|  |
| --- |
|  |
|  |
|  |

|  |  |
| --- | --- |
|  |  |

|  |
| --- |
| EU Roaming regulation III  Interface & Protocol  Detailed Technical specifications  Version 1.1  Last Update 31/01/2014 |

Document History

|  |  |
| --- | --- |
| History | |
| V 0.0 | 29/01/2013: Initial version with “empty” chapters |
| V 0.1 | 10/03/2013: 1st draft version with CR already discussed (but not final) |
| V 0.2 | 19/04/2013: 2nd draft including all CR to date |
| V 0.2.1 | 19/04/2013: Adding ‘Telefonica CR for Diameter (IF1)’ and Annex for homerouting |
| V 0.3 | 21/05/2013: integration of adjusted sections (IF1, IF2, IF3,IF4 and IF5). The section will be subject to additional adjustement as agreed to F2F Meeting on May 13-14 |
| V 0.4 | 18/06/2013: integration of working assumptions, revised IF1 and IF3. |
| V 0.5 | 11/07/2013: integration of comments received from Christian (E+), Normunds (TSG), Ignacio (TEF), Fredrik (Tele2) and David (RW).  17/07/2013: includes complete document review adaptation (David)  Includes editorial (font, alignment, etc) adaptations.  22/07/2013: includes adjustments for short codes, CAMEL operation, LBO scope |
| V 1.0 | 27/07/2013: Agreement on all latest changes  Minor change on SMS ECUR flow: added Used Service Unit AVP in Termination Request |
| V1.1 | 31/01/2014: Added Description of the LBO-IF2. Amendments of the IF4 content for ensuring coherence with OMA specs, Correction of examples and removal of the storing requirement for IF4 (consistence with other interfaces). |

**Summary**

[References 7](#_Toc378975178)

[Definitions 8](#_Toc378975179)

[Abbreviations 11](#_Toc378975180)

[1 Scope 12](#_Toc378975181)

[1.1 Document structure 12](#_Toc378975182)

[1.2 Working Assumptions 14](#_Toc378975183)

[1.2.1 Generic Requirements 14](#_Toc378975184)

[1.2.2 Single IMSI implementation 15](#_Toc378975185)

[1.2.3 LBO implementation 18](#_Toc378975186)

[2 Interface definition for single imsi 19](#_Toc378975187)

[2.1 ARP – DSP Connectivity 19](#_Toc378975188)

[2.1.1 SIGTRAN 19](#_Toc378975189)

[2.2 Interface overview 25](#_Toc378975190)

[2.2.1 Generic rules for interface definition 26](#_Toc378975191)

[2.2.2 Preliminary Note 26](#_Toc378975192)

[2.3 SI-IF1 : Voice Control 27](#_Toc378975193)

[2.3.1 Description 27](#_Toc378975194)

[2.3.2 Detailed Procedures for MO Calls 27](#_Toc378975195)

[2.3.3 Detailed Procedures for MT Calls 31](#_Toc378975196)

[2.3.4 Interface Primitives 34](#_Toc378975197)

[2.3.5 Parameters, Definitions and Use 34](#_Toc378975198)

[2.3.6 Error handling 34](#_Toc378975199)

[2.4 SI-IF2 : SMS Control 36](#_Toc378975200)

[2.4.1 Context 36](#_Toc378975201)

[2.4.2 Description 37](#_Toc378975202)

[2.4.3 CAMEL for SMS Control 38](#_Toc378975203)

[2.4.4 DIAMETER 41](#_Toc378975204)

[2.4.5 Detailed Procedures at DSP 43](#_Toc378975205)

[2.4.6 Detailed Procedures at ARP 44](#_Toc378975206)

[2.4.7 Interface primitives 44](#_Toc378975207)

[2.4.8 Parameters Definitions and Use 46](#_Toc378975208)

[2.4.9 Error Handling 48](#_Toc378975209)

[2.4.10 Limitations 48](#_Toc378975210)

