ETSI TS 102 677 V1.1.1 (2019-07)

Lawful Interception (LI);
Dynamic Triggering of Interception

Reference
DTS/LI-00058

Keywords
dynamic triggering, lawful interception, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Lawful Interception (LI).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document describes in high level terms an architecture for the lawful interception of dynamically-allocated flows in a secondary communications domain, triggered by the activity of permanent identities in a primary domain. Examples of this include:

- SIP/SDP for VoIP call set-up and a proxy for the RTP sessions.
- A VoIP STUN/TURN/ICE server and one or more networks when traffic goes peer-to-peer.
- OAuth enabled logins in one service authenticated by another.
- Messaging platforms which enable file transfer via the cloud.
- S8HR and similar roaming scenarios.
- Systems with strong control/user plane separation.

The architecture aims to separate logic in the primary domain into that which understands the primary domain protocol (the Triggering Originating Function, TOF) and that which provides LI functions and connectivity (the Triggering Control Function, TCF1). This potential reduces the implementation of primary domain LI to the implementation of domain-specific TOF functionality along with interfaces to a commodity, domain-agnostic, TCF1.

Dynamic triggering as defined in the present document is intended to be able to complement the use of ETSI TS 103 221-1 [2], X1 interface specification, where X1 has been used to arm basic interception on non-dynamic identifiers in the primary domain.

The present document is independent of the particular communications technology or protocol in any signalling or transport plane, or layer or slice of a network.

Implementation notes of particular relevance to 3GPP networks are provided in an informative annex; normative implementation profiles should be described in separate technology-specific documents.

Outline triggering solutions already exist for specific technologies, for example the IMS Voice and S8HR VPLMN Roamer scenarios described in ETSI TS 133 107 [1]. The present document is consistent with those scenarios and provides a unified basis for future triggering solutions, whilst also offering much of the logical detail necessary for interoperability between differing technologies (for example, an over-the-top application server triggering LI on media carried by a mobile network operator).

1 Scope

The present document defines an architecture for the lawful interception of dynamically-allocated flows in a secondary communications domain, triggered by the activity of permanent identities in a primary domain.

Dynamic triggering as defined in the present document is intended to be able to handle a service that is handled by more than one CSP or network (for example one CSP handling the communication set up and another CSP handling the content exchange).

The present document is applicable only where national legal frameworks permit it. Issues concerning national legal frameworks are out of scope.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 133 107: "Universal Mobile Telecommunications System (UMTS); LTE; Digital cellular telecommunications system (Phase 2+) (GSM); 3G security; Lawful interception architecture and functions (3GPP TS 33.107)".

[2] ETSI TS 103 221-1: "Lawful Interception (LI); Part 1: Internal Network Interface X1 for Lawful Interception".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

Not applicable.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

deactivation: cessation of lawful interception in an LI function directly as a result of actions by the administration function in relation to a warrant

dynamic triggering: dissemination of an interception obligation for a certain target's communication between network elements

NOTE: Typically, these network functions will belong to the same network, and be under the control of a single network operator. Alternatively, the interception obligation may pass from one network operator to another network operator within the same jurisdiction. The network functions may have been supplied by different vendors.

dynamic triggering command: message sent between functions involved in dynamic triggering to invoke, modify, maintain or revoke DT LI

point of intercept: network function, comprised of physical and logical locations within the network, responsible for the isolation and access of the content of communication and intercepts related information

EXAMPLE: In the case where Dynamic Triggering is enabled in a network, the POIs interface with the Triggering Origination and Triggering Receiving Functions to transmit or receive target identities and other information which enable Dynamic Triggering to occur.

primary domain: communications domain within which targets' long-term identities are present, and from which dynamic triggers for LI are generated into the secondary domain

EXAMPLE: A SIP service / IMS signalling.

primary domain Triggering Control Function (TCF): function handling LI matching and triggering functions in the primary domain

primary identity: long-term identifier for a communicant in the primary domain, e.g. their SIP URI

primary session: communications in the primary domain containing targets' primary identities

EXAMPLE: A SIP session between explicitly-listed SIP URIs.

secondary domain: communications domain that conveys dynamically-addressed content, and into which dynamic triggers for LI are sent

EXAMPLE: The mobile network infrastructure over which RTP (IMS media) flows.

secondary flow: communications in the secondary domain associated with a particular primary session, for example the RTP packets associated to a particular SDP/SIP session

NOTE: The secondary flow is addressed in the primary domain by secondary flow indicators, and in the secondary domain by secondary flow locations.

