Geschäftsstelle: ÖFEG, Postfach 147, 1006 Wien, e-mail: ak-tk@oefeg.at

E M P F E H L U N G

Lawful Interception für IMS in Österreich -

Erläuterungen und Festlegungen zu ETSI TS 102 232-1 und ETSI TS 102 232-5

Zuordnung: AG Schnittstellendefinition

Ausgabenübersicht

Ausgabe Nr.	1				
Ausgabe Datum	21.11.2017				
Editor	Franz Edler				
AK-TK Geschäftsstelle	Helmut Malleck				

Inhaltsverzeichnis

1 Allgemeines

1.1 Einleitung

Mit der geplanten Novelle der ÜVO sollen für „Voice over LTE" (VoLTE) und „Voice over WiFi" (VoWiFi) entsprechende Standards für die Übermittlung von Verkehrs- und Inhaltsdaten im Zuge gerichtlich angeordneter Überwachungen festgelegt werden. Diese Empfehlung beschreibt die technischen Einzelheiten zur Umsetzung der Maßnahmen zu den Standards ETSI TS 102 232-1 und ETSI TS 102 232-5.

Diese Empfehlung wird vom Arbeitskreis für Technische Koordination in der Telekommunikation (AK-TK) herausgegeben und von der Arbeitsgruppe Schnittstellendefinition (AG IF) erstellt.

Die Empfehlung EP 023 - Ausg. 1 wurde in der 53. Sitzung des AK-TKneu am 21.11.2017 von den anwesenden stimmberechtigten Mitgliedern abgestimmt.

Die Veröffentlichung dieser Empfehlung erfolgt gemäß AK-TK Geschäftsordnung § 7, Absatz 5:

Auf Antrag eines stimmberechtigten Mitglieds entscheidet der Arbeitskreis über die Veröffentlichung der Beschlüsse. Um die Veröffentlichung zu beschließen, ist die Einstimmigkeit aller anwesenden Mitglieder gemäß § 3 Abs. 2 lit. a und c erforderlich, wobei allen anderen Mitgliedern ein Einspruchsrecht innerhalb von 10 Tagen nach Aussendung des Protokolls zu gewähren ist. Geschäfts– und Betriebsgeheimnisse sind jedenfalls zu wahren. Die Veröffentlichung erfolgt über die RTR.

Vom Bundesministerium für Inneres erfolgte ebenfalls eine Zustimmung für die Veröffentlichung über die RTR.

1.2 Mandat der Arbeitsgruppe

Per Umlaufbeschluss wurde der AG Schnittstellendefinition folgendes Mandat erteilt: *„Die Einführung der IMS-Technologie in Kommunikationsnetzen erfordert neue Standards für die Ausleitung (Lawful Interception). Die Standards enthalten Optionen, die in der Arbeitsgruppe Österreich-spezifisch verbindlich festzulegen sind."*

Die Empfehlung enthält somit alle, gemeinsam mit dem Bundesministerium für Inneres (BM.I) abgestimmten, erforderlichen Ergänzungen und Klarstellungen zu den Spezifikationen ETSI TS 102 232-1, V3.10.1 und ETSI TS 102 232-5, V3.5.1, wobei jeweils immer auf den Originaltext Bezug genommen wird.

Es werden im Dokument nur jene Kapitel und Testpassagen angeführt, für die Ergänzungen oder Klarstellungen erforderlich sind. Alle Anmerkungen sind am Beginn der Zeile mit *„AK-TK:"* markiert.

1.3 Teilnehmer der Arbeitsgruppe

A1 Telekom Austria AG
Bundesministerium für Inneres
fonira Telekom GmbH
KAPPER NETWORK-COMMUNICATIONS GmbH
Hutchison Drei Austria GmbH
MASS Response Service GmbH
mediainvent Service GmbH
Rundfunk und Telekom Regulierungs-GmbH
T-Mobile Austria GmbH
Tele2 Telecommunication GmbH
UPC Business Austria GmbH/UPC Telekabel Wien GmbH
WNT Telecommunication GmbH

2 Modifikationen zu ETSI TS 102 232-1, V3.10.1

Die angeführten Kapitelnummern sind dem Originaltext entnommen und stellen keine Überschriften im Dokument dar.