[2.4.11 Special Use Case: Short Code 48](#_Toc378975211)

[2.4.12 Summary table 49](#_Toc378975212)

[2.5 SI-IF3 : Data Control 50](#_Toc378975213)

[2.5.1 Architecture, Description and Definitions 50](#_Toc378975214)

[2.5.2 Definitions 52](#_Toc378975215)

[2.5.3 Detailed Procedures at DSP 52](#_Toc378975216)

[2.5.4 Interface primitives 53](#_Toc378975217)

[2.5.5 Parameters Definitions and Use 67](#_Toc378975218)

[2.5.6 Error Handling 67](#_Toc378975219)

[2.5.7 Summary table 68](#_Toc378975220)

[2.6 SI-IF4 : Mobility Control 69](#_Toc378975221)

[2.6.1 Description 69](#_Toc378975222)

[2.6.2 Detailed Procedures at DSP 69](#_Toc378975223)

[2.6.3 Detailed Procedures at ARP 69](#_Toc378975224)

[2.6.4 Interface primitives 70](#_Toc378975225)

[2.6.5 Parameters Definitions and Use 71](#_Toc378975226)

[2.6.6 Error Handling 76](#_Toc378975227)

[2.7 SI-IF5 : USSD Control 78](#_Toc378975228)

[2.7.1 Description 78](#_Toc378975229)

[2.7.2 Detailed Procedures at DSP 79](#_Toc378975230)

[2.7.3 Detailed Procedures at ARP 80](#_Toc378975231)

[2.7.4 Interface primitives 80](#_Toc378975232)

[2.7.5 Parameters Definitions and Use 81](#_Toc378975233)

[2.7.6 Error Handling 82](#_Toc378975234)

[2.8 SI-IF9 : SMS Wholesale Interface (MO+MT) 83](#_Toc378975235)

[2.8.1 Description 83](#_Toc378975236)

[2.8.2 Detailed Procedures at ARP 83](#_Toc378975237)

[2.8.3 Detailed Procedures at DSP 84](#_Toc378975238)

[2.8.4 Interface primitives 84](#_Toc378975239)

[2.8.5 Parameters Definitions and Use 86](#_Toc378975240)

[2.8.6 Error Handling 86](#_Toc378975241)

[3 Interface definition for LBO 87](#_Toc378975242)

[3.1 Assumptions 87](#_Toc378975243)

[3.2 Interface overview 87](#_Toc378975244)

[3.3 LBO-IF1 : Mobility / Profile Control 88](#_Toc378975245)

[3.3.1 Description 88](#_Toc378975246)

[3.3.2 Detailed Procedures at HPMN 88](#_Toc378975247)

[3.3.3 Detailed Procedures at LBO 89](#_Toc378975248)

[3.3.4 Interface primitives 90](#_Toc378975249)

[3.3.5 Parameters Definitions and Use 91](#_Toc378975250)

[3.3.6 Error Handling 92](#_Toc378975251)

[3.4 LBO-IF2 : LBO notification interface 93](#_Toc378975252)

[3.4.1 Description 93](#_Toc378975253)

[3.4.1.1 Interface Setup Description 93](#_Toc378975254)

[3.4.1.2 Information Exchange Description 94](#_Toc378975255)

[3.4.2 Implementation Details 95](#_Toc378975256)

[3.4.2.1 Prerequisites 95](#_Toc378975257)

[3.4.2.2 Implementation Approach Samples 96](#_Toc378975258)

[3.4.3 Detailed Procedures at HPMN 97](#_Toc378975259)

[3.4.4 Detailed Procedures at LBO 97](#_Toc378975260)

[3.4.5 Interface primitives 98](#_Toc378975261)

[3.4.6 Message Details 98](#_Toc378975262)

[3.4.6.1 MAP SRI-SM 98](#_Toc378975263)

[3.4.6.2 MAP SRI-SM ACK 98](#_Toc378975264)

[3.4.6.3 MAP MT-FWD-SM or FWD-SM 99](#_Toc378975265)