EXAMPLE: An RTP flow.

secondary flow indicator: means by which the primary domain addresses a secondary flow

EXAMPLE: A "5-tuple" of (source IP, source port, protocol, destination IP, destination port).

secondary flow location: means by which the secondary domain addresses a secondary flow

EXAMPLE: The EPS bearer id and the network addresses of the infrastructure that handles that bearer.

secondary domain Triggering Control Function (TCF): function that is the gateway into the secondary domain for primary-initiated dynamic lawful interception requests

Triggering Originating Function (TOF): function encapsulating all of the relevant primary domain protocol processing logic, with minimal LI-specific functionality

Triggering Receiving Function (TRF): traditional IRI-or-CC internal interception function, except that it takes its targeting instructions from the dynamic triggering protocol (targeting dynamically-allocated flows) rather than from a traditional AF (targeting static identities)

Trusted Third Party (TTP): optional interworking mediation service between the primary and secondary domains

NOTE: The TTP relays dynamic triggering messages between domains and may perform actions to ensure messages are authorized and correct.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
ADMF	Administration Function
API	Application Programming Interface
ASN	Abstract Syntax Notation
CC	Content of Communication
CSP	Communication Service Provider
DF	Delivery Function
DIR	Directory
IBE	Identity Based Encryption
ICE	Intercepting Control Elements
IMS	IP Multimedia Sub-System
IP	Internet Protocol
IRI	Intercept Related Information
KMS	Key Management Server
LEA	Law Enforcement Agency
LI	Lawful Interception
LIID	Lawful Interception IDentifier
MF	Mediation Function
MF/DF	Mediation Function/Delivery Function
POI	Point of Intercept
RTP	Real Time Protocol
STUN	Simple Traversal of UDP through NATs
TCF1	primary domain Triggering Control Function
TCF2	secondary domain Triggering Control Function
TLS	Transport Layer Security
TOF	Triggering Originating Function
TRF	Triggering Receiving Function
TTP	Trusted Third Party
TURN	Traversal Using Relays around NAT
VPLMN	Visited Public Land Mobile Network

4 Overview of Dynamic Triggering

4.1 Reference architecture

4.1.1 Dynamic triggering functions and interfaces

A reference architecture is depicted in Figure 4.1.1-1 when the optional TTP is present. The TTP shall be used where mediated internetworking is required.

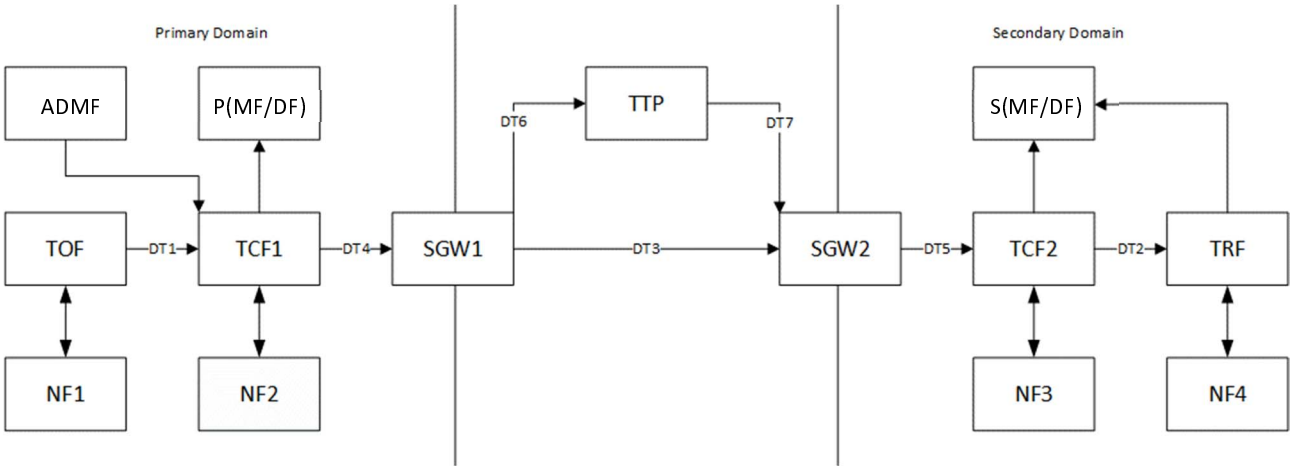

Figure 4.1.1-1: Reference architecture

The core dynamic triggering functions are TOF, TCF1, TCF2 and TRF.

