Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP
Post and Telecommunications Surveillance Service

INFORMATIVE ONLY

Summary and description of the changes brought to the VD-ÜPF Annex 1 version 1.1 "Technical requirements for the handover interfaces for the conduct of the Surveillance of Telecommunications" of March 1st, 2019

Introduction and scope

This document is informative only and intends to summarize the main changes proposed to the new version 1.1 of the VD-ÜPF Annex 1 "Technical requirements for the handover interfaces for the conduct of the Surveillance of Telecommunications" and bring some description and background information. As the version 1.1 will replace the version 1, the numbering of the sections remains identical in order to facilitate the comparison and the references between the previous version 1 and the new version 1.1. The sections that are abrogated in the new version 1.1 are kept with the title "Void".

Editorial changes and corrections of spelling mistakes are not mentioned in this summary.

Replaced the term "order" by "instruction". As "order" is used for the warrant sent from the prosecutor office to the PTSS.

1. Scope of application
No change.

2. Abbreviations
Added "BSSID", "CS"
Replaced "ISC-EJPD" by "ISC-FDJP"

3. Definitions
No change.

4. Administrative Handover Interfaces
Tables 4-1 and 4-2: New version of ETSI TS 102 657 V1.22.1 and editorial changes.

4.2.2 HI-1 XML over HTTP administrative interface for instructing real-time interceptions

Following the technical developments in the IKT-ProgFMÜ-P1 project and the corresponding changes requests approved at the ETSI TC LI#48, the HI-A interface refers to the new version ETSI TS 102 657 V1.**22**.1. In the same context, to ease the accounting/invoicing there was a need to add a new field "ExternalIdentifier" in the HI-1 object of ETSI TS 103 120 V1.2.1. This field "ExternalIdentifier" will allow the correlation of several LITask with different LIID.

Removed the attributes "Rejected", "Expired", "Invalid" from the dictionary Status and Desired Status.
Removed the "ProvisioningTime" from the Time Span.

Following the entry into force of the PTSS Testing Concept V1-0 on July 1st, 2018, the field "Flags" refers to a new dictionary "FlagsStatus" with the following new values that are

aligned with the PTSS Testing Concept. The new dictionary authorized values are: Normal, TEST_PTE, TEST_PTSA, TEST_PTSE, TEST_PTSTR, TEST_PTSTE, TEST_CTT, TEST_ATT

Following the technical developments in the IKT-ProgFMÜ-P1 project and to avoid any potential ambiguity about the instance to which the interceptions results shall be delivered, the new field "`DeliveryProfile`" is added in the LITask object.
New dictionary name "`DeliveryProfile`" with authorized values: Production, Integration_1,
Integration_2

4.2.3 Ad hoc HI-1 XML over HTTP administrative interface for intructing the real-time interceptions
Added the "`ExternalIdentifier`", "`FlagStatus`" and "`DeliveryProfile`" as in section 4.2.2 above.

Removed the attributes "`Rejected`", "`Expired`", "`Invalid`" and "`ProvisioningTime`" as in section 4.2.2 above.

4.2.3.9 Ad hoc HI-1 interface format and coding of real-time interception simple activation and deactivation
Figure 4-11: New labels to the message types and corrected the transaction identifiers examples. Examples were corrected according to the general amendments.

Added new sub-section 4.2.3.9.9. with an example for error message.

4.3 Secure Email Exchange
Changes of Figure 4-12, 4-13, 4-14, 4-15, 4-17. Messages names and "Content" descriptions were amended.

5. Target Identifiers
Editorial changes.

6. Real-time Surveillance (Lawful Interception)

6.3.10 Access Network Information for IMS-based services
New section about the P-Access-Network-Info in SIP for IMS-based services.

6.5.2.2 ETSI TS 133 108 V13.5.0 requirements and options for the packet switched domain
Added that SIP and XCAP messages must be copied in the IRI records delivered to the LEMF.