[3.4.7 Error Handling 101](#_Toc378975266)

[3.4.8 Security Note 101](#_Toc378975267)

[3.5 ANNEX - Study on Home Routing and Legal interception cases 102](#_Toc378975268)

[3.5.1 DSP Home Routing – CAP v1 102](#_Toc378975269)

[3.5.2 DSP Home Routing – CAP v2 103](#_Toc378975270)

[3.5.3 ARP Home Routing – CAP v1 104](#_Toc378975271)

[3.5.4 ARP Home Routing – CAP v2 105](#_Toc378975272)

[3.5.5 Legal Interception 106](#_Toc378975273)

[3.5.6 Summary of the solutions 106](#_Toc378975274)

**Figures**

[Figure 1 – Requirement hierarchy & classification 12](#_Toc379143536)

[Figure 2 – Overview: IP transport for different protocols 19](#_Toc379143537)

[Figure 3– M3UA stack overview 20](#_Toc379143538)

[Figure 4 – the communication between two SIGTRAN M3UA nodes in the OSI layer model 20](#_Toc379143539)

[Figure 5 – M2PA stack overview 21](#_Toc379143540)

[Figure 6 – The Communication between two SIGTRAN / M2PA nodes in the OSI layer model 21](#_Toc379143541)

[Figure 7 – SCTP Multihoming (IP) – option 1 22](#_Toc379143542)

[Figure 8 – SCTP Multihoming (SPC) – option 1 22](#_Toc379143543)

[Figure 9 – SCTP Multihoming (IP) – option 2 23](#_Toc379143544)

[Figure 10 – SCTP Multihoming (SPC) – option 2 23](#_Toc379143545)

[Figure 11 – SCTP Multihoming (IP) – option 3 23](#_Toc379143546)

[Figure 12 – SCTP Multihoming (SPC) – option 3 24](#_Toc379143547)

[Figure 13 – Single IMSI interface definition 25](#_Toc379143548)

[Figure 14 – Generic rules for function mapping 26](#_Toc379143549)

[Figure 15 – Voice / CAMEL architecture and associated functions 27](#_Toc379143550)

[Figure 16 – Sequence diagram for SCCP level relay of CAMEL operations (option 1) 29](#_Toc379143551)

[Figure 17 – Sequence diagram for MO call handling with separate CAMEL dialogues 30](#_Toc379143552)

[Figure 18 – Sequence diagram for MT call handling with separate CAMEL dialogues 32](#_Toc379143553)

[Figure 19 – Sequence diagram for Anti trombone solution 33](#_Toc379143554)

[Figure 20 – SMS architecture and associated functions 37](#_Toc379143555)

[Figure 21 – Generic SMS interception mechanism for online charging 37](#_Toc379143556)

[Figure 22 – SMS control over CAMEL (existing roaming agreement) 39](#_Toc379143557)

[Figure 23 – SMS control over CAMEL (MAP intercept) 40](#_Toc379143558)

[Figure 24 – SMS control over Diameter (MAP intercept and IEC mode) 42](#_Toc379143559)

[Figure 25 – SMS control over Diameter (MAP intercept and ECUR mode) 43](#_Toc379143560)

[Figure 26 – Data architecture and associated functions 50](#_Toc379143561)

[Figure 27 – MMS architecture and associated functions 51](#_Toc379143562)

[Figure 28 – Start of Data Session call flow: control at PDP context creation 54](#_Toc379143563)

[Figure 29 – Start of Data Session call flow: control at first packet received 55](#_Toc379143564)

[Figure 30 – Start of Data Session call flow: split authentication and quota management 56](#_Toc379143565)

[Figure 31 – Middle of Data Session call flow 57](#_Toc379143566)

[Figure 32 – Termination of Data Session call flow (user-termination) 58](#_Toc379143567)

[Figure 33 – Termination of Data Session call flow (ARP-termination)- case 1 59](#_Toc379143568)