The core functions will require access to some of their respective domain's network functions. This access, and the mechanism by which the core functions obtain the required data is implementation specific and out of scope of the present document (for example, TOF could be integrated into an existing function, access data through an API, or utilize in-line packet inspection).

ADMF and P(MF/DF), S(MF/DF) are standard LI functions.

The primary and secondary domain boundaries are as illustrated. The primary and secondary domains may be in control of the same CSP but are logically separate. The primary and secondary domains may also be in control of two (or more) CSPs.

SGW1 and SGW2 are security gateways between the domains. They are not directly involved in the dynamic triggering of LI.

The TTP, if used, sits between domains: the primary and secondary domains both trust the TTP more than they trust each other.

SGW1, SGW2 and TTP may rewrite message content (e.g. for topology hiding). They may not create Dynamic Triggering messages that invoke LI.

4.1.2 Link to interface X1

A basic instantiation of a set of Dynamic Triggering protocols is presented based on ETSI TS 103 221-1 [2], also called LI_X1 in the 3GPP architectures.

Specifically, the X1 interface is used to provide each of the following:

- A profile that may be used to provide the transport functionality (if this meets the requirements) (see clause 5.1 and Annex B).
- A minimum set of parameters that shall be used (potentially along with others) (see clauses 5.1, 5.2 and 5.3).

- A profile that may be used for the encoding of the parameters (optional, if this met the requirements) (see Annex B).

4.1.3 Integration with traditional LI

There are two natural options in the primary domain for the integration of dynamic triggering with traditional LI (in particular with a POI):

- The **monolithic** option is a combined TOF/TCF1/POI, developed specifically for the primary domain in question, into which all primary sessions are copied (e.g. from a service slice of the network to an inner LI enclave).
- The **modular** option is a commodity TCF1/POI in the LI enclave of a network, supplied with triggering information and IRI and/or CC by the technology-specific TOF that operators outside of the enclave.

In either case it is assumed that, once it has derived or been supplied with IRI and/or CC, the POI operates in the normal manner per existing LI specifications. The POI is not specified further in the present document.

4.2 Illustrative use-case

An illustrative use-case for dynamic triggering, describing how an Identity-Based Encryption (IBE) voice service might implement LI in a modular fashion, is given below. The case with no TTP is treated.