5.2.1 Version

The header shall state which version of the handover header is in use.

NOTE: Some techniques (e.g. ASN.1 with BER) automatically include version numbering as part of the data encoding process. In these cases, it is not necessary to add a version number as a separate field.

AK-TK: By use of the OID in ASN.1 it is not necessary to add a version number as a separate field.

5.2.3 Authorization country code

The authorization country code states the country within which the authorization was granted. The authorization country code makes the LIID internationally unique. Two-letter codes are used as per ISO 3166-1 [10].

AK-TK: All operators in Austria will use the code 'AT' in the LIID field.

5.2.4 Communication identifier

The communication identifier consists of the Network Identifier (NID), Communications Identity Number (CIN) and Delivery Country Code (DCC).

The CIN is used to identify uniquely the communications session (as defined in ETSI TS 101 671 [4]).

For some services, the CIN field defined in ETSI TS 101 671 [4] may not be sufficiently flexible to identify sessions uniquely and easily. The CIN extension field may be used, where permitted in the service specific standard (but shall not be used otherwise). The CIN shall then be considered to be the combination of communicationIdentityNumber field and the cINExtension field. If the CIN Extension Field in itself constitutes a unique identifier for the communications session, then the communicationIdentityNumber field does not need to be present.
...

The Network Identifier (NID) consists of the operator identifier and, optionally, the network element. The operator identifier identifies the CSP performing the intercept and is mandatory. The network element identifier can be used within a CSP to identify the relevant network element carrying out the LI operations and is optional. If it is used, the network element needs to be uniquely identified within the CSP domain and either the networkElementIdentifier structure or the eTSI671NEID structure imported from ETSI TS 101 671 [4] needs to be used.

The delivery country code makes the Communication Identifier internationally unique. The delivery country code identifies the geographical location of the Mediation Function. The DCC will be coded according to ISO 3166-1 [10]. The DCC should be used if MF and LEMF are not located in the same country.

AK-TK: The cINExtension field is optional.
If a network element identifier is used, a specific list of all used identifier and the related network elements has to be provided to BM.I.
The operator identifier is set to the used five-digit operator identifier.
Operator with no identifier have to align a new one with BM.I.
The delivery country code is set to the two characters "AT".

5.2.5 Sequence number

The sequence number (as defined in ETSI TS 101 671 [4]) counts individual intercepted protocol data units within a communications session of a target identity.

AK-TK: When HI2 is generated at different network elements in parallel, the sequence number counts are always kept separate (not aligned).

5.2.6 Payload timestamp

The timestamp is mandatory for IRI for all services. CC shall also contain a timestamp (exceptions are possible for CC timestamps on a service-by-service basis).

NOTE 1: A PS header field is used to transfer the timestamp information specific for IRI and CC payloads; the transfer of the timestamp within each IRI and CC payload fields is strictly required only in case of aggregation of payloads (clause 6.2.3).

NOTE 2: Either the ASN.1 GeneralizedTime or the ASN.1 MicroSecondTimeStamp may be used, subject to national agreement.

NOTE 3: The timeStampQualifier field may be used to indicate what time the timestamp represents, subject to national agreement.

AK-TK: Both methods mentioned in NOTE 2 can be used.
The timestamp qualifier field is used in case of aggregation of payloads (see 6.2.3).

5.2.7 Payload direction

Indicates the direction of the intercepted data (to target or from target). The payload direction is optional for IRI; it shall only be used if specified in the service-specific details and shall only be used in the manner described in the servicespecific details. The payload direction is optional for CC.

AK-TK: For IRI the payload direction is not used.
For CC the payload direction is mandatory.

5.2.11 Interception Point Identifier

The Interception Point Identifier is an optional field. If the Interception Point ID is used, the Service Provider shall assign each interception point within its network an identifier of up to 8 characters. The identifier shall be unique within the Service Provider. If used, the Interception Point ID shall be attached to each CC and IRI PDU from that interception point.

