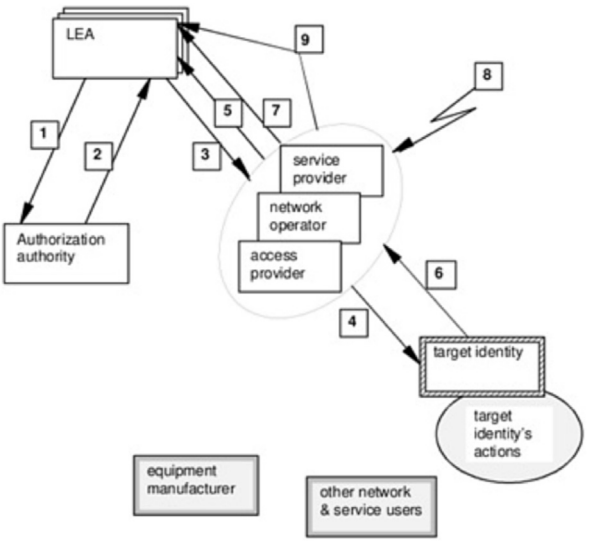

Fig. 1. Workflow in ETSI Lawful Interception framework (ETSI, April 2002).

ETSI Lawful Interception standards

The specifications produced by the ETSI Technical Committee Lawful Interception define a reference handover interface for the provision of Lawful Interception (LI) from a *Network Operator* (NWO), *Service Provider* (SvP) or *Access Provider* (AP) to a Law Enforcement Agency (LEA).

The following specifications are basic to understand the LI framework defined by ETSI:

- ETSI Technical Specification 101 331 (ETSI, 2009) provides the set of requirements for lawful interception from the LEA point of view.
- ETSI Standard 201 158 (ETSI, April 2002) describes the common network functions and the general architec-ture to be applied to all network technologies.
- ETSI Technical Specification 101 671 (ETSI, 2011) specifies the generic flow of information, procedures and information elements.
- ETSI Technical Specification 102 232 has seven parts that define, among others, the IP-based LI handover interface (ETSI, 2011) and how IP messaging (ETSI, 2012a) and Internet access services (ETSI, 2012b) should be intercepted.

The ETSI, together with the Third Generation Partnership Project (3GPP), also specify how to intercept voice and other multimedia services carried out by circuit-switched PSTN/ISDN networks, cellular services, or IP Multimedia Services (IMS). This paper is focused on data communications over IP networks, although our proposal could be also extended to those multimedia services as well.

The information to be provided to the LEA is divided into two types: *Intercept Related Information* (IRI) and *Content of Communication* (CC). The former is basically meta-information associated with the communication, such as the time or the user's location. The latter is the actual data exchanged between two or more users (i.e. flow of TCP/IP datagrams or an e-mail message).

Fig. 1 shows the main steps of the flow of information among the different players in the ETSI LI framework:

1. A LEA (e.g. the Police) makes a lawful interception request for a particular subject to the authorization authority.
2. The authorization authority (e.g. a judge) issues a lawful authorization (i.e. wiretap warrant) for the LEA.
3. The LEA hands over this authorization to the NWO/AP/SvP, who determines the relevant target identities from the information contained in the authorization.
4. The NWO/AP/SvP configures its interception facilities to monitor the relevant target identities (e.g. a cellular line and the Internet connection at home).
5. The NWO/AP/SvP informs the LEA that the lawful authorization has been received and acted upon. Information relating to the target identities and the target identification may be also passed.
6. The CC sent by the target identity is intercepted by the NWO/AP/SvP.
7. The CC and associated IRI are handed over from the NWO/AP/SvP to the LEA monitoring facility.
8. Either on request from the LEA or when the period of the lawful authorization expires, the NWO/AP/SvP ceases the interception.
9. The NWO/AP/SvP announces this cessation to the LEA.

The communications between the *LEA Monitoring Facility* (LEMF) and the NWO/AP/SvP domain occurs through the *Handover Interface* (HI), which is a generic reference interface that is logically split in three sub-interfaces to exchange administrative (HI1), IRI (HI2) and CC (HI3) information as shown in Fig. 2.

HI1 exchanges administrative information between the LEA and the NWO/AP/SvP such as the requests to establish or remove an interception from the LEA to the NWO/AP/SvP, the acknowledgement messages back to the LEA, and

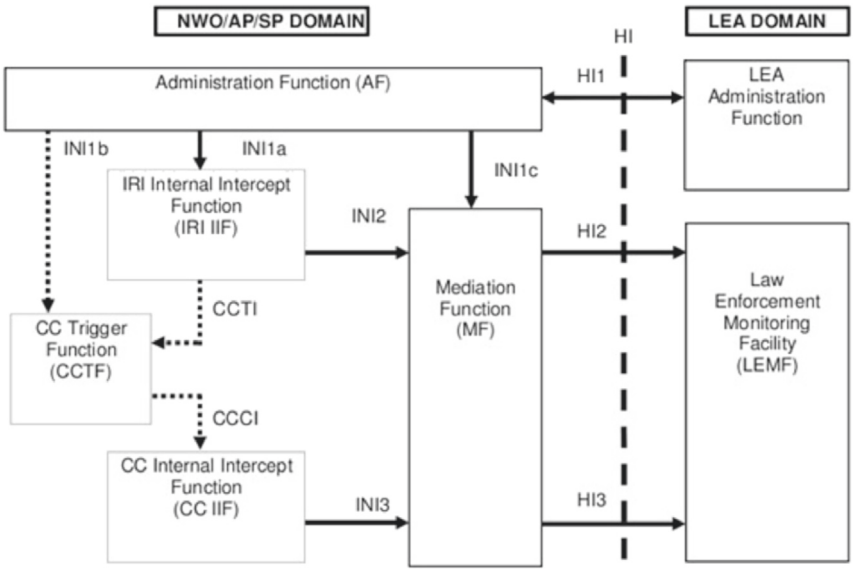

Fig. 2. Reference model of ETSI lawful interception framework for packet services (ETSI, 2011).

status reports such as alarms or other information related to the interception functions.

HI2 transports the Intercept Related Information (IRI) from the NWO/AP/SvP to the LEMF. That is, the signalling information used to establish the communication service and to control it, and any other supplementary service or location information, for instance the IP address of the target.

HI3 transports the Content of Communication (CC) from the NWO/AP/SvP to the LEMF. It must be a cleartext copy of the information flow. If the NWO/AP/SvP provides encryption for its customers (i.e. webmail over HTTPS), then the result of interception needs to be handed over to the LEA already decrypted by the NWO/AP/SvP. Fig. 2 shows in more detail the internals of the NWO/AP/SvP domain. The *Internal Interception Function* (IIF) is a set of logical entities that comprises the functions internal to the network that perform the actual interception: IRI-IIF, CC-IIF and *CC Trigger Function* (CCTF). The *Internal Network Interfaces* (INI) is a set of interfaces that carry information among the Administration Function (AF), the IIFs, and what is called a Mediation Function (MF), which acts as a proxy and passes information through the Handover Interfaces to the LEMF.

The *Administration Function* (AF) ensures that an intercept request from a LEA via HI1 is provisioned for delivery from the network to the LEA. It provides IRI-IIF, CCTF and MF with the required information to perform their tasks.

The IRI-IIF generates IRI information associated with sessions, calls, connections and any other meta-information involving intercepted targets. It notifies target activity to the CCTF via the *CC Trigger Interface* (CCTI) to enable dynamic provisioning (e.g. in the case of an Access Provider operating multiple WiFi hotspots across the country), in addition to static provisioning (e.g. if the target employs a fixed xDSL access). CCTF determines the location of the CC-IIF device associated to the target CC traffic, and controls it via the *CC Control Interface* (CCCI). This CC-IIF device, that we call *Monitoring Station* (MS) in the sequel, captures the CC from the network.

The *Mediation Function* (MF) must be first provisioned by the AF. It then receives information related to active intercepts from the IRI-IIFs and CC-IIFs, and correlates and formats such information for delivery to the LEMF over the HI2 (IRI) and HI3 (CC) handover interfaces. If more than one LEA has requested the interception of the same target, the captured information is duplicated and sent to those LEAs. In order for the MF to distinguish among the information that corresponds to each LEA, and to keep the knowledge about the targets limited within the authorized NWO/AP/SvP operators and the LEAs handling agents, an opaque *Lawful Interception Identifier* (LIID) shall be agreed between each LEA and the operator. This is a main component of the CC and IRI, and is used for identification and correlation purposes.

