



Lawful Interception (LI); Dynamic Triggering of Interception

ITeH STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/5f115824-82ab-4c01-b71b-a23c2a99d1e9/etsi-ts-102-677-v1.1.1-2019-07>

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

Important notice

The present document can be downloaded from:
<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at <https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2019.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M™ logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners.

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	4
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	8
3.3 Abbreviations	8
4 Overview of Dynamic Triggering	9
4.1 Reference architecture	9
4.1.1 Dynamic triggering functions and interfaces	9
4.1.2 Link to interface X1	9
4.1.3 Integration with traditional LI.....	10
4.2 Illustrative use-case	10
5 Message Specification.....	11
5.1 Introduction	11
5.2 Minimum message contents	11
5.3 Field semantics	11
6 Security.....	12
6.1 Threats and countermeasures.....	12
6.2 Channel and message security.....	12
Annex A (informative): General implementation notes.....	13
A.1 Architecture.....	13
A.2 Presentation and transport	13
Annex B (normative): Base profile	14
Annex C (informative): Change Request History.....	15
History	16

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).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/5fe5e3a4-82ab-4c01-b71b-a23c2a99d1e9/etsi-ts-102-677-v1.1.1-2019-07>

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	3 rd 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.

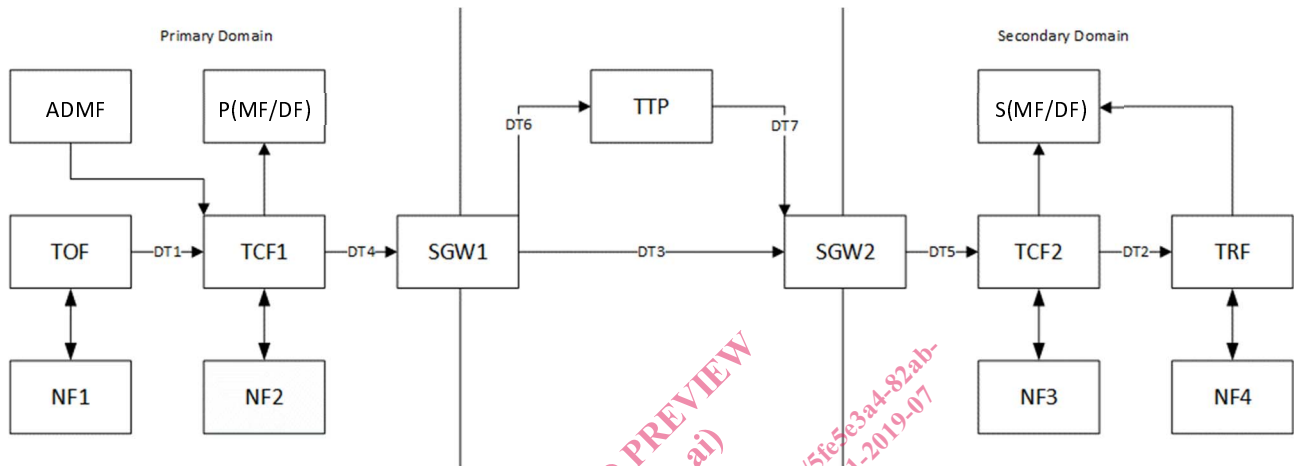


Figure 4.1.1-1: Reference architecture

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 LL_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).