AK-TK: No specific national requirements.

5.2.12 Session direction

The sessionDirection parameter for IRI messages is optional; it shall only be used if specified in the service-specific details and shall only be used in the manner described in the service-specific details.

AK-TK: The session direction parameter for IRI is not used.

6.2.2 Error reporting

The MF Handover Manager shall collect error reports from the lower layers at the CSP. It shall report errors to the LEMF Handover Manager according to agreements between the CSP and LEA. A TRI message of type OperatorLeaMessage may be used to transfer these error reports.

AK-TK: No TRI message are used, the error reporting is done via a separate channel (e.g. telephone, e-mail).

6.2.3 Aggregation of payloads

It may be beneficial to aggregate a number of payloads to be transported within one larger unit (Protocol Data Unit or PDU). The advantage is a saving in bandwidth (one PDU header covers a number of payloads). The main disadvantage is that some payloads are delayed while waiting for the aggregation to take place; additionally there is extra processing overhead. Payload aggregation may be used if agreed by the CSP and LEA. If payload aggregation is used, it shall be implemented as follows.

To aggregate payloads, they may only have different timestamps, directions (for IRI or CC payloads) or IRI-types (for IRI payloads). Payloads may not be aggregated if their associated information differs in other ways (e.g. different LIID, or different operator). One aggregated PDU then has a single sequence number (i.e. aggregated payloads are not assigned individual sequence numbers). The order of packets in the aggregated PDU shall be in the same sequence as they arrived at the Handover Manager. It is acceptable either to assign one timestamp to the whole PDU (in the PDU header) or, if more detailed timestamp information is required, then one timestamp shall be assigned to each payload as indicated in annex A. A "timeStampQualifier" in each payload can be used to indicate what this timestamp represents. An additional timestamp may be assigned to the PDU header to indicate when the aggregated PDU was created. In this case the value "timeOfAggregation" shall be the time the complete PDU is created.

The implementation of aggregation (i.e. when aggregation is applied, use of "timeStampQualifier", and how many packets can be aggregated together) shall be subject to the agreement of CSP and LEA to meet national requirements.

AK-TK: Aggregation of payloads is not used

6.2.5 Padding data

By agreement, it is permitted to transfer "padding" data over the Handover Interface.

AK-TK: No Padding data are used.

6.3.1 General

The Delivery Function is responsible for maintaining a single transport connection as described in clause 6.3.2. The transport connection can be a TCP socket, a TLS IETF RFC 5246 [21] session or other transport connection.

AK-TK: For the transport connection TCP/IP is used.

6.3.2 Opening and closing connections

When it is created, the MF Delivery Function shall immediately attempt to open a transport connection. It is acceptable for the MF or LEMF Delivery Function to terminate the transport connection if they require.

AK-TK: No specific national requirements.

6.3.4 Keep-alives

To meet requirement R16 (see annex B) it is recommended to use session-layer “keep-alives”. If used, “keep-alives” shall be implemented as described in this clause.

The MF Delivery Function starts a timer when the connection is established, and is reset whenever data is sent. When the timer reaches TIME1, the MF Delivery Function shall send a “keep-alive” message. It is acceptable for the “keep-alive” message to be sent before TIME1 if required. The LEMF Delivery Function shall respond to this “keep-alive” message within TIME2. If the MF does not receive a response in TIME3, the MF shall terminate the connection at the Transport Layer and attempt to establish a new one.

NOTE: The CSP and the LEA should agree on values for TIME1, 2 and 3. A typical value for TIME1 would range from 120 s to 360 s. A typical value for TIME2 would be 30 s. The value for TIME3 should be long enough to allow for the transport connection to recover from transient failures (e.g. to cover TCP retransmissions including exponential back-off). A typical value for TIME3 would be 60 s. Note that TIME3 will need to be larger than TIME2.

AK-TK: No specific national requirements.

6.4.2 TCP settings

The source and destination port numbers shall be within the dynamic port range for TCP. The value of the source port number is chosen by the CSP.