6.5.3   ETSI TS 102 232-1 V3.11.1 Handover specification for IP delivery
For IP/TCP delivery of interceptions data with ETSI TS 102 232-1, it is added that PTSS will provide to the CSP the TCP port number that shall be used for the different services.

6.6 Applicable ASN.1 module versions for real-time interceptions
Adding that ASN.1 module OID shall always be delivered.

7. Historical Data (Retroactive Surveillance)

Following the technical developments in the IKT-ProgFMÜ-P1 project and the corresponding changes requests approved at the ETSI TC LI#48, the HI-A and HI-B interfaces refer to the new version ETSI TS 102 657 V1.**22**.1 and its associated XML schema version "RDMessagever20.xsd".

7.1 General
Along the technical developments in the IKT-ProgFMÜ-P1 Retained Data Component (RDC) it was agreed to alter the initial retained data service model by integrating the "Telephony" service in the "Synchronous Multi-media" service. This allows for the simplification of the request/response model by using only one multi-media type of request and response for all telephony and multi-media services.

7.2 Historical data (retroactive) interception types
Adapted the tables 7-2, 7-3, 7-4 by removing the "Telephony" service (ETSI TS 102 657 V1.22.1 Annex B).

7.3.1 XML elements of the header for historical data requests by PTSS
Amended `rdHeaderId` parameter with the new version 0.4.0.2.3.0.20

To align with the HI-1 and LITask objects for real-time interceptions orders (see section 4) the new elements "`externalIdentifier`" and "`requestFlag`" have been added in the request headers of HI-A, table 7-5.

The `requestParameters` structure was extended with the requestConstraints "`isAMemberOf`".

The `deliveryPointHIB` was amended with the URI, Email address and the Civic address example.

7.3.2 XML elements of the header for retained data responses by CSP
Amended `rdHeaderId` parameter with the new version 0.4.0.2.3.0.20

7.4.1 Void
This section previously for "Telephony" service is abrogated. The necessary "Telephony" elements (SMS, MMS, etc…) are newly implemented in the "Multimedia" section 7.4.3.

7.4.2 HD_30_EMAIL Asynchronous message service usage request and responses
The "`msgStoreID`" element is specified as a "string" and not as a "hexBinary" in the XML schema.
The request uses only the `msgTransmission` type.

7.4.3 HD_29_TEL Multimedia service usage request and responses
Requests and responses support retained data telephony and multimedia service usage.

7.4.3.1 Multimedia service usage request criteria elements and structure
Changes to the elements and structures: `iMSI, iMEI`

7.4.3.2 Multimedia service usage response elements
The multimedia response is extended with the following elements and structures in order to support the "telephony" service values and the new IMS-based VoIP services: `partyRole,`

```
natureOfAddress, iMSI, partyNumber, eCGI, tAI,
userLocationInformation, bSSID, paniHeaderContent,
privateUserIdentity, iMEI, communicationType, bearerService,
smsInformation, mmsInformation
```

7.4.4 HD_28_NA Network access service usage request and responses

7.4.4.1 Network access service usage request criteria elements and structure
Changes to the elements and structures: `naAuthID, ePSInformation, iMEISV`

7.4.4.2 Network access service usage response elements
The "Location" structure is extended with: `bSSID` (for WLAN access)

7.4.5 HD_31_PAGING & EP_35_PAGING Proprietary handover interface for the delivery of the last active location
Added a new step (3) in Table 7 where PTSS issues and sends the corresponding request as specified in section 7.4.5.1

New sub-sections 7.4.5.1 for the request elements definition and 7.4.5.2 for the response with the table parameters.

7.4.5.1 Paging request elements
New request definition for HD_31_PAGING and EP_35_PAGING

7.4.5.2 Table of parameters to be delivered for the last active location
Table 7-8 placed in this new sub-section.

7.4.6 AS_32_PREP_COV Network analysis in preparation of a search by cell coverage area (NEW section)

7.4.6.1 Network analysis preparation request elements
New request definition.

7.4.6.2 Network analysis preparation response elements
New response definition.

7.4.7 AS_33_PREP_REF Determination of reference calls or sessions in preparation of a search by cell coverage area (NEW section)

7.4.7.1 Reference calls or sessions preparation request elements
New requests definition for Multimedia & telephony request and Networks access request.