In addition to the featured interfaces, ETSI Technical Report 103 690 (ETSI, February 2012c), has recently specified an electronic interface, called *eWarrant* interface, for the reception of requests for real-time or stored information (i.e. subject to data retention policies) by an issuing authority possessing lawful authorization to initiate such a request. Although this digital interface may be similar to the proposed DWW concept, it does only consider the administrative part of the LI, and thus does not protect the LI data path as DWW does. Nevertheless, it is interesting to note the increasing importance of security and privacy within the ETSI LI Technical Committee.

Current limitations of ETSI Lawful Interception

ETSI LI standards only include a small number of considerations regarding the security of the LI framework (ETSI, 2006), other than common ICT security best practices. In particular, it addresses security by protecting the

communication between consecutive LI elements (i.e. in a hop-by-hop basis). It recommends using X.509 certificates to authenticate the endpoints, and Transport Layer Security (TLS) or IPSec-based Virtual Private Network (VPN) technologies to protect the exchanged information among all framework entities, and especially across the handover interface (HI). Therefore, intermediate systems, like the NWO Mediation Function (MF), could access all captured information, since it is only encrypted in transit from the Monitoring Station (MS) to the MF and from the MF to the Law Enforcement Mediation Function (LEMF). In our opinion, this reduced security framework leads to the following limitations of ETSI LI standards from the point of view of guaranteeing civil liberties:

Wiretap warrant authorization is just an administrative process. This means that NWO/AP/SvP staff may misuse the deployed LI framework to illegally monitor its customers, gather information about current LEAs investigations, etc.

Privacy only among contiguous entities (e.g. from MS to MF and from MF to LEMF). Intermediate entities, like the NWO MF, have access to all captured information in cleartext.

ETSI LI standards do not include any reference to guaranteeing a proper evidence chain of custody, in order to allow captured data being safely employed as evidence in a court of justice.

Digital Wiretap Warrant (DWW) proposal

To address the aforementioned issues, we propose enhancing the ETSI LI standards with the so-called *Digital Wiretap Warrant* (DWW) in order to better guarantee civil rights by technical means. The DWW proposal has been designed as a complement to current ETSI LI standards and systems, instead of calling for a complete overhaul of those. The main principles of the DWW proposal are:

Lawful Interception equipment must be only enabled by a valid DWW. Any lawful interception system that may monitor the communications of citizens must be limited in time, minimize the data to be captured, and be explicitly approved by the appropriate authority. In particular, no element of the LI framework must be able to work without a valid DWW.[2]

Privacy and protection of captured content. All content captured during the investigations must be strictly private, and thus it should only be disclosed to the authorized personnel of the LEA, under the need-to-know principle. Therefore, all communication contents must be encrypted from the moment they are captured, and only the LEA that requested the wiretap (i.e. not even the NWO/AP/SvP, or any third party that may store them) should have access to the decryption key. At any moment, the lawful interception platform must know where communications are stored, the actual number of copies, and who/when accessed them.

Secure chain of custody. Any exchanged information between LI systems and access to the seized content must be authorized by cryptographic means, guaranteeing the integrity of data and the identity of both peers. Although these considerations are mostly applicable to the internal LEA systems, the LI framework must also ensure that every transaction is digitally signed by the source entity, and securely time-stamped. This is the pre-requisite for any future auditing process that may be performed by an independent expert in order to guarantee the validity of digital evidence.

No evidence tampering/fabrication, even in confabulation scenarios. Besides a secure chain of custody, the LI platform should hinder any attempt of evidence fabrication/tampering, even if several entities (e.g. LEA and NWO) confabulate. This requires technical mechanisms, but also administrative ones. For instance, the LI platform should provide automatic mechanisms to securely capture, transfer and store the seized information, but other key tasks, such as the approval of the wiretap by the judge or the NWO, require human supervision to evaluate non-technical issues, such as the proportionality of the wiretap with respect to the investigated crime and the probable cause. On the other hand, the digital nature of DWW can simplify the administrative process by performing automatic checks, and thus avoiding common human mistakes. Therefore, we do not propose replacing the current LI procedures or human supervision, but to improve them with additional tools.

Support for off-line transport and storage of information. Unlike current ETSI LI standards, this proposal is not only focused on securing data transmission, but data itself. This means that information is protected even when not in transit, for instance when stored in the MF proxy. This also enables any kind of transport mechanism, including off-line ones (e.g. sending a hard disk with the captured data to the LEA), which may be necessary in some cases due to the huge volume of information that a complete data wiretap could entail.

DWW architecture: main concepts

The DWW architecture consists of four main players: the Law Enforcement Agency (LEA), the Network Operator (NWO),[3] the Judicial System (JS) and a global Time Stamping Authority (TSA_{global}) that may be also hosted by the Judicial System or another party. Our proposal has been designed to avoid major changes to the standard ETSI LI architecture. In particular, ETSI LI systems keep most of their behaviour and communication technologies. Our proposal is focused on the application-level messages exchanged through standardized interfaces (both for administrative and mediation functions), in order to fulfil the target security requirements. All exchanged

[2] Notice that this would prevent "emergency" wiretaps that allow LEAs to start monitoring a suspect before asking for court approval. However this practice may be still supported by allowing the Judicial System to automatically sign short-term "emergency" DWWs to LEAs, which are later replaced by a properly judge-supervised one without disrupting the ongoing interception.

[3] For simplicity, in this paper we only refer to Network Operators (NWOs), but all discussions are also applicable to Access Providers (APs) and Service Providers (SvPs).

information among platform elements are encrypted and signed, and the most important data are also time-stamped to protect the evidence custody chain and enable auditing.

The typical operation of the DWW architecture requires the exchange of different information by the administrative interfaces of the LEA, the NWO and the JS involved in interception LI. If all administrative, security and legal checks are right, the NWO starts the requested interception and all seized data is handed over to the appropriate LEAs.

As explained later, a DWW is divided into two different parts: DWW_{NWO} and DWW_{LEA}. The judge first gives to the requesting LEA the DWW_{NWO} part, so the LEA could request a specific NWO to start the interception, once the order has been validated (both, technically and administratively). The DWW_{LEA} part is only be provided to the LEA when the judge considers that it may start analysing the seized data. These two DWW orders make use of symmetric and asymmetric cryptography for achieving these aims.

In addition to the described domains, the Monitoring Station (MS) is the core element of our platform. It resides in the NWO but it is not fully under NWO administration. To accomplish the objectives of our proposal, the monitoring station implements additional security mechanisms that will be described in the following sections. It is worth noting that a MS only works with a valid DWW_{NWO} signed by a judge. All information captured by the MS is encrypted, signed and time-stamped. Therefore, any intermediate element cannot access this information, but only a specific LEA can decrypt it when the judge provides the DWW_{LEA} part.

Technical description of the DWW framework

In order to guarantee confidentiality, integrity, authentication and non-repudiation at the administrative function level, each administrative entity must have at least one pair of asymmetric keys (provided as digital certificates):

Judicial System Administration: $< JS_{pub}, JS_{priv} >$

Law Enforcement Agency Administration:
$< LEA_{pub}, LEA_{priv} >$

Network Operator Administration:
$< NWO_{pub}, NWO_{priv} >$

A *Judge* (J) can only communicate with other domains through the judicial system administration. An interception is only possible with a digital wiretap warrant, signed by the judge authorized to do so. Every judge that is able to authorize a LI must have a key pair (as a digital certificate) in order to digitally sign the DWWs:

Judge: $< J_{pub}, J_{priv} >$

A trusted, global Time Stamping Authority (TSA_{global}) must also exist. The TSA securely time-stamps the transactions between systems in different administrative domains. The TSA may be hosted by the Judicial System to improve its auditing and oversight capabilities, although being an independent entity could provide additional security against confabulation. This element is essential to guarantee the evidence chain of custody, since it allows knowing when communications took place and prevents the erasure of information as it will be described later. In order to hinder Denial of Service (DoS) attacks, the access to TSA should be limited, so only the systems defined by the LEAs and NWOs should be able to access it. TSA authentication and integrity are also achieved using a key pair:

TSA_{global} : $< TSA_{global-pub}, TSA_{global-priv} >$

Each domain may have its own Public Key Infrastructure (PKI) in order to issue certificates and validate the ones from the local domain, as well as to validate the public certificates from other domains by means of peer agreements (i.e. cross-signing the certificates of peer entities). The administrative communication among different domains is always similar:

1. The emitter domain signs the message to be sent with its private key (providing authentication and integrity) and encrypts it with the public key of receiver (providing privacy).
2. Then the receiver domain communicates with the TSA_{global} to obtain a timestamp that demonstrates the reception of the message sent by the emitter domain.
3. Finally the receiver domain sends an acknowledgment of this message, including its timestamp (TSA_{global}), to the emitter domain. With this information both domains have non-repudiation proofs of their interaction thanks to the trustworthy TSA_{global}.