[Figure 34 – Termination of Data Session call flow (ARP-termination) - case 2 60](#_Toc379143569)

[Figure 35 – MMS MO using IEC without quota management for data volume 61](#_Toc379143570)

[Figure 36 – MMS MO using IEC with quota management for data volume 62](#_Toc379143571)

[Figure 37 – MMS MT using IEC 64](#_Toc379143572)

[Figure 38 – MMS MT using ECUR 66](#_Toc379143573)

[Figure 39 – Mobility management architecture and associated functions 69](#_Toc379143574)

[Figure 40 - Roaming status change notification 70](#_Toc379143575)

[Figure 41 – Architecture of USSD Services 78](#_Toc379143576)

[Figure 42 – IF5 USSD interface 79](#_Toc379143577)

[Figure 43 – MO/MT SMS architecture and associated functions 83](#_Toc379143578)

[Figure 44 – Typical SMPP request/response sequence for an SMS from ARP to DSP 85](#_Toc379143579)

[Figure 45 – Typical SMPP request/response sequence for an SMS from DSP to ARP 85](#_Toc379143580)

[Figure 46 – LBO interface definition 87](#_Toc379143581)

[Figure 47 – GLR – HLR interface 90](#_Toc379143582)

[Figure 48 – Update GPRS Location call flow 92](#_Toc379143583)

[Figure 49 – Notification flow between LBO-V and LBO-H 94](#_Toc379143584)

[Figure 50 – Implementation example: LBO-V using a SMS-C to communicate with LBO-H 96](#_Toc379143585)

[Figure 51 – Implementation example: LBO-V communicating directly with LBO-H 97](#_Toc379143586)

[Figure 52 – DSP Home Routing with CAP v1 interface to ARP 102](#_Toc379143587)

[Figure 53 – DSP Home Routing with CAP v2 interface to ARP 103](#_Toc379143588)

[Figure 54 – ARP Home Routing with CAP v1 interface to ARP 104](#_Toc379143589)

[Figure 55 – ARP Home Routing with CAP v2 interface to ARP 105](#_Toc379143590)

## References

1. Regulation (EU) No 531/2012 of the European Parliament and the Council of 13 June 2012 on roaming on public mobile communications networks within the Union
2. Regulations, Commission Implementing Regulation (EU) No 1203/2012 of 14 December 2012 on the separate sale of regulated roaming services within the Union

Following documents are for information only (given for supporting the consultation).

No binding requirements should be derived from there.

1. BoR (12) 68: ROAMING REGULATION - CHOICE OF DECOUPLING METHOD: A consultation to assist BEREC in preparing advice to the Commission on its forthcoming Implementing Act, June 2012, 72 pages.
2. BoR (12) 109: ROAMING REGULATION - CHOICE OF DECOUPLING METHOD, BEREC opinion on article 5 implementing act, 27 Sept 2012, 7 pages
3. BoR (13) 82: BEREC GUIDELINES ON ROAMING REGULATION (EC) NO 531/2012 (THIRD ROAMING REGULATION) (Articles 4 and 5 on Separate Sale of Roaming Services)
4. 3GPP TS 32.240, Telecommunication management; Charging management; Charging architecture and principles
5. 3GPP TS 22.011: Service accessibility
6. 3GPP TS 23.122: Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode
7. EU Roaming regulation III, Structural Solutions, High Level Technical specifications v1.0

## Definitions

Below mentioned definitions are adopted by 3GPP TS 32.240 [5] “Charging architecture and principles” and “Implementation Act”