AK-TK: Destination port numbers will be provided by the BM.I

7.1.1 General

The network used for data exchange influences how the handover requirements from annex B should be met. The choice of the network will be made on a national basis for legal and pragmatic reasons.

AK-TK: The public Internet is used for transport of handover information. Security is provided via a VPN connection.

7.2.1 General

In annex B, requirements are identified for Confidentiality, Authentication and Integrity. These requirements can be met by use of a private, managed delivery mechanism (clause 7.1.2). However, if the underlying mechanism is based on a public network (clauses 7.1.3 and 7.1.4), then further security mechanisms are strongly recommended.

The requirements for Confidentiality, Authentication and Handover Integrity can be met by using a VPN application. VPN applications provide secure, network-to-network, host-to-network, or host-to-host tunnels - virtual point-to-point connections. The technical details for the VPN applications including IPSec are outside the scope of the present document.

AK-TK: Security is provided via a VPN connection.

7.3.2 Timeliness

The timeliness requirement is that the results of interception are not delayed unnecessarily (R14), with no requirement to preserve the real-time nature of CC in LI delivery. Under normal conditions, all the network types in clause 6.2 will meet this timeliness requirement when using the delivery mechanism in clause 7.

AK-TK: Any unnecessary delay must be avoided.

3 Modifikationen zu ETSI TS 102 232-5, V3.5.1

Die angeführten Kapitelnummern sind dem Originaltext entnommen und stellen keine Überschriften im Dokument dar.

4.3 General Requirements

The following requirements regarding the interception of signalling shall apply:

1) Annex B provides the functional description of the minimal set of information that is to be provided to Law Enforcement for each intercepted communication.
2) The present document supports the interception of communication services defined in the following IETF/ITU-T standards and recommendations:

   - IETF RFC 3261 [4] (SIP);
   - IETF RFC 3550 [5] (RTP);
   - IETF RFC 4975 [15] (MSRP);
   - Recommendation ITU-T H.323 [6];
   - Recommendation ITU-T H.225.0 [12];
   - Recommendation ITU-T H.245 [13];
   - Recommendation ITU-T T.38 [16].

3) Any deviation from the supported IETF and ITU-T specifications identified in item 2, e.g. vendor specific parameters, shall be agreed in advance between the Communications Service Provider (CSP) and Law Enforcement Agency (LEA).

AK-TK: All intercept related information (HI2) within and outside of a communication session is provided via IRI report, which contain the SIP message or XCAP message.
The above mentioned recommendations IETF RFC 4975 (MSRP) and ITU-T H.323, ITU-T H.225.0 and ITU-T H.245 are not used.

5.2.2 Provisioning of the H.323 IRI IIF

H.323 call signalling, call control and subscriber controlled input messages are reported as Intercepted Related Information (IRI) for the interception of multi-media services. H.323 call signalling and control messages refer to the basic call signalling (H.225.0), call control (H.245) and those messages required for the signalling of supplementary services (i.e.: H.450.x). Subscriber controlled input messages refer to those messages generated as a result of user procedures for the control of Supplementary Services (activation/deactivation/interrogation).

All H.323 call signalling, call control and subscriber controlled input messages that are transmitted on behalf of the target subscriber are subject to intercept at the IRI IIF. Based upon the network configuration, the AF shall provision IRI IIF with either a H.323 Unique Resource Locator (H.323-URL), or a H.323 Identity (H.323-ID), or a public E.164 telephone number.

If available events related to the Registration, Administration and Status (i.e. H.323 RAS) of the target subscriber's terminal equipment are also subject to intercept at the IRI IIF.

AK-TK: H.323 call signalling is not used in public networks.

5.2.3 Location information

The IRI Internal Interception Function (IIF) may report location information to satisfy the requirement in clause B.3. The availability and format of location information in the IRI IIF may depend on the network access technology. The present document uses the common parameter from ETSI TS 102 232-1 [2] to signal this information. Use of this parameter is subject to national agreement.

AK-TK: For mobile subscriber served via cellular network the location information of the cell site will be delivered in WGS84 coordinates. For fixednet numbers no location information is provided.