Handover of DWW from LEA to NWO

When some investigation department of a LEA wants to intercept the communications of a particular suspect, it has to first request it to the internal LEA LI department for approval, which should be the only one able to communicate with the judicial system. Our proposal, like ETSI LI specifications, does not mandate how the internal LEA structure should be, but only that there should be a single communication point with the judicial system and NWOs. However, it is recommended that internal LEA communications are also secure, in order to guarantee the confidentiality, integrity, authentication and non-repudiation, and to prevent unauthorized information leaks, such as knowing whether a LEA is investigating a particular person.

The wiretap request (DWW_{rqst}) from the LI administrative department of the law enforcement agency (*LEA*) is sent to the judicial system (*JS*). This request contains at least the following information: the target network operator (NWO_{id}), all available information to identity the suspect (U_{name}), the data to be captured (CC_{type}) -e.g. the complete packet, including its application payload, or just its TCP/IP headers-, the requested wiretap duration (W_{time}), the address of the LEA monitoring facility where the captured data will be sent ($LEMF_{addr}$), including its public key to authenticate it, and the investigated case identifier (IC_{id}). The IC_{id} is employed as the LI Identifier (LIID) by all lawful interception systems to identify the captured data.

Thus it has to be globally unique, but it should not contain any meaningful structure, such as LEA or department identifiers, to avoid leaking information about the internal structure of the LEA to third parties. Finally, the DWW request should also include a detailed explanation by the LEA agents about why the DWW is requested, the kind of crime being investigated, the role of the suspect, any evidence against him, etc., so the judge can decide whether the DWW request has legal grounds, or it has to be rejected.

The LI administrative department of the judicial system performs the appropriate technical and administrative checks, and sends the DWW_{rqst} to the assigned judge. As in the LEA case, this proposal does not mandate any internal structure for the judicial system, although communications should be encrypted and digitally signed when possible. In this case, both the administrative department (*JS*) and the judge (*J*) have a public-private key pair to sign the DWWs, therefore it can also be leveraged to protect internal communications.

After evaluating the legal aspects of the wiretap request and approving it, the judge creates a digital wiretap warrant, $DWW = \{DWW_{NWO}, DWW_{LEA}\}$, and digitally signs each part with her private key. Previously, a pair of asymmetric keys is also generated by the judge per *Investigation Case* $<IC_{pub}, IC_{priv}>$. The purpose of these keys is to protect all information captured by the NWO with a symmetric key that is then encrypted with the public key of the case (IC_{pub}). Thus, such information can only be accessed by possessing the private key (IC_{priv}). Therefore the DWW_{NWO} part includes the public key of the case (IC_{pub}) in order to encrypt data, while the DWW_{LEA} part contains the private key (IC_{priv}) to decrypt such data. Moreover, this mechanism links the issued DWW to the whole interception process, as described later. By generating one key per case, instead of relying on some global LEA key, only the agents assigned to a case will be able to access to the seized information, and only when the judge provides them with the private key of the case ($DWW_{LEA}|IC_{priv}$).

The DWW_{NWO} is the only part of the digital wiretap warrant that the LEA will hand over to the suspect's network operator (NWO). It should contain at least all wiretap warrant details (WW) as in the ETSI eWarrant (ETSI, February 2012c), content (CC_{type}) and temporal limits (W_{start} and W_{end} times) of the wiretap, the case ID provided by the LEA (IC_{id}), LEA address and public key ($LEMF_{addr}$), a certificate with the IC_{pub} key signed by the judge, plus the certificate of the judge (J_{cert} containing J_{pub}) issued by the judicial system PKI.

The DWW_{LEA} contains the case ID (IC_{id}) and the private key of the investigated case (IC_{priv}) as a certificate signed by the judge. The key is provided to the LEA when the judge dictates, in order to permit the LEA to access the seized data.

This DWW proposal adheres to current ETSI specifications where the network operator (NWO) administrator knows the suspect being monitored, which LEA has requested the wiretap, as well as the particular judge that approved it. Besides, the LEA knows who the NWO of the suspect is. The DWW proposal could be adapted to a more anonymous scenario by modifying the request information and the certificates employed to sign them. For instance, when a LEA requests a DWW to the judicial system, the judge may ask the NWO to send the seized information to their own proxy systems, before reaching the LEMF (instead of directly to the LEA). This way the NWO cannot know which LEA is investigating its customer. Moreover, the judge may employ anonymous certificates, still issued by the judicial system PKI, so the NWO may know that a DWW is valid, but not who is the specific judge that approved it. However this is not just a technical decision, but the need of identifying all peers involved in a LI may be a requisite of the national legislation.

For simplicity, this description refers to a single user and a single network operator. However, in case there are several targets, or the suspect employs several NWOs, it is only necessary to generate a different DWW and LIID per user/NWO pair. This prevents different NWOs to be aware of each other, or knowing whether monitored users are associated or belong to different cases. Therefore, a multi-user/multi-provider LI scenario can be reduced to several single-user/single-provider scenarios running in parallel, which can later be integrated and correlated by the LEA.

At this point the LEA has a valid DWW (DWW_{NWO}), approved by an authorised judge, and it is now able to hand it over to the NWO in order to request the monitoring of all (or part) of the suspects communications.

The next paragraphs show the described message exchange and the main cryptographic operations[4]:

The *LEA* requests a DWW to Judicial System (*JS*) and Judge (*J*):

$$DWW_{rqst} = \{NWO_{id}, U_{name}, CC_{type}, W_{time}, LEMF_{addr}, IC_{id}\}$$
$$Sign_{LEA}DWW_{rqst} = sign_{LEA_{priv}}(DWW_{rqst})$$
$$Send_{LEA-JS}DWW_{rqst} = enc_{JS_{pub}}(\{DWW_{rqst}, Sign_{LEA}DWW_{rqst}\})$$

The Judicial System (*JS*) requests a timestamp ($Date_{global}$) to TSA_{global} as a receipt of the received information, and sends an acknowledgment back to the *LEA*:

$$TSA_{global}Sign_{LEA}DWW_{rqst} = tstamp_{TSA_{global-priv}}(Date_{global}, Sign_{LEA}DWW_{rqst})$$
$$Sign_{JS}TSA_{global}DWW_{rqst} = sign_{JS_{priv}}(\{Date_{global}, TSA_{global}Sign_{LEA}DWW_{rqst}\})$$
$$ACK_{JS-LEA}DWW_{rqst} = enc_{LEA_{pub}}(\{Date_{global}, TSA_{global}Sign_{LEA}DWW_{rqst}, Sign_{JS}TSA_{global}DWW_{rqst}\})$$

If the Judge (*J*) authorizes the LEA request, an Investigated Case (IC) key pair is generated $<IC_{pub}, IC_{priv}>$ and both parts of the DWW are signed to enable such LI:

$$DWW_{NWO} = \{WW, CC_{type}, W_{start}, W_{end}, LEMF_{addr}, IC_{id}, IC_{pub}, J_{cert}\}$$
$$DWW_{LEA} = \{IC_{id}, IC_{priv}, J_{cert}\}$$
$$Sign_JDWW_{NWO} = sign_{J_{priv}}(DWW_{NWO})$$
$$Sign_JDWW_{LEA} = sign_{J_{priv}}(DWW_{LEA})$$

[4] $enc_K(M)$ means encrypting message M with key K; $hash(M)$ means applying a cryptographic hash function over message M; $sign_K(M) = enc_K(hash(M))$ means digitally signing message M with key K; and $tstamp_K(D,S) = sign_K(D|S)$ means time-stamping signature S with date D by digitally signing the concatenation of date D and the signature S.