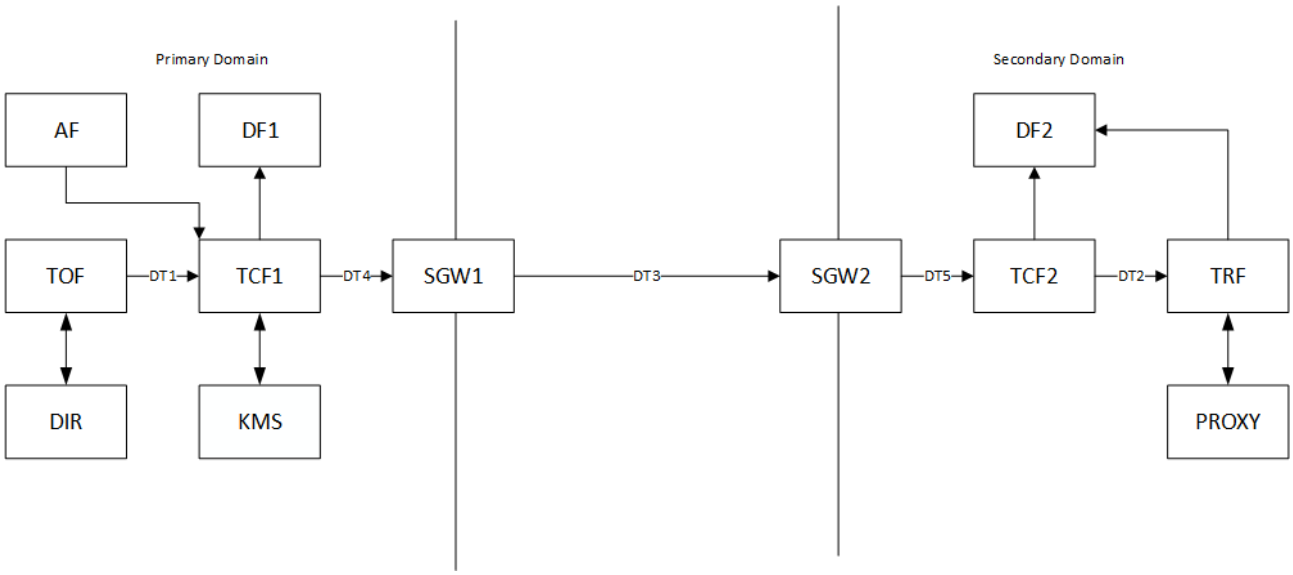

Figure 4.2-1: Reference architecture

End-user devices have been supplied with public/private keys stored in a Key Management Server (KMS) which resides in a secure enclave. When making a call, the devices connect initially through a Directory server (DIR) to establish a session key, then the call is routed through a network element in a secondary domain (PROXY). The KMS is capable of deriving voice decryption keys in response to requests from an authorized LI function. LI is implemented with:

- TOF that interfaces with DIR.
- A dynamic triggering interface on the KMS.
- A commodity TCF1/IRI-POI configured to interface to existing LI administration and delivery functions.
- Co-operating TCF2 instances in the data networks over which the IBE voice service operates.

Call setup begins. The directory server TOF extracts the participants' identities, cryptographic parameters from the key exchange and the 5-tuple (IP addresses, protocol, ports) over which the encrypted voice will flow. These are sent to TCF1, along with any additional IRI that might be required for LI purposes (e.g. codec). If TCF1 determines that one of the parties to the call is an LI target, it requests the session key from the KMS and delivers primary domain IRI to DF1. TCF1 delivers sufficient information to TCF2 to enable the secondary domain to collect and deliver IRI and CC for the associated secondary flow passing over PROXY through TRF and DF2.

5 Message Specification

5.1 Introduction

In common with many protocols, an implementation of dynamic triggering would consist of:

- A transport mechanism, including headers specifying source/destination addresses, flow control (sequencing, retries) and security features.
- Messages consisting of various fields. The breakdown of dynamic triggering messages into fields is specified in clause 5.2 (this clause provides a minimum set of required fields); the meaning of each field-type is specified in clause 5.3.
- An encoding of the messages/fields, for example in ASN.1.

The de-scoped items (transport and encoding) would form a dynamic triggering *profile*. An illustrative sketch of a profile for dynamic triggering interfaces in mobile networks is provided in Annex B. A network component implementing dynamic triggering would be expected to demonstrate compliance on the appropriate interfaces with the present document and, with possible variation across interfaces, profiles appropriate for the intended operating environment.

5.2 Minimum message contents

The underlying goal is to ensure that, as a minimum, the information in clause 6.2 of ETSI TS 103 221-1 [2] can be delivered from TCF1 to TCF2. Depending on the network configuration, it may also be necessary to supply the information in clause 6.3 of ETSI TS 103 221-1 [2]. If the functionality is required, then the messages in clauses 6.4 to 6.7 of ETSI TS 103 221-1 [2] shall also be supported.

Therefore:

- DT3, DT4, DT5 shall all support at least the messages and fields from clause 6.2 (and clauses 6.3 to 6.7 if necessary) of ETSI TS 103 221-1 [2]. Further information may also be necessary e.g. for the Security Gateways.
- DT1 shall supply those components of clause 6.2 (and 6.3 to 6.7 if necessary) of ETSI TS 103 221-1 [2] which cannot be supplied from P(MF/DF) or ADMF.
- DT2 shall supply those components of clause 6.2 (and 6.3 to 6.7 if necessary) of ETSI TS 103 221-1 [2] which are required for the TRF to perform its role.

5.3 Field semantics

Many of the elements in clause 5.2 are defined by referring to the ETSI TS 103 221-1 [2]. For those fields, the field semantics are also provided by reference to the ETSI TS 103 221-1 [2].