7.4.7.2 Reference calls or sessions preparation response elements
New responses definition for Multimedia & telephony response and Networks access response.

7.4.8 AS_34 & AS_34_MORE Search by cell coverage area by mobile telephony and network access (NEW section)

7.4.8.1 Search by cell coverage area requests
New requests definition for Multimedia & telephony request and Network access request.

<u>7.4.8.2 Search by cell coverage area responses</u>
Responses adaptation.

7.4.9 EP_38_HD Combined network access and multimedia service usage for emergency paging (NEW section)

<u>7.4.9.1 Combined network access and multimedia service usage request criteria elements and structure</u>
New requests definition for Multimedia & telephony request and Network access request.

<u>7.4.9.2 Combined network access and multimedia service usage response elements</u>
New responses definition for Multimedia & telephony response and Networks access response.

7.5 Historical data handover interface requirements and options
Added guidance for procedure in case of no response is received to an HTTP POST.

Amended that the Third-Party CSP ID is not supported.

Precisions about the configuration of HI-A and HI-B interfaces:
      Mutual client/server
      HTTP POST method
      HTTP content-type: text/xml
      XML Schema definition

7.6 Applicable XML schema version for historical data interceptions
New version of the XML schema: RDMessagever20.xsd.
With the changes of some elements values definition: use of "string" in CH instead of "hexBinary" for the following elements: `MsgSubscriberID, MsgStoreID, MultimediaBillingIdentifier, MultimediaDeviceID`

8. Information Requests
Along the technical developments in the IKT-ProgFMÜ-P1 Information Requests Component (IRC) it was agreed to alter the initial retained data service model by integrating the "Telephony" service in the "Synchronous Multi-media" service. This allows the simplification of the request/response model by using only one multi-media type of request and response for all telephony and multi-media services.

8.2 Information request types
Adapted the tables 8-1, 8-2, 8-3 by removing the reference to the "Telephony" service (ETSI TS 102 657 V1.22.1 Annex B).

IR_17_PAY, IR_18_ID, IR_19_BILL, IR_20_CONTRACT uses only the Multi-media service for all the requests.

8.3.1 XML elements of the header for information requests by PTSS
To align with the HI-1 and LITask objects for real-time interceptions orders (see section 4) the new fields "`externalIdentifier`" has been added in the request headers of HI-A, table 8-4.

As there is no priority attribute and test targets in the Information Requests, the `requestFlag` and `requestPriority` parameters were removed from the requestMessage.

The `deliveryPointHIB` element was amended with the URI.

8.3.2 XML elements of the header for information responses by CSP

The `rdHeaderId` element was updated to the latest version.

8.4   Formats and coding requirements for information requests

8.4.1   Network access information requests and responses

Adapted all the information requests and responses elements and structure to the RDMessagever20.xsd as per the latest developments and amendments in the IKT-ProgFMÜ-P1 IRC.

8.4.1.1 IR_4_NA & IR_5_NA_FLEX request criteria elements and structure for subscription information
Changes to the elements and structures: `options, registeredICCIDs, allocatedDevices, OrganizationInfo, IndividualInfo`

8.4.1.2 IR_4_NA & IR_5_NA_FLEX response elements and structure for subscription information
Allowed the Multi-Device & Multi-IMSI subscription information.
Changes to the elements and structures: `naProviderID, naAuthID, iMSI, OrganizationInfo, registeredICCIDs, AddressInformation, AuthenticationInfo`

8.4.1.3 IR_6_NA request criteria elements and structure for service information
Changes to the elements and structures: `IMSI, IMEI, subscriberID`