The *LEA* receives the DWW_{NWO} signed by the Judge (*J*) from the Judicial System (*JS*):

$$Sign_{JS-J}DWW_{NWO} = sign_{JS_{priv}}(Sign_{J}DWW_{NWO})$$
$$Send_{JS-LEA}DWW_{NWO} = enc_{LEA_{pub}} \times (\{DWW_{NWO}, Sign_{J}DWW_{NWO}, Sign_{JS-J}DWW_{NWO}\})$$

The *LEA* requests another timestamp ($Date'_{TSA_{global}}$) as a receipt of the DWWs reception. It sends an acknowledgment to Judicial System (*JS*):

$$TSA_{global}Sign_{JS-J}DWW_{NWO} = tstamp_{TSA_{global-priv}} \times \left(Date'_{global}, Sign_{JS-J}DWW_{NWO}\right)$$
$$Sign_{LEA}TSA_{global}DWW_{NWO} = sign_{LEA_{priv}} \times \left(\left\{Date'_{global}, TSA_{global}Sign_{JS-J}DWW_{NWO}\right\}\right)$$
$$ACK_{LEA-JS}DWW_{NWO} = enc_{JS_{pub}}\left(\left\{Date'_{global}, TSA_{global}Sign_{JS-J}DWW_{NWO}, Sign_{LEA}TSA_{global}DWW_{NWO}\right\}\right)$$

The *LEA* sends the DWW_{NWO} to the suspect's Network Operator (*NWO*). It receives as acknowledgement a third timestamp from the *NWO*, which was previously requested to TSA_{global}:

$$Sign_{LEA-J}DWW_{NWO} = sign_{LEA_{priv}}(Sign_{J}DWW_{NWO})$$
$$Send_{LEA-NWO}DWW_{NWO} = enc_{NWO_{pub}}(\{DWW_{NWO}, Sign_{J}DWW_{NWO}, Sign_{LEA-J}DWW_{NWO}\})$$
$$TSA_{global}Sign_{LEA-J}DWW_{NWO} = tstamp_{TSA_{global-priv}} \times \left(Date''_{global}, Sign_{LEA-J}DWW_{NWO}\right)$$
$$Sign_{NWO}TSA_{global}DWW_{NWO} = sign_{NWO-priv} \times \left(\left\{Date''_{global}, TSA_{global}Sign_{LEA-J}DWW_{NWO}\right\}\right)$$
$$ACK_{NWO-LEA}DWW_{NWO} = enc_{LEA_{pub}} \times \left(\left\{Date''_{global}, TSA_{global}Sign_{LEA-J}, Sign_{NWO}TSA_{global}DWW_{NWO}\right\}\right)$$

The administrative department of the NWO that handles LI requests validates the DWW_{NWO} sent by LEA, both at technical (e.g. checking the cryptographic signatures) and regulatory levels (e.g. checking the jurisdiction of the judge and the LEA), and asks for further details if necessary, as it is done today with paper wiretap warrants, although certain automatic checks are now possible.

Communications interception by NWO. Hand over to LEA

Before explaining the technical details of how communication interception is performed and secured, it is necessary to discuss some aspects of the network operator (NWO) role, and the importance of the Monitoring Station (MS).

Monitoring Station (MS)

Most interception functions, including the CC Trigger Function (CCTF) and the IRI Internal Interception Function (IRI-IIF), heavily depend on the inner workings of the NWO (i.e. internal topology and user session management, respectively), and thus are difficult to standardize. Instead, this paper is focused on the CC Internal Interception Function (CC-IIF), which performs the data capturing process itself (i.e. sniffing IP packets), and thus it is much easier to employ standard devices. ETSI LI does not specify whether the CC-IIF should be implemented in a NWO network node or as a separate, dedicated device that receives a copy of the traffic to be captured. The former reduces the LI deployment cost, whereas the latter simplifies management and network upgrades. For simplicity, we call *Monitoring Station* (MS) to the ETSI CC-IIF element, independently of how it is implemented (either as a separate element or integrated in a NWO router). The monitoring station is a key element of the DWW proposal, since it enables the following features:

Enforcement of DWW. The monitoring station must only be able to capture the communications of a suspect if it has been enabled by a valid digital wiretap warrant, which specifies the type of contents to be captured and its temporal limits.

End-to-end privacy. All captured information is encrypted before leaving the monitoring station using the public key of the case (IC_{pub}). The only way to access such information is by means of the private key of the case (IC_{priv}) generated by the judge. Therefore, not even the NWO is able to peek into the captured data.

Secure chain of custody. Monitoring stations timestamp and sign capture files in order to trace back all digital evidence, as well as to link it with a particular DWW. This may be essential during a trial to ensure that evidence has not been tampered and that it was captured at the claimed time.

Misuse of LI framework. In most countries, NWO must deploy LI infrastructure by law, and in some cases the government may fund part of the investment. Therefore, this infrastructure must be employed for legal interception purposes only, avoiding any kind of misuse, either from unauthorized users or by the NWO itself (i.e. to monitor the traffic exchanged by its customers), even if monitoring stations are managed by NWO staff.

Therefore, in order to improve the lawful interception security, the DWW proposal only requires adding certain features to this monitoring device, because it is the key element of the DWW data path. However, as far as it is certified for LI, the monitoring stations can be manufactured by any vendor, and thus the NWO can freely choose the MS best suited for its network. The most important features of a DWW-certified monitoring station are the cryptographic functions (digital signing, secure random number generation, and symmetric key generation), performed by a Hardware Security Module (HSM) such as (Thales nShield Solo hardware security module, 2015). The HSM is the only MS subsystem not managed by the NWO but by the judicial system. Therefore, in order to be trusted, it has to be tamper-proof (i.e. physical access to the HSM should be controlled with seals). The HSM may be owned by the judicial system itself for greater security, or any certified HSM may be installed by the NWO for greater flexibility.

Each monitoring station has an asymmetric key pair $<MS_{pub}, MS_{priv}>$, generated by the HSM itself, as well as a unique serial number (MS_{id}). Before deploying it, a technician from the judicial system or other auditing agency certifies the

monitoring station by signing the MS_{pub} key (MS_{priv} must never leave the HSM). The signed MS_{pub} key is given to the NWO as a certificate issued by the judicial system, so the LI department of the NWO is able to verify the validity of the certificate (e.g. if it has been revoked or it has expired), and the public key can be employed to send private information to a given monitoring station. The JS technician also installs the public root certificate of the judicial systems PKI, in order to allow the HSM to validate the DWWs from authorized judges, as well as his/her own public key (JS_{tech}) signed by the judicial system. After the initial deployment, as any other certified equipment like gas pumps, monitoring stations should be subject to periodic reviews by auditors from the judicial system who check that the seals of the monitoring station have not been broken and that the HSM only contains the original keys and trusted certificates, as well as updating the MS revocation list with invalid certificates (if any).

Once this certification procedure is in place, the NWO is able to verify whether the monitoring station is working properly (i.e. the certificate has not been revoked or expired), but it cannot tamper the captured data because the HSM private key of the monitoring station (MS_{priv}) is unknown even to the JS, and it is not able to re-generate a new key (MS_{pub}) because it would not be signed by the judicial system. In any case, both the physical and logical access to monitoring stations should be restricted to a minimum set of trusted people, ideally from the LI department of the NWO and the JS.

Obviously, the NWO could still somehow tamper the data before being captured by the monitoring station, such as filtering some traffic (to avoid being captured), changing the clock of the monitoring station to corrupt the time-stamps or disable the capture altogether (i.e. if the time is outside the DWW limits), or by dropping the captured data sent by the monitoring station. There are some partial solutions to these problems (i.e. chained signatures and hierarchical TSA) that will be described later, so once a LI capture is performed it is not possible to delete it and deny that it was performed.

In summary, the proposed monitoring station allows the LI system to be more secure, while minimizing the effect on the internal operations of the NWO. Now that the procedures to guarantee a certain security level for the monitoring station are clear, let us describe the exchange of information between the NWO and the LEA, once the judge has signed the DWW.

Lawful Interception of a communication

The NWO uses the information about the suspect inside the DWW_{NWO} to look for the identifiers of that specific customer. The IRI Internal Intercept Function (IRI-IIF) and the CC Trigger Function (CCTF) elements defined by ETSI LI are employed to decide when and where a legal interception should be initiated. For instance the targeted user may have an xDSL subscription, which may be monitored continuously by a MS in the local DSLAM. Although the suspect may also connect to a WiFi hotspot in a different place, involving a separate monitoring station that must only capture data when that particular data session is active. Therefore, it is not possible to add any further technical information (like the user's IP address or a static MS identifier) to the DWW in order to further restrict what data should be captured, because such technical data may be highly dynamic (i.e. a dynamic IP address or a mobile user connecting to different hotspots). Instead, the appropriate CC Internal Intercept Function (CC-IIF)/Monitoring Station (MS) can be selected dynamically, and it should receive the technical information to perform the capture (i.e. the IP address assigned by the DHCP server to the user) from the CCTF, together with the DWW_{NWO} that authorizes such interception. All data captured by the MS is sent to the mediation function (MF), which merely acts as a proxy. The investigation case identifier (IC_{id}) of the DWW_{NWO} warrant allows the MF to send the intercepted information to the appropriate LEA ($LEMF_{addr}$). In general, a MS that receives a DWW_{NWO} performs the following steps:

