ETSI TS 102 232-3 V3.6.1 (2017-08)

Lawful Interception (LI);
Handover Interface and
Service-Specific Details (SSD) for IP delivery;
Part 3: Service-specific details for internet access services

Reference
RTS/LI-00145-3

Keywords
access, internet, IP, lawful interception, security, service

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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 2017.
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 protected for the benefit of its Members.
GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intellectual Property Rights 6
Foreword 6
Modal verbs terminology 6
Introduction 6
1 Scope 7
2 References 7
2.1 Normative references 7
2.2 Informative references 8
3 Definitions and abbreviations 8
3.1 Definitions 8
3.2 Abbreviations 9
4 General 10
4.1 Internet Access Service (IAS) 10
4.2 Target identity and IP address 10
4.3 Lawful Interception requirements 11
4.3.0 Introduction 11
4.3.1 Target identity 11
4.3.2 Result of interception 11
4.3.3 Intercept related information messages 12
4.3.4 Time constraints 12
4.3.5 Preventing over and under collection of intercept data 12
5 System model 13
5.1 Reference network topologies 13
5.1.0 Introduction 13
5.1.1 Dial-up access 13
5.1.2 xDSL access 14
5.1.3 Cable modem access 15
5.1.4 IEEE 802.11 Access (with Wireless LAN profile) 16
5.2 Reference scenarios 16
5.2.1 Logon 16
5.2.2 Multi logon 16
5.2.3 Multilink logon 17
5.2.4 IP transport 17
5.2.5 Logoff 17
5.2.6 Connection loss 17
6 Intercept Related Information (IRI) 18
6.1 IRI events 18
6.2 HI2 attributes 19
6.2.0 List of HI2 attributes 19
6.2.1 Use of targetIPAddress, additionalIPAddress and otherTargetIdentifiers fields 20
6.2.2 Use of location field 21
7 Content of Communication (CC) 21
7.1 CC events 21
7.2 HI3 attributes 21
8 ASN.1 for IRI and CC 21
Annex A (informative): Stage 1 - RADIUS characteristics 27
A.1 Network topology 27
A.1.0 RADIUS deployment options 27
A.1.1 RADIUS server 27
A.1.2 RADIUS proxy 28

A.2 RADIUS service 29
A.2.1 Authentication service 29
A.2.2 Accounting service 29
A.3 RADIUS protocol 30
A.3.1 Authentication protocol 30
A.3.2 Accounting protocol 30
A.4 RADIUS main attributes 31
A.5 RADIUS interception 32
A.5.0 Introduction 32
A.5.1 Collecting RADIUS packets 32
A.5.2 Processing RADIUS packets 32
A.5.2.1 Mapping events to RADIUS packets 32
A.5.2.2 Functional model 33
A.5.2.3 RADIUS spoofing 37
A.5.3 Mapping RADIUS on the IRI structure 37
Annex B (informative): Stage 1 - DHCP characteristics 38
B.1 Network topology 38
B.2 DHCP service 38
B.3 BOOTP protocol 39
B.4 DHCP protocol 39
B.4.0 Overview 39
B.4.1 Address assignment 40
B.4.2 Message transmission and relay agents 41
B.4.3 Security and authentication 41
B.5 DHCP main attributes 41
B.6 DHCP interception 42
B.6.1 Introduction 42
B.6.2 DHCP packets 42
B.6.3 State machine 43
B.6.3.0 Overview 43
B.6.3.1 Mapping DHCP packets to events 43
B.6.3.2 Timers and administrative events 44
B.6.3.3 State information 44
B.6.3.4 State machine diagram 45
B.6.4 Mapping DHCP on the IRI structure 45
Annex C (informative): IP IRI interception 47
C.1 Introduction 47
C.2 Requirements 47
C.3 Proposed implementation 47
Annex D (informative): TCP and UDP IRI interception 48
D.1 Introduction 48
D.2 Requirements 48
D.3 HI2 requirements 48
D.4 HI3 requirements 49
D.5 General requirements 49
Annex E (informative): Bibliography 50
Annex F (informative): Change Request history 51

History 54

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document 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).

The present document is part 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [2].

The ASN.1 module is also available as an electronic attachment to the original document from the ETSI site (see clause 8 for more details).

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 intention of the present document has been to follow the advice given at ETSI meetings in all cases.

The present document focuses on intercepting IP data in relation to the use of Internet Access Services (IAS) and is to be used in conjunction with ETSI TS 102 232-1 [2]. In the latter document the handing over of the intercepted data is described.

1 Scope

The present document contains a stage 1 description of the interception information in relation to the process of binding a "target identity" to an IP address when providing Internet access and a stage 2 description of when Intercept Related Information (IRI) and Content of Communication (CC) need to be sent, and what information it needs to contain.

The study includes but is not restricted to IRI based on application of Dynamic Host Configuration Protocol (DHCP) and Remote Authentication Dial-in User Service (RADIUS) technology for binding a "target identity" to an IP address and CC for the intercepted IP packets.

The definition of the Handover Interface 2 (HI2) and Handover Interface 3 (HI3) is outside the scope of the present document. For the handover interface is referred to ETSI TS 102 232-1 [2].

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 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

NOTE: Periodically TS 101 671 is published as ES 201 671. A reference to the latest version of the TS as above reflects the latest stable content from ETSI/TC LI.

[2] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".

[3] IETF RFC 1122: "Requirements for Internet Hosts - Communication Layers".

[4] IETF RFC 1570: "PPP LCP Extensions".

[5] IETF RFC 1990: "The PPP Multilink Protocol (MP)".

[6] IETF RFC 2131: "Dynamic Host Configuration Protocol".

[7] IETF RFC 7542: "The Network Access Identifier".

[8] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".

[9] IETF RFC 2866: "RADIUS Accounting".

[10] IETF RFC 3046: "DHCP Relay Agent Information Option".

[11] IETF RFC 3118: "Authentication for DHCP Messages".

[12] IETF RFC 3396: "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)".