|  |  |  |
| --- | --- | --- |
| **alternative roaming provider**: a roaming provider different from the domestic provider; It can be single IMSI alternative roaming provider – named ARP or LBO roaming provider - called LBO provider. | |  |
| **billing:** function whereby CDRs generated by the charging function(s) are transformed into bills requiring payment; | |  |
| **call control function (CCF)**: CCF is the Call Control Function in the network that provides call/service processing and control (see ITU-T Recommendation Q.1224) | |  |
| **CAMEL:** network feature that provides the mechanisms to support operator specific services even when roaming outside HPLMN; | |  |
| **charging data record (CDR):** formatted collection of information about a chargeable event (e.g. time of call set-up, duration of the call, amount of data transferred, etc) for use in billing and accounting. For each party to be charged for parts of or all charges of a chargeable event a separate CDR shall be generated, i.e. more than one CDR may be generated for a single chargeable event, e.g. because of its long duration, or because more than one charged party is to be charged; | |  |
| **charging:** function within the telecommunications network and the associated OCS/BD components whereby information related to a chargeable event is collected, formatted, transferred and evaluated in order to make it possible to determine usage for which the charged party may be billed (offline charging) or the subscriber’s account balance may be debited (online charging); | |  |
| **circuit switched domain:** domain within GSM / UMTS in which information is transferred in circuit switched mode; | |  |
| **domestic provider**: an undertaking that provides a roaming customer with domestic mobile communications services;  **domestic provider or Domestic Service Provider (DSP)**: an undertaking that provides a roaming customer with domestic mobile communications services - Mobile Network Operator or a Mobile Virtual Network Operator. | |  |
| **donor roaming provider:** the roaming provider, that is currently providing roaming services to a customer; | |  |
| **EUInternet access point name (APN):** a common identifier set, manually or automatically, in the roaming customer's mobile device and recognized by the home network and visited network to indicate the roaming customer's choice to use local data roaming services (LBO Provider); | |  |
| **home network / HP(L)MN**: a public communications network located within a Member State and used by the roaming provider for the provision of regulated retail roaming services to a roaming customer. The MCC+MNC of the customer's IMSI corresponds to a MCC+MNC of this network's identity. | |  |
| **local data roaming service:** a regulated data roaming service provided, temporarily or permanently, to roaming customers directly on a visited network, by an alternative roaming provider without the need for roaming customers to change their SIM card or mobile device; | |  |
| **mobile number portability:** The ability for a mobile subscriber to change subscription network within the same country whilst retaining their original MSISDN(s). | |  |
| **network barring:** a control function used by the home network operator aimed at avoiding the selection of certain visited networks for its roaming customers; | |  |
| **offline charging:** charging mechanism where charging information **does not** affect, in real-time, the service rendered. | |  |
| **online charging system:** the entity that performs real-time credit control. Its functionality includes transaction handling, rating, online correlation and management of subscriber accounts/balances. | |  | | |
| **online charging:** charging mechanism where charging information can affect, in real-time, the service rendered and therefore a direct interaction of the charging mechanism with bearer/session/service control is required. | |  |
| **packet switched domain:** domain in which data is transferred between core network elements. | |  |
| **premium service**: call from VPLMN to premium rate service or value added service number of the VPLMN country; call to destination in EU, where the interconnection cost is not regulated on national termination market, including in the VPLMN country | |  |
| **real-time:** real-time charging and billing information is to be generated, processed, and transported to a desired conclusion in less than 1 second. | |  |
| **recipient roaming provider:** a roaming provider, that will provide roaming services instead of roaming services currently provided by the donor roaming provider after the change of roaming provider; | |  |
| **resale of retail roaming services:** a provision of regulated roaming services, provided as a bundle, and associated services, such as voice mailbox services, that are usually available to roaming customers, without the need for roaming customers to change their SIM card or mobile device, in accordance with a wholesale agreement concluded between an alternative roaming provider and a domestic provider; | |  |
| **retail charging**: see charging | |  |
| **roaming customer:** a customer of a roaming provider of regulated roaming services, by means of a terrestrial public mobile communications network situated in the Union, whose contract or arrangement with that roaming provider permits Union-wide roaming | |  |
| **roaming provider**: an undertaking that provides a roaming customer with regulated retail roaming services; | |  |
| **roaming:** The ability for a user to function in a serving network different from the home network. The serving network could be a shared network operated by two or more network operator. | |  |
| **traffic steering**: a control function used by the home network operator aimed at the selection of visited networks for its roaming customers based on a priority list of preferred visited networks; | |  |
| **union-wide roaming**: the use of a mobile device by a roaming customer to make or receive intra-Union calls, to send or receive intra-Union SMS messages, or to use packet switched data communications, while in a Member State other than that in which the network of the domestic provider is located, by means of arrangements between the home network operator and the visited network operator; | |  |
| **visited network /VP(L)MN**: a public mobile communications network located within a Member State other than that of the roaming customer’s HPLMN that permits a roaming customer to make or receive calls, to send or receive SMS messages or to use packet switched data communications, by means of arrangements with the home network operator. The MCC+MNC of the customer's IMSI does not correspond to a MCC+MNC of this network's identity. | |  |