1. It first checks the signature of the DWW_{NWO} by means of the judge's public certificate (J_{pub}). The MS checks that this certificate is valid using the public root certificate of the judicial system (pre-installed in all MSs HSMs).
2. The HSM of the MS generates a new random session key (K) that is employed by a symmetric cipher to encrypt all captured information during a specific pre-configured amount of time (e.g. the whole data session, one hour, etc.). This key is then encrypted with the public key of the case: $enc_{ICpub}(K)$. If we assume that the certification process is reliable, and thus that the monitoring station is a trusted device that cannot be externally manipulated to obtain K or affect its generation, only the ones with the private key of the case (IC_{priv}) are able to obtain K, and thus to access the captured data in clear text. The usage of a symmetric key protected with the asymmetric key of the investigated case has additional benefits due to the higher performance of symmetric ciphers. For instance, if a suspect is being monitored by two LEAs, which should not be aware of each other due to security reasons, the monitoring station can just encrypt and send the captured data once to the MF, and then it is only necessary to encrypt the symmetric key twice, using the IC_{pub} keys of each LEA case.
3. The intercepted contents of communication (CC) data, as defined by the CC_{type} field in the DWW_{NWO}, are signed and time-stamped to enable a proper chain of custody. The signature is performed using the private key of the monitoring station (MS_{priv}), which is securely stored at its HSM, whereas the timestamp comes from a local time-stamping authority (TSA_{NWO}) that must send these timestamps to the TSA_{global} periodically, in order to avoid MSs connecting directly to the TSA_{global}. Direct MS-TSA_{global} connections may require excessive changes in the NWO infrastructure or be non-compliant with NWO corporate policy or national legislation. To limit desynchronization and other attacks (e.g. information deletion, forgery of NWO clock, etc.) a number of precautions in the interactions between TSA_{NWO} and TSA_{global} are considered. It is important to remember that each monitoring station relies on current time for several operations, such as deciding whether a certificate is still valid, when to start/stop a LI capture as

defined in the DWW, and specially in order to timestamp the captured data, which may be essential evidence in some trials (e.g. the suspect knew certain information before the crime was made public).

The local TSA_{NWO} should be also certified and audited by JS technicians, and any unauthorised modification should lead to a criminal investigation. However, since it provides dynamic information, let us assume that it may be temporarily subverted by the NWO but then restored before the next JS audit. In order to prevent this, it should send every T seconds a summary of all received time-stamping requests during that period to the TSA_{global}, which is no longer under control of the NWO, that time-stamps and logs them:

$$Send_{MS-TSA_{NWO}} HashCC_{data1} = hash(CC_{data1})$$

$$Send_{TSA_{NWO}-MS} TSA_{NWO} CC_{data1} = \Big\{ Date_{NWO}, tstamp_{TSA_{NWO-priv}} \times (Date_{NWO}, hash(CC_{data_1})) \Big\}$$

$$Send_{TSA_{NWO}-TSA_{global}} TSA_{NWO} CCs = \Big\{ tstamp_{TSA_{NWO-priv}} \times (Date_{NWO}, hash(CC_{data1})), tstamp_{TSA_{NWO-priv}} \times (Date'_{NWO}, hash(CC_{data_2})), \ldots \Big\}$$

After obtaining a timestamp from the TSA_{NWO}, the MS can send the captured information to the MF. We consider two possible modes of operation: Block Mode and Packet Mode.

In *Block Mode* (BM) the captured information is not sent to the LEA until some size or time threshold (e.g. 10 MB or 1 h) is reached:

$$CapturedBlock = enc_K(CC)$$

$$AnonymousMS_{id} = enc_{JS_{tech}}(\{nonce, enc_{nonce}(MS_{id})\})$$

$$BlockMetaInfo = \Big\{ enc_{IC_{pub}}(K), Block_{id}, Block_{counter}, IC_{id}, AnonymousMS_{id}, hash(CapturedBlock) \Big\}$$

$$Sign_{MS} BlockMetaInfo = sign_{MS_{priv}}(BlockMetaInfo)$$

$$TSA_{NWO} BlockMetaInfo = tstamp_{TSA_{NWO-priv}} \times (Date_{NWO}, Sign_{MS} BlockMetaInfo)$$

$$SendCapturedBlock_{MS-LEA} = \Big\{ CapturedBlock, BlockMetaInfo, Sign_{MS} BlockMetaInfo, Date_{NWO}, TSA_{NWO} BlockMetaInfo \Big\}$$

In *Packet Mode* (PM) each packet is sent in real time to the LEA:

$$SendCapturedPacket_{MS} = \{enc_K(CC), Block_{id}\}$$

However, in order to protect packet integrity in Packet Mode, every $packets_{num}$ packets a new "virtual block" (*VBlock*) starts, generating a new key for the next "virtual block" and signing the previous one with its hash chain:

$$VBlockMetaInfo = \Big\{ enc_{IC_{pub}}(K), Block_{id}, Block_{counter}, IC_{id}, AnonymousMS_{id}, CCHashChain \Big\}$$

$$Sign_{MS} VBlockMetaInfo = sign_{MS_{priv}}(VBlockMetaInfo)$$

$$TSA_{NWO} VBlockMetaInfo = tstamp_{TSA_{NWO-priv}} \times (Date_{NWO}, Sign_{MS} VBlockMetaInfo)$$

$$SendVBlock_{MS} = \Big\{ VBlockMetaInfo, Sign_{MS} VBlockMetaInfo, Date_{NWO}, TSA_{NWO} VBlockMetaInfo \Big\}$$

The meaning of the previous parameters is as follows:

$enc_K(CC)$: Captured Content of Communication (CC), either a single packet (in PM) or a whole block (in BM), encrypted with symmetric session key K.
$Block_{id}$: It numerates the block or specifies that the packet belongs to a specific block. Its initial value is random and it is increased by every new block generated by the MS, independently from the active investigation cases or LEAs. This prevents a LEA knowing if other LEAs are investigating the same suspect at the same time. A MS can send blocks or packets from different interceptions associated to different LEAs using the same $Block_{id}$.
$Block_{counter}$: Block counter per interception of each LEA in this MS. It is incremented by 1 each new block. It allows the LEA detecting missing blocks.
$AnonymousMS_{id}$: In order to hide the NWO's topology, the MS identifier could be hidden from LEAs, but be still accessible by the judicial systems auditors. The MS_{id} can be encrypted with a random number (*nonce*) generated for every block that acts as the key. This encryption prevents a LEA knowing if two different blocks come from the same monitoring station. Only the judicial authority is able to know the real MS identifier (MS_{id}), when it wants to validate some evidence (with the private key of JS_{tech}).
CCHashChain: This allows securely chaining the packets, to send only one digital signature every $packets_{num}$ packets in order to protect them all. It also allows identifying dropped or corrupted packets, because, unless all packets are received correctly, the combined signature will not match (Table 1).

In each operation mode there are general CC information and meta-information. Only Meta-information is associated with a specific LEA. This allows the same CC to be delivered to different LEAs without knowing that there are other involved LEAs. The MS sends all this information to the MF which separates and delivers it to the appropriate LEA using the IC_{id}.

Table 1
Hash-chain of consecutive packets.

$CC_1 = enc_K(packet_1)$	$CC_1Hash = hash(CC_1)$
$CCHashChain = CC_1Hash$;	
$CC_2 = enc_K(packet_2)$	$CC_2Hash = hash(CC_2)$
$CCHashChain = hash(CCHashChain \vert CC_2Hash)$;	
$CC_n = enc_K(packet_n)$	$CC_nHash = hash(CC_n)$
$CCHashChain = hash(CCHashChain \vert CC_nHash)$;	

Finally, it is worth noting that although the above description has been focused on the captured Content of Communication (CC), because it is the one with more stringent performance requirements, the same mechanisms can be employed to protect Intercept Related Information (IRI) by applying the proposed changes to the MS to the IRI IIF function that handles communication metadata. Furthermore, the two modes of operation allow this DWW proposal to be employed with other technologies considered by ETSI LI beyond IP-based communications. For instance Packet Mode can be also applicable to layer 2 data communications (e.g. Ethernet VPNs), whereas Block Mode is more appropriate for application-layer services that exchange complete messages like e-mail.

For additional security, the communication channel between the NWO (MF) and the LEA ($LEMF_{addr}$) should be also based on IPSec or TLS, which may be employed to convey both, the CC and the IRI from a single case, or even from multiple cases, since each case is uniquely identified (IC_{id}).

Once the information has arrived to a LEA, it also asks for a secure timestamp in order to acknowledge the reception of such information. As in the NWO case, the LEA may deploy its own Time Stamping Authority (TSA_{LEA}), and just send all locally-signed records to the global TSA (TSA_{global}) periodically (as described for the TSA_{NWO}). At the end of this process, the LEA stores in a database, for further analysis, the information shown in Table 2. For simplicity, it only shows /tone CC block, from a single MS.