6 Security

6.1 Threats and countermeasures

An implementation of dynamic triggering shall provide assurance to the LEA and to the primary and secondary domain operators that LI targeting is being applied correctly and securely. In particular, evaluation of dynamic triggering functions should seek to demonstrate countermeasures to (at least) the following general threats:

- Platform exploitation. The function, and node or container in which it operates, shall be resistant to "hacking" and should survive a penetration-testing exercise.
- Logic errors. The function shall perform its role accurately, even in the face of malformed data. "Fuzzing" tests should fail to induce unexpected behaviour.
- Data leakage, corruption and replay. The function shall secure its data in storage and in transit; attempts to modify or replay security-critical messages shall be rejected.
- Spoofing. The function shall resist attempts by unauthorized elements to subvert its interfaces; network connections shall be mutually authenticated.
- Rogue nodes. It should be possible to detect and identify a single malfunctioning node, e.g. a TOF whose recent software update was unsuccessful, and remove it from the dynamic triggering solution without having to shut-down the entire TCF1/TCF2 interface due to consequential errors in the secondary domain. Robust monitoring of [Log] messages is required.

Maximum assurance should be sought for any function that handles raw LI targeting (identities, warrants, etc.) as provisioned by the ADMF. High assurance should be sought for any function that generates or handles dynamic triggers, IRI or CC. It may be pragmatic to seek slightly less assurance for any function that protects the security of general user traffic (before possible targeting for LI delivery), especially when that function operates outside of a secure LI enclave - e.g. in an edge computing environment.

Particular attention should be paid to the security of inter-domain interfaces, especially when the networks either side of them are subject to separate national/legal regulations.

6.2 Channel and message security

Inter-node network connections that protect dynamic triggers and unprocessed LI targeting in particular, and possibly other network connections to/from dynamic triggering functions, should be cryptographically protected. Standard technologies such as IPsec and (D)TLS can provide the required protection, provided that strict architectural separation (e.g. keeping the TCF1/TCF2 interface closed to all but those functions) is enforced through a combination of cryptographic and firewall/proxy-type mechanisms.

Annex A (informative): General implementation notes

A.1 Architecture

The present document is useful for genuinely cross-domain triggering scenarios, where the primary and secondary domains are not tightly integrated and a cost-effective, modular, engineering solution is sought. In contrast, a tightly integrated implementation of, say, a single mobile network operator's IMS service running over their own IP network may be able to operate a more performant (e.g. lower latency) LI solution built from proprietary components.

The present document implies that when more than one participant in a primary session is a target, TCF2 receives multiple Dynamic Trigger messages and invokes multiple (likely duplicate) interceptions at the TRF. This is potentially wasteful, but if implementations of the present document wish to de-dupe such flows then it is important that they avoid the situation that revocation of one participant's LIID results in the entire de-duped flow being discarded.

A.2 Presentation and transport

Messages are described in clause 5.1 in terms of the minimum set of fields required to implement dynamic triggering. A profile of the present document should describe any additional fields that may be required for the communications domain in question and needs to choose how to present them. For example, one option is to have strictly-defined message types (indicated by an octet, say, at the start of the message) that contain a known list of fields in a known order; another option is to have a single catch-all message type that can contain any field types, with dynamic triggering functions reading from and adding to those messages as necessary.

Profiles specify the encoding of each field: both the generic syntax to be used (for example, aligned BASIC-PER ASN.1 as used in certain 3GPP protocols), and the specific enumerated types used to describe the many different subtypes of each field (for example, it may be necessary when constructing a Secondary Indicator to tag the component parts as IP addresses, ports, protocol, etc.). The encoding of fields that relate to secondary flows (such as the Secondary Indicator and Processing Hints) indicates to which flow or flows the field applies, for example by tagging each entry with a flow number or bit-field of applicable flows, or by grouping the fields by flow id.

The present document does not specify the sequencing and flow-control of dynamic triggering messages. Whilst heavy-duty flow-control should probably be avoided (at least on inputs to TCF1) for latency reasons, some option for timeouts and retries may be desirable. There is also no explicit provision for failure reporting, and so no means for example for control functions to black-list misbehaving upstream nodes. Record-route functionality may be desirable for diagnostic purposes. All of these are considerations for a technology-specific profile.

Annex B (normative): Base profile

A base transport, encoding and security profile is provided by using the details given in the ETSI TS 103 221-1 [2]. It is recommended to use Transport and Encoding Profile A and the security details.

Other profiles may be used e.g. to meet lower-latency requirements than can be achieved using the base profile.

Annex C (informative): Change Request History

Status of the present document: ETSI TS 102 677 Dynamic Triggering of Interception		
TC LI approval Date	**Version**	**Remarks**
July 2019	1.1.1	First publication of the TS through Remote Consensus after TC LI#51 (11-13 June 2019, Texel, The Netherlands). Prepared by rapporteur.

History

Document history		
V1.1.1	July 2019	Publication