## Abbreviations

3GPP Third Generation Partnership Project

APN Access Point Name

ARP Alternative Roaming Provider

BEREC Body of European Regulators for Electronic Communications

CAP CAMEL Application Part

CC Country Code

CDR Charging Data Record

CF Call Forwarding

CS Circuit Switched

DSP Domestic Service Provider

ESME External Short Message Entity

EU Member States of the European Union, the outermost regions of the European Union and countries adopting Regulation

FQDN Fully Qualified Domain Name

GGSN Gateway GPRS Service Node

GSM Global System for Mobile communication

GSMA GSM Association

GT Global Title

HLR Home Location Register

HPMN Home Public Mobile Network

IANA Internet Assigned Numbers Authority

IF Interface

IMSI International Mobile Subscriber Identity

IP Internet Protocol

ITU International Telecommunication Union

LBO Local (Data) Break Out

LTE Long Term Evolution

MAP Mobile Application Part

ME Mobile Equipment

MMS Multimedia Messaging Service

MFC Mobile Forwarded Call

MOC Mobile Originating Call

MSISDN Mobile Subscriber ISDN Number

MTC Mobile Terminating Call

MNO Mobile Network Operator

MVNO Mobile Virtual Network Operator

MVNE MVNO Enabler

NDC National Destination Code

NNI Network to Network Interface

NRA National Regulatory Authority

OCS On-line Charging System

ORLCF Optimal Routing Late Call Forwarding

OTA Over The Air

PDP Packet Data Protocol

QoS Quality of Service

RG Rating Group

SGSN Serving GPRS Support Node

SIM Subscriber Identity Module

SMS Short Messaging Service

SMSC Short Message Service Center

TAP Transferred Account Procedure

TBC To Be Confirmed

TBD To Be Defined

USSD Unstructured Supplementary Services Data

VLR Visited Location Register

VPMN Visited Public Mobile Network

# Scope

The objective of this document is to describe the detailed technical specifications defining the interface and protocols supporting the implementation of the roaming unbundling for EU roaming regulation III.

The document relies on interface requirement defined in the high level architecture document.

The HL document identifies basic requirements for securing the implementation of the regulation and the service decoupling between the DSP and the ARP.

The reader is invited to refer to this document for getting a complete understanding of the set of requirements, obligations, etc related to the Regulation III.



Customer

End User Services

(Associated use cases)

Architecture Definition & Specifications

(Functional architecture, interface definition, function mapping)

Detailed Design

(Interfaces & protocols)

Detailed Design

(Billing & Provisioning)

Detailed Design

(Processes)

Operator Obligations

(Interface, function)

Figure 1 – Requirement hierarchy & classification

## Document structure

The core of this document contains detailed definition of the following interfaces (with associated use cases)

* + Single IMSI interfaces: IF1, IF2, IF3, IF4, IF5 and IF9
  + LBO interfaces : IF1 and IF2

Additionally a test book will be provided as a separate document to list out procedures and scenarios in order to validate those interfaces.