Since seized information may be later employed as digital evidence, all captured data should also be archived into some secure, off-line, long-term storage, like backup tapes, abiding all appropriate data retention laws. Notice that, since all captured data is still in an encrypted form, it can (and should) be handled by a LEA department different to the one performing the investigation. For instance, backup tapes may be stored by the LI administration department of the LEA and/or the judicial system one. The LEA can only process the intercepted data when the judge sends it the DWW_{LEA} warrant:

$$Sign_{JS-J}DWW_{LEA} = sign_{JS_{priv}}(Sign_{J}DWW_{LEA})$$
$$Send_{JS-LEA}DWW_{LEA} = enc_{LEA_{pub}}(\{DWW_{LEA}, Sign_{J}DWW_{LEA}, Sign_{JS-J}DWW_{LEA}\})$$

The administrative department of the LEA receives the DWW_{LEA} from the judge. It contains the private key of the case (IC_{priv}) that should be distributed internally only to the team of agents investigating that particular case. Since anyone with access to the key may access the captured information, the LEA should also employ secure mechanisms to convey this information locally in an encrypted form (i.e. using the public keys of the agents).

DWW threat model

The Digital Wiretap Warrant (DWW) proposal guarantees confidentiality, integrity, timeliness and authenticity of the exchanged information end-to-end, by means of public key cryptography and digital signatures (i.e. PKI and TSA). The Monitoring Station (MS) is able to check whether the DWW is valid (i.e. signed by an authorized judge) before it starts capturing any data. Also a forensic expert can certify the source MS of any evidence during a trial. Additionally, the DWW framework defines a key distribution protocol for the symmetric keys employed to encrypt the captured information (i.e. $enc_{ICpub}(K)$), which are also protected end-to-end. Thus, the Network Operator (NWO) cannot peek into the captured data, even when it traverses its Mediation Function (MF) proxy, but only the Law Enforcement Agency (LEA) agents that know the private key of the case (IC_{priv}). Secure logging and timestamping enables auditing by registering who did what and when all operations were performed. Moreover, the extensive usage of digital signatures provides non-repudiation properties to most inter-organization operations.

Therefore, the DWW proposal defines security mechanisms against all general security attacks specified by ETSI, including denial of service and sabotage, as analysed later. Furthermore, the DWW proposal also considers advanced attacks that are specific to LI platforms, such as evidence fabrication or tampering, even in confabulation scenarios.

Evidence fabrication, tampering and deletion

The DWW proposal has been designed so that it is very hard to fabricate or tamper evidence once it has been delivered to the LEA (i.e. the NWO may be able to delay or delete data while on transit by controlling the MS communications, although those attempts may still be detected by auditing the MS/TSA logs). Once registered by the LEA, they are protected even if the NWO and the LEA confabulate, unless the Judicial System and the global

Table 2
Information about captured data (one block) stored by the LEA.

Content of Communication (CC):	
$CapturedBlock$	$enc_K(CC)$
CC Meta Information:	
$BlockMetaInfo$	$\{enc_{IC_{pub}}(K), Block_{id}, Block_{counter}, IC_{id}, AnonymousMS_{id}, hash(CapturedBlock)\}$
$Sign_{MS}BlockMetaInfo$	$sign_{MS_{priv}}(BlockMetaInfo)$
$Date_{NWO}$	When the *MS* captured the CC
$TSA_{NWO}BlockMetaInfo$	$tstamp_{TSA_{NWO-priv}}(Date_{NWO}, Sign_{MS}BlockMetaInfo)$
TSA_{LEA}:	
$Date_{LEA}$	When *LEA* received the captured CC
$TSA_{LEA}BlockMetaInfo$	$tstamp_{TSA_{LEA-priv}}(Date_{LEA}, Sign_{MS}BlockMetaInfo)$

time-stamping authority (TSA_{global}) also cooperate with them.

Evidence fabrication or tampering: All seized data is digitally signed by the monitoring station that captured it. Therefore, unless the monitoring station is compromised (e.g. the MS_{priv} key is extracted from the HSM), such information cannot be modified later on. Even if the NWO is able to feed the MS with any traffic it wants, the information must be time-stamped by the TSA_{NWO} and TSA_{global} (and thus logged). Therefore, it is not possible to change the evidence date to the past, and in any case the attack can only be performed before the DWW time limit is over.

Deleting evidence: Even though all elements of the LI platform should be accessed by authorized personnel only, somebody (by being blackmailed or bribed) may try to sabotage/delete some key evidence, as well as the local logs of the system to hide his steps. Therefore, some trusted third party is necessary to log what information was exchanged and when. In particular, the time-stamping authorities (TSAs) securely log all information (i.e. its hash) that has been time-stamped. Therefore, by auditing TSA_{global} logs, it would be possible to know the last system (e.g. the MF or LEMF) that received certain missing information, and therefore corner the perpetrator.

Therefore, TSAs are also key elements of the DWW proposal and thus, they should be certified and the LI information shown in Table 3 should be securely logged and backed up.

Once the captured data arrives to the LEA and it is backed-up in different places, deleting all copies of some evidence would be quite challenging. Therefore, the most vulnerable time is when the captured data is in transit. For instance, some NWO operator may try to drop some of the captured data (because dropping it all could be easily detected by the LEA). But even in that case the NWO or LEA may notice that some block or set of packets is missing because blocks are sent periodically (even if empty) or due to the proposed hash chaining mechanism explained previously.

Denial of service attacks and off-line communications

Like the ETSI LI architecture, the DWW proposal clearly identifies the interfaces between elements of the LI system. In particular there are a limited number of points where inter-organization communications take place, and in most cases they involve proxies that hide internal elements. For instance, monitoring stations do never communicate with other elements outside the NWO network. Captured data is sent to the LEA through the MF proxy, and timestamps are obtained from the local TSA_{NWO}. Therefore, it should be more difficult to target internal elements by external attackers, because only the intermediate systems are accessible, which are fewer and thus easier to protect. Moreover, even if public networks like Internet are employed for inter-organization communication, the topology is fairly static in the sense that there are a small number of organizations (i.e. a single national Judicial System, few LEAs and several NWOs) that have long-term relationships. Therefore, it is reasonable to build a Virtual Private Network (VPN) with mutual authentication, like IPSec, between NWOs and LEAs, as well as between the TSA_{global} and TSA_{NWO}/TSA_{LEA}, and filter the traffic from any other source. However, if the attacker knows the public IP address of the NWO or LEA mediation function, it still can try to flood its upstream link or network, albeit such kind active attack will be easily detected and acted upon.

Finally, an additional benefit of the end-to-end encryption and explicit time-stamping of the DWW proposal is that inter-organization communications may be easily performed off-line, whereas the current ETSI specification implicitly assumes that captured traffic is sent to the LEA in real time (and thus the capture time is roughly the same as when received by the LEA). On the contrary, in a DWW-enabled LI system captured traffic can be securely stored by any intermediate element until communications are restored, since it is encrypted and time-stamped at capture time. Therefore, a sustained DoS attack may delay when LEAs receive captured data, but it will eventually arrive (e.g. in a hard disk delivered in a courier van). The only subsystem that requires some real-time performance is the TSA hierarchy, and thus TSA_{global} is an important element that should be protected accordingly. Moreover, if TSA_{NWOs} and TSA_{LEAs} are properly certified, they can even work independently of TSA_{global} during limited periods of time.

Technical limitations of the DWW framework

Currently, ETSI LI standards are based on the administrative trust among domains, and especially on the NWO side. The DWW platform fixes the problems derived from trusting in domains that could be corruptible or subverted. Only the new features introduced into each monitoring station could be considered truly intrusive, but they are necessary for enhancing the aimed security, privacy and civil rights guarantees. Although it tries to minimize the trust in the NWO, there are some problems that do not have practical technical solutions, without severely interfering with the NWO infrastructure. For instance, a NWO can inject traffic, modify or eliminate it before reaching the monitoring station, so even a fully trusted MS HSM cannot

Table 3
Information stored by the global Time Stamping Authority (TSA_{global}).

Name of TSA_{global} record	Content of TSA_{global} record ($+Date_{global}$)
$TSA_{global}Sign_{LEA}DWW_{rqst}$	$tstamp_{TSA_{global-priv}}(Date_{global}, Sign_{LEA}DWW_{rqst})$
$TSA_{global}Sign_{JS-J}DWW_{NWO}$	$tstamp_{TSA_{global-priv}}(Date_{global}, Sign_{JS-J}DWW_{NWO})$
$TSA_{global}Sign_{LEA-J}DWW_{NWO}$	$tstamp_{TSA_{global-priv}}(Date_{global}, Sign_{LEA-J}DWW_{NWO})$
List of $TSA_{NWO}BlockMetaInfo$	$tstamp_{TSA_{NWO-priv}}(Date_{global}, Sign_{MS}BlockMetaInfo)$
List of $TSA_{LEA}BlockMetaInfo$	$tstamp_{TSA_{LEA-priv}}(Date_{global}, Sign_{MS}BlockMetaInfo)$

identify or solve this situation (nor current WW-based LI platforms). However, these measures seem quite sophisticated compared to just telling the suspect that is been monitored so he does not send any incriminating traffic. Therefore, LI operations (either WW- or DWW-based ones) must be always handled by a small set of trusted NWO personnel.