8.4.1.4 IR_6_NA response elements and structure for service information
Allowing the Multi-Device & Multi-IMSI subscription information.
Changes to the elements and structures: `IMSI, registeredICCID, naDeviceId, IMEI, registeredICCIDs`

8.4.1.5 IR_7_NA request criteria elements and structure for identification of a user by its unique assigned IP address
Changes to the element and structure: `assignedTime`

8.4.1.6 IR_7_NA response elements and structure for identification of a user by its unique assigned IP address
Changes to the elements and structures: `naAuthID, subscriberID, naDevice`

8.4.1.7 IR_8_IP (NAT) request criteria elements and structure for identification of a user by its shared assigned IP address
Changes to the element and structure: `validity`

<u>8.4.1.8 IR_8_IP (NAT) response elements and structure for identification of a user by its shared assigned IP address</u>
Changes to the elements and structures: `naAuthID`, `endReason`, `NAEndReason`, `subscriberID`, `naDevice`

<u>8.4.1.9 IR_9_NAT request criteria elements and structure for network access translation information</u>
Changes to the element and structure: `validity`

8.4.2   Multimedia and telephony information requests and responses

As the "Telephony" service is integrated in the "Multi-media" service the reference to the Annex B of ETSI TS 102 657 V1.22.1 was removed.

<u>8.4.2.1 IR_10_TEL & IR_11_TEL_FLEX request criteria elements and structure for subscription information</u>
Changes to the elements and structures: `OrganizationInfo`, `otherAdresses`, `IndividualInfo`, `registerICCIDs`

<u>8.4.2.2 IR_10_TEL & IR_11_TEL_FLEX response elements and structure for subscription information</u>
Allowing the Multi-Device & Multi-IMSI subscription information.
Changes to the elements and structures: `OrganizationInfo`, `IndividualInfo`, `providerID`, `serviceType`, `connectionDate`, `iMSI`, `subscriptiontype`, `registeredICCIDs`

<u>8.4.2.3 IR_12_TEL request criteria elements and structure for service information</u>
Changes to the elements and structures: `registeredICCID`, `iMEIs`, `privateUserIdentities`, `allocatedDeviceIDs`

<u>8.4.2.4 IR_12_TEL response elements and structure for service information</u>
Allowing the Multi-Device & Multi-IMSI subscription information.
Changes to the elements and structures: `registeredICCIDs`, `iMEIs`, `privateUserIdentities`, `allocatedDeviceIDs`

<u>8.4.2.5 Void</u>
This section previously for "Telephony" service was abrogated. The necessary "Telephony" subscription information elements were implemented in the "Multimedia" section 8.4.2.3.

<u>8.4.2.6 Void</u>
This section previously for "Telephony" service was abrogated. The necessary "Telephony" subscription information elements were implemented in the "Multimedia" section 8.4.2.4.

8.4.3   Message services information requests and responses

<u>8.4.3.1 IR_13_EMAIL & IR_14_EMAIL_FLEX request criteria elements and structure for subscription information</u>
Changes to the element and structure: `MsgStore`

8.4.3.2 IR_13_EMAIL & IR_14_EMAIL_FLEX response elements and structure for subscription information

Changes to the elements and structures: `msgStoreID, msgForwardingAddresses, msgStoreSubscriberRelatedIDs, OrganizationInfo, IndividualInfo`

8.4.4   Communication services information requests and responses

8.4.4.1 IR_15_COM & IR_16_COM_FLEX request criteria elements and structure for subscription information

Changes to the elements and structures: `naAuthID, allocatedDevices, OrganizationInfo`

8.4.4.2 IR_15_COM & IR_16_COM_FLEX response elements and structure for subscription information

Changes to the elements and structures: `naProviderID, naAuthID, otherAddresses, OrganizationInfo, IndividualInfo`

8.4.5   Payment details information requests and responses

8.4.5.1 Void

This section previously for "NetworkAccess" service was abrogated. The request uses only the "Multimedia" elements in the section 8.4.5.3.