Each section of this document covers usually the following outline:

* Context
  + This section explains the roaming environment for the interface being defined.
* Description
  + This section explains the role of the interface, call flows and implementation challenges to be addressed.
  + The call flows usually show only the relevant fields applicable for enabling the separation of retail sales.
* Detailed Procedures at DSP
  + This section explains how the DSP triggers the interface and the actions to be taken upon receiving the answer from the ARP.
  + It includes procedures related to error handling.
* Detailed Procedures at ARP
  + This section explains the actions to be taken upon receiving the initial trigger from the DSP.
  + It includes procedures related to error handling.

* Interface primitives
  + This section highlights the primitives relevant when using the interface between the ARP and the DSP. The associated details can be found in the relevant 3GPP or OMA standards.
* Parameters Definitions and Use
  + This section highlights the field / parameters that are used in the protocol(s) for enabling the decoupling of roaming.
* Summary table
  + This section captures the information which is expected to be exchanged between the DSP and ARP for setting up and maintaining the interface.

**Important**: This document will contain obligation and option.

* “Shall” will describe an obligation
* “May” will describe an option

## Working Assumptions

The purpose of this section is to explain the working assumptions for ensuring the decoupling of retail roaming services in the context of Single IMSI or Local Data Break-Out implementations.

It will clarify the expected information and identifiers to be shared by the involved parties: end-user, Domestic Service Provider (DSP), Alternative Roaming Provider (ARP) or Local Data Break-Out Provider (LBO).

## Generic Requirements

* + - 1. Decoupling Solution Failure

It is expected the roaming services will be interrupted in case of the unavailability of the solution enabling the decoupling of the retail roaming services when the customer uses the roaming services offered by an ARP or an LBO provider.

This ensures the retail and wholesale charges are always aligned.

The DSP and ARP may agree to continue serving customers in case of failure of the decoupling solution and will have appropriate dispute resolution procedure in place.

* + - 1. Activity termination at ARP/DSP Registration

The DSP may have the ability to terminate the on-going activity of a subscriber when the change of roaming provider happens when the subscriber roams.

There are multiple ways to realize such termination mechanism as described in standard specifications and fraud-handling document. This is out of scope of this document.

* + - 1. No discrimination principle

The DSP shall not alter the profile characteristics determining the quality of service of the roaming subscribers when swapping to ARP or to LBO provider.

In the case of LBO, the DSP shall provide the EUinternet APN with the same QoS settings as the internet service for his roaming subscribers using the usual HPMN APN for accessing the internet.

The DSP may restrict access to supplementary services that provides capability beyond the roaming scope (e.g. multi-party call, call hold/call wait, etc).

## Single IMSI implementation

The online interfaces that are defined further in this document enable a real-time charging and management of the customer (mobility) at the ARP.

* + - 1. Architecture

Inside the Single IMSI architecture, the following parameters shall be unique and controlled by the DSP

* HLR to VLR SS profile,
* SMSC address,
* APN for data services,
* PCRF parameters
  + - 1. Conditions for triggering the Proxies for enabling separation of sale

The following table summarizes the conditions to be fulfilled for triggering the corresponding interface.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IF | Event | Subscriber | Location | Destination | Type |
| IF1 | MOC | Calling subscriber belongs to ARP | In ARP coverage | In ARP destination set | In ARP call type |
| IF1 | MFC | Redirecting subscriber belongs to ARP | In ARP coverage | In ARP destination set | In ARP call type |
| IF1 | MTC | Called subscriber belongs to ARP | In ARP coverage | n.a. | In ARP call type |
| IF2 | SMS-MO | Calling subscriber belongs to ARP | In ARP coverage | In ARP destination set | n.a. |
| IF3 | DATA | Data Session initiator  belongs to ARP | In ARP coverage | n.a. | n.a. |
| IF3 | MMS-MO | Data Session initiator  belongs to ARP | In ARP coverage | In ARP destination set | n.a. |
| IF3 | MMS-MT | Recipient of the MMS belongs to ARP | In ARP coverage | n.a. | n.a. |
| IF4 | Mobility | Moving subscriber belongs to ARP | In ARP