Due to the dynamic nature of monitoring, a NWO could modify the CCTF and/or MF functions to try to target a different user with a valid DWW issued for another suspect. However, since the MS encrypts all captured traffic, the NWO won't be able to access this information, unless it is able to compromise the security of the certified MS HSM. Therefore, although a NWO can still deploy additional equipment to spy its customers, it can no longer abuse the DWW-enabled, mandatory LI infrastructure for any illegal purposes.

Evaluation of the DWW framework

This section first analyses the dimensioning of the DWW databases that store all seized data and the logs of each investigation case. Tables 4–6 show the analytical expressions to calculate the total size of the LEA and

Table 4
Size of TSA_{global} logs per investigation case.

Size of each TSA_{global} log entry:	
Date (64 bits timestamp)	8 bytes
Digital signature (Padded RSA 2048)	256 bytes
Size of 3 log entries for administrative exchanges (LEA-JS, JS-LEA, LEA-NWO)	$3*(8+256)$ bytes
Size of logs for timestamped data ($TSA_{NWO} - TSA_{global}$ and $TSA_{LEA} - TSA_{global}$)	$2*(NumBlocks)*(8+256)$ bytes $NumBlocks = CCSize/N$ bytes $CCSize$: Total size of captured data N: Size of each Block (Block Mode) or VBlock of $packets_{num}$ (Packet Mode)
Total size of TSA_{global} logs	$(3+2*NumBlocks)(8+256)$ bytes $= 792 + 528*NumBlocks$ bytes

Table 5
Size of LEA database per investigation case using Block Mode.

Block Mode Database		
$CapturedBlock$	$enc_K(CC)$	N bytes
$BlockMetaInfo$	$enc_{IC_{pub}}(K)$	256 bytes
	$Block_{id}$	8 bytes
	$Block_{counter}$	8 bytes
	IC_{id}	16 bytes
	$Block_{id}$	8 bytes
	$enc_{JS_{tech}}(\{nonce,$	
	$enc_{nonce}(MS_{id})\}$	256 bytes
	$hash(CapturedBlock)$	32 bytes
$Sign_{MS}BlockMetaInfo$	$sign_{MS_{priv}}(BlockMetaInfo)$	256 bytes
$Date_{NWO}$		8 bytes
$TSA_{NWO}BlockMetaInfo$	$tstamp_{TSA_{NWO-priv}}(Date_{NWO}, Sign_{MS}BlockMetaInfo)$	256 bytes
Total size per block of N bytes		$N + 1096$ bytes
Total size per investigated case		$NumBlocks*(N+1096)$ bytes
Security overhead		$NumBlocks*1096$ bytes

Table 6
Size of LEA database per investigation case using Packet Mode.

Packet Mode Database		
$SendCapturedPacket_{MS}$	$enc_K(CC)$	M bytes
(CC: single packet)	$Block_{id}$	8 bytes
$N = packets_{num}*packet_{\overline{size}}$	$packet_{\overline{size}} = M$	$N + 8*packets_{num}$
$V\ BlockMetaInfo$	$enc_{IC_{pub}}(K)$	256 bytes
	$Block_{id}$	8 bytes
	$Block_{counter}$	8 bytes
	IC_{id}	16 bytes
	$enc_{JS_{tech}}(\{nonce, enc_{nonce}(MS_{id})\}$	256 bytes
	$CCHashChain$	32 bytes
$Sign_{MS}V\ BlockMetaInfo$	$sign_{MS_{priv}}(V\ BlockMetaInfo)$	256 bytes
$date$		8 bytes
$TSA_{NWO}VBlockMetaInfo$	$tstamp_{TSA_{NWO-priv}}(Date, Sign_{MS}V\ BlockMetaInfo)$	256 bytes
Total V Block size of $packets_{num}$ packets of M bytes on average		$N + 8*packets_{num} + 1096$ bytes
Total size per investigated case		$NumBlocks*(N + 8*packets_{num} + 1096)$ bytes
Security overhead		$NumBlocks*(8*packets_{num} + 1096)$ bytes

TSA_{global} logs per investigation case. In our calculations, we suppose AES-256 for symmetric encryption, SHA-256 for hashing and RSA-2048 for signing. With these expressions, Table 7 provides some storage size and overhead values for an example scenario.

Finally, Table 8 shows the cryptographic operations executed by the MS to protect the captured data in a DWW-enabled LI platform. The sustained throughput of the MS is limited by the performance of the symmetric encryption of captured data and the size of the blocks to be signed, which define the number of asymmetric operations.

In order to validate the feasibility of the proposed security mechanisms, Fig. 3 shows the performance of the whole data protection process, both in Block and Packet Modes, implemented in Java with its standard Cryptographic API, and executed in an off-the-shelf sever featuring two Intel Xeon E5420 processors (with 4×2.50 GHz cores) and 8 GB of RAM. The throughput has been computed by measuring the time to encrypt and sign blocks of the specified sizes (or 512 bytes-long packets and their associated VBlocks) 100 times and then computing the average block processing time and resulting throughput. Each experiment has been repeated 5 times with different data in order to obtain a 95% confidence interval.

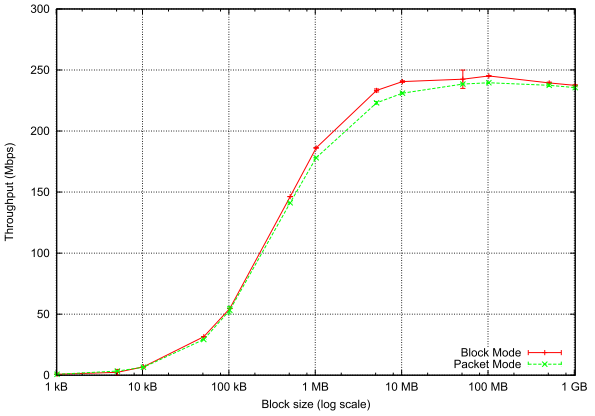

Fig. 3. Performance of block and packet encryption for different block sizes.

Clearly, the size of the block has a significant impact on the performance of the monitoring station, because of the asymmetric operations that have to be performed to sign each block. But even with this proof-of-concept, non-optimized software implementation, a monitor station using 10 MiB blocks should be able to encrypt data at 240 Mbps or 231 Mbps, in Block and Packet Modes

Table 7
Approximate overhead to capture 8 GiB ($=8*2^{30}$ bytes) from a suspect.

Parameters		
$CCSize$	8 GiB	
$packet_{\overline{size}}$	512 bytes (on average)	
N	10 MiB (Block Mode) or 20 480 packets * $packet_{\overline{size}}$	
$NumBlocks = CCSize/N$	820 blocks	
Database size	Block Mode	Packet Mode
TSA_{gobal}	$792 + 528{*}NumBlocks = 433\ 752 = 423$ KiB	$792 + 528{*}NumBlocks = 433\ 752 = 423$ KiB
LEA	$NumBlocks{*}(N{+}1096) = CCSize + NumBlocks\ {*}1096 = CCSize + 877$ KiB	$NumBlocks{*}(N + 8{*}packets_{num} + 1096) = CCSize + 129$ MiB
LEA overhead	0.01045%	1.5747%

Table 8
Cryptographic operations of Monitoring Station for protecting the captured data.

Block Mode	Cryptographic operations
$enc_K(CC) \rightarrow t = (N/256$ bits)	t symmetric encryptions
$enc_{IC_{pub}}(K)$	1 asymmetric encryption
$enc_{JS_{tech}}(\{nonce, enc_{nonce}(MS_{id})\})$	1 symmetric encryption + 1 asymmetric encryption
$hash(CapturedBlock)$	1 hash
$Sign_{MS_{priv}} BlockMetaInfo$	1 hash + 1 asymmetric encryption
Total operations per Block:	$(t + 1)$ symmetric encryptions + 3 asymmetric encryptions + 2 hashes
Packet Mode	Cryptographic operations
Per packet:	
$enc_K(CC) \rightarrow p = packet_{\overline{size}}/256$ bits	p symmetric encryptions
$CCHashChain$	1 hash
Per Virtual Block of $packets_{num}$:	
$enc_{IC_{pub}}(K)$	1 asymmetric encryption
$enc_{JS_{tech}}(\{nonce, enc_{nonce}(MS_{id})\})$	1 symmetric encryption + 1 asymmetric encryption
$CCHashChain$	1 hash
$Sign_{MS_{priv}} VBlockMetaInfo$	1 hash + 1 asymmetric encryption
Total operations per VBlock:	$packets_{num}{*}(p$ symmetric encryptions + 1 hash) + 3 asymmetric encryptions + 1 symmetric encryption + 1 hash

respectively. The lower performance of Packet Mode is due to the additional hash operations performed for the hash chaining of packets. Moreover, by executing seven Java processes in parallel in our test server (leaving the 8th core for other processes), a sustained throughput of 1.65 Gbps in block mode (i.e. 236 Mbps per core) has been achieved. Furthermore, these results should be considered just a lower performance bound. Optimized software implementations in microprocessors with AES-NI instructions support cipher/decipher speeds in the order of 4 GB/s (32 Gbit/s) (TrueCrypt— hardware acceleration, 2014).