8.4.5.2 Void

This section previously for "NetworkAccess" service was abrogated. The response uses only the "Multimedia" elements in the section 8.4.5.4.

8.4.5.3 IR_17_PAY request criteria elements and structure for payment details

Changes to the elements and structures: `providerID, bIC, nationalBankNumber, billingIdentifier`

8.4.5.4 IR_17_PAY response elements and structure for payment details

Changes to the elements and structures: `providerID, bIC, nationalBankNumber, bankName, billingIdentifier`

8.4.6   Identity document copy information requests and responses

8.4.6.1 Void

This section previously for "NetworkAccess" service was abrogated. The request uses only the "Multimedia" elements in the section 8.4.6.3.

8.4.6.2 Void

This section previously for "NetworAccess" service was abrogated. The response uses only the "Multimedia" elements in the section 8.4.6.4.

8.4.6.3 IR_18_ID request criteria elements and structure for identity document copy

Changes to the elements and structures: `registeredeICCID, iMEIs, registeredeICCIDs, allocatedDeviceID`

8.4.6.4 IR_18_ID response elements and structure for identity document copy

Changed the method to provide the response by uploading the necessary document via the GUI of the Information Request Component application.

8.4.7 Billing document copy requests and responses

8.4.7.1 Void
This section previously for "NetworkAccess" service was abrogated. The request uses only the "Multimedia" elements in the section 8.4.7.3.

8.4.7.2 Void
This section previously for "NetworAccess" service was abrogated. The response uses only the "Multimedia" elements in the section 8.4.7.4.

8.4.7.3 IR_19_BILL request criteria elements and structure for billing document copy
Changes to the elements and structures: `MultimediaSubscriber`, `MultimediaSubscriberID`, `subscribedMultimediaServices`, `registeredIdentifiers`, `paymentDetails`, `iMEIs`, `allocatedDeviceIDs`

8.4.7.4 IR_19_BILL response elements and structure for billing document copy
Changed the method to provide the response by uploading the necessary document via the GUI of the Information Request Component application.

8.4.8 Contract document copy information requests and responses

8.4.8.1 Void
This section previously for "NetworkAccess" service was abrogated. The request uses only the "Multimedia" elements in the section 8.4.8.3.

8.4.8.2 Void
This section previously for "NetworkAccess" service was abrogated. The response uses only the "Multimedia" elements in the section 8.4.8.4.

8.4.8.3 IR_20_CONTRACT request criteria elements and structure for contract document copy
Changes to the elements and structures: `registeredeICCID`, `iMEIs`, `registeredeICCIDs`, `allocatedDeviceIDs`

8.4.8.4 IR_20_CONTRACT response elements and structure for contract document copy
Changed the method to provide the response by uploading the necessary document via the GUI of the Information Request Component application.

8.4.9 Technical information requests and responses

8.4.9.1 IR_21_TECH request criteria elements and structure for mobile and WLAN network access information
Changes to the element and structure: `bSSID`

8.4.9.2 IR_21_TECH response elements and structure for mobile and WLAN network access information
Changes to the elements and structures: `otherInformation`, `bSSID`

8.4.9.3 Void
This section previously for "naNwElementID" for the BSSID was abrogated. The request uses the "bSSID" element in the section 8.4.9.1.

<u>8.4.9.4 Void</u>
This section previously for "naNwElementID" for the BSSID was abrogated. The response uses the "bSSID" element in the section 8.4.9.2.

8.6   Applicable XML schema version for information requests

New version of the XML schema: RDMessagever20.xsd.
With the changes of some elements values definition: use of "string" in CH instead of "hexBinary" for the following elements: `MsgSubscriberID, MsgStoreID, MultimediaBillingIdentifier, MultimediaDeviceID`

9. Security

Editorials

10. List of Technical Specifications

Updated version of ETSI TS 102 657 V1.22.1
Added ETSI TS 124.229 V13.13.0