5.3 Assigning a value to the Communication Identity Number

In order to produce useful IRI records from events, the IRI and CC records of a communication session shall be correlated with a single value for the Communication Identity Number (CIN) field. The CIN should be assigned upon first IRI or CC message.

AK-TK: No specific national requirements.

5.3.1 Assigning a CIN value to SIP related IRI

All IRI events resulting from SIP messages in a single call will be assigned the same value for the CIN. A call may consist of two or more call signalling legs (e.g. when communicating via a SIP proxy). The various related call signalling legs are correlated. Implementation of SIP leg correlation is out of scope for the present document, a possible option is to use the P-Charging-Vector header (see TS 33.108 [9] Annex F) if present.

AK-TK: No specific national requirements.

5.4 Events and IRI record types

Table 1 summarizes the mapping between event type and record type sent to the LEMF.

Table 1: Mapping between IP MM Events and HI2 Records Type

Event	IRI Record Type
At assignment of a new CIN value	BEGIN/REPORT
All intermediate signalling, other than the last event	CONTINUE/REPORT
The last event related to a communication session	END/REPORT
Delayed IRI events related to an already ended session	REPORT
Events that are not mapped	REPORT
NOTE: Not mapped events could for example be encapsulated SIP messages.	

AK-TK: For communication session related signalling IRI record types BEGIN/CONTINUE/END shall be used. For all other types of signalling messages IRI record type REPORT shall be used.

5.5 Interception of Content of Communication

…

The RTP CC shall also contain the RTP header, UDP header and IP header, except by agreement between CSP and LEA (for example these headers may not be available at the point of interception). Each IPMMCC PDU shall contain one intercepted packet.

The UDPTL CC shall follow the same principles.

The MSRP CC shall contain the TCP header.

The frameType field indicates which headers are present in a given CC stream.

In the case where the RTP header is unavailable, one may be inserted by the mediation function, subject to agreement between LEA and CSP. The addition of an inserted RTP header may aid processing the audio stream at the receiver. When an artificial header is used, this shall be signalled using the artificialRtpFrame parameter of the FrameType structure.

AK-TK: The RTP CC shall also contain the RTP header, UDP header and IP header. No MSRP is intercepted.

5.6 Direction for IMS IRI for Signalling Messages

In order to indicate the direction of a signalling message carried in the IRI payload, the payloadDirection parameter (as defined in ETSI TS 102 232-1 [2]) parameter may be used. Use of this parameter is subject to national agreement. If the payloadDirection parameter is used then it shall be populated as follows:

- if the signalling message was sent from the target, the fromTarget value shall be used;
- if the signalling message was sent to the target, the toTarget value shall be used;
- if the direction could not be determined reliably, the indeterminate value shall be used.

The values combined and notapplicable shall not be used unless by specific national agreement.

AK-TK: The payloadDirection parameter is not used for IMS IRI for Signalling Messages.

5.7.1 Direction for SIP sessions

In order to indicate the direction of a SIP session, the sessionDirection parameter (as defined in ETSI TS 102 232-1 [2]) may be used. Use of this parameter is subject to national agreement.

AK-TK: The sessionDirection parameter for SIP sessions must be provided.

7 ASN.1 specification for IRI and CC

…

```
SIPMessage ::= SEQUENCE
{
     iPSourceAddress [0] IPAddress,
     iPDestinationAddress [1] IPAddress,
     sIPContent [2] OCTET STRING,
     ...
}
```

AK-TK: The ASN.1 parameters "ìPSourceAddress" and "iPDestinationAddress" contain public IP addresses from network side if they are available.

4 Einführung neuer Codecs

Mit Ausg. 1 werden folgende Codecs unterstützt:

G.711a, G.726, G.729A, T.38, AMR-NB, AMR-WB/G.722.2, EVS
sowie Telephony events gem. RFC4733

Für die Einführung weiterer bzw. neuer Codecs bei einem Netzbetreiber ist mind. 6 Monate vorher von diesem das Einvernehmen mit dem BM.I herzustellen.