The minimum block size to be employed is limited by the number of asymmetric operations performed by the Hardware Security Module (HSM). Recent studies show that at least hundreds of asymmetric operations per second for RSA-2048 are feasible. For instance, the Thales nShield Solo PCIe 6000 (Thales nShield Solo hardware security module, 2015) is able to execute 3000 asymmetric operations per second. As the monitoring station performs 3 asymmetric operations per block or every $packets_{num}$ packets, then it is able to process 1000 blocks per second (or 1000*$packets_{num}$). Thus, a 10 Gbps link requires blocks of 10Mbits (1.25 MB or higher) or 2441 packets of 512 bytes in average. Therefore, we consider that our proposal is able to work in high-speed links employing commercial, off-the-shelf HSM devices.

The major cost of deploying the proposed LI solution would be adding HSMs to existing monitoring stations and the (optional) certification and auditing process of such DWW-enabled monitoring stations. Since the same procedures and elements of the ETSI LI architecture are maintained, the impact of deploying the rest of the DWW framework should be quite limited. In particular our proposal only requires deploying additional tools and services to be employed by current LI personnel in the NWO, LEA and judicial system. Therefore, apart from the training in the new tools, the remaining costs may come from the new standard security services like public key infrastructures (PKIs) and time stamping authorities (TSAs). However, we do consider that most organizations might have already deployed such PKI and TSA services, since they are useful for many other purposes beyond secure lawful interception.

Conclusions and future work

This paper proposes the so-called Digital Wiretap Warrant (DWW) to enhance the security and privacy of Lawful Interception (LI) specifications employed nowadays, while maintaining all existing procedures and human supervision. In particular, the DWW proposal is fully compatible with current ETSI LI requirements and specifications, albeit it expands them in a number of ways.

First of all, by turning paper-based wiretap warrants into digital documents, it is now possible that all elements of the LI infrastructure verify, by means of cryptographic signatures, whether a given capture session has been approved by an authorized judge. Moreover, a DWW-enabled monitoring station signs and encrypts all captured data end-to-end, so only the law enforcement agency that requested the DWW is able to decrypt it; as opposed to the current practice of encrypting the captured data hop-by-hop, where any intermediate node of the network operator is able to alter or peek into such data.

The DWW proposal also improves the chain of custody of digital evidence by securely signing and time-stamping all captured data. This is enabled by certified monitoring stations with hardware security modules, and a hierarchy of timestamp authorities, which guarantee that seized evidence has not been fabricated, tampered or silently deleted, even in confabulation scenarios.

Moreover, since the global Time Stamping Authority (TSA) is a third party that oversights all messages exchanged by the LI platform, including the data plane ones, it may be also employed for improved LI auditing. Nowadays Lawful Interception is subject to public scrutiny by requiring the Judicial System to publish periodically the number of wiretap requests by how many agencies, affecting how many suspects, etc. Currently this information is collected at administrative level. Our proposal maintains the current administrative auditing practices, but it enables advanced auditing by collecting also technical data such as the number of active warrants, their durations, the number of captured data blocks, etc. This technical data can be then correlated with the statistics gathered at the administrative level to check any kind of mismatch that may require further probing. This enhanced auditing process will be studied in future works.

The deployment costs and scalability of the proposed DWW framework and its encryption mechanisms have been evaluated qualitatively, but also quantitatively using a proof-of-concept software encryption implementation. It has been concluded that the proposed DWW-enabled monitoring stations can achieve a reasonable performance with commercial off-the-shelf devices, since the data path is based on a symmetric cipher, whereas public key cryptography is only employed for secure key distribution, even when several LEAs are monitoring the same suspect.

Acknowledgements

The work presented in this paper has been funded by the INDECT project (Ref 218086) of the 7th EU Framework Programme. The authors would also like to acknowledge the Spanish-funded CRAMnet (Grant no. TEC2012-38362-C03-01).

References

Baker F, Foster B, Sharp C. Cisco architecture for lawful intercept in IP networks, RFC 3924. Internet Engineering Task Force; October 2004. Bates A, Butler K, Sherr M, Shields C, Traynor P, Wallach D. Accountable wiretapping -or- i know they can hear you now. In: 19th Network and Distributed Systems Symposium (NDSS '12), San Diego (USA); 2012. p. 1–15.

Bellovin S, Blaze M, Clark S, Landau S. Going bright: wiretapping without weakening communications infrastructure. IEEE Secur Priv 2013; 11(1):62–72. http://dx.doi.org/10.1109/MSP.2012.138.

Clayton R, Murdoch SJ, Watson RNM. Ignoring the great firewall of China. In: 6th Workshop on Privacy Enhancing Technologies (PET06); 2006. p. 20–35. http://dx.doi.org/10.1007/11957454_2.

Cross T. Exploiting lawful interception to wiretap the internet. In: Black Hat 2010, Las Vegas (USA); 2010.

Diffie W, Landau S. Privacy on the line: the politics of wiretapping and encryption. 2nd ed. MIT Press; 2007.

Diffie W, Landau S. Communications surveillance: privacy and security risk. Commun ACM 2009;52(11):42–7. http://dx.doi.org/10.1145/1592761.1592776.

Electronic Frontier Foundation, EFF: CALEA, [Online; accessed: 30.04.14]. URL https://w2.eff.org/Privacy/Surveillance/CALEA/.

ETSI. Telecommunications security; Lawful Interception (LI); Requirements for network functions, ES 201 158. European Telecommunications Standards Institute; April 2002.

ETSI. Lawful Interception (LI); handover interface and Service-Specific Details (SSD) for IP delivery; Part 2: service-specific details for messaging services, TS 102 232–2. European Telecommunications Standards Institute; February 2012.

ETSI. Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; part 3: service-specific details for internet access services, TS 102 232–3. European Telecommunica-tions Standards Institute; February 2012.

ETSI. Lawful Interception (LI); eWarrant interface, TR 103 690. European Telecommunications Standards Institute; February 2012.

ETSI. Lawful Interception (LI); concepts of interception in a generic network architecture, TR 101 943. European Telecommunications Standards Institute; November 2006.

ETSI. Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic, TS 101 671. European Telecommunications Standards Institute; November 2011.

ETSI. Lawful Interception (LI); requirements of law enforcement agencies, TS 101 331. European Telecommunications Standards Institute; October 2009.

ETSI. Lawful Interception (LI); handover interface and service-specific details (SSD) for IP delivery; part 1: handover specification for IP delivery, TS 102 232–1. European Telecommunications Standards Institute; October 2011.

K. Poulsen. 12 true tales of creepy NSA cyberstalking, Wired Magazine.

Prevelakis V, Spinellis D. The Athens affair. IEEE Spectr 2007;44(7):26–33. http://dx.doi.org/10.1109/MSPEC.2007.376605.

Reporters without borders. Countries under surveillance: Egypt [Online; accessed: 30.04.14]. March 2011. URL, http://en.rsf.org/surveillance-egypt, 39740.html.

Riabov A. IESG, IETF policy on wiretapping, RFC 2804. Internet Engineering Task Force; May 2000.

J. Risen, E. Lichtblau, Bush lets U.S. spy on callers without courts, New York Times.

Sherr M, Shah G, Cronin E, Clark S, Blaze M. Can they hear me now?: A security analysis of law enforcement wiretaps. In: 16th ACM Conference on Computer and Communications Security (CCS09), ACM, Chicago (USA); 2009. p. 99–116. http://dx.doi.org/10.1145/2068816.2068827.

R. Singel, Whistle-blower outs NSA spy room, Wired Magazine.

Thales nShield Solo hardware security module. 2015 [Online; accessed: 21.05.15]. URL, http://www.thales-esecurity.com/products-and-services/products-and-services/hardware-security-modules/general-purpose-hsms/nshield-solo.

M. Townsend, Security services to get more access to monitor emails and social media, the Guardian.

TrueCrypt – Hardware Acceleration, [Online; Accessed: 30.04.14]. URL http://www.truecrypt.org/docs/hardware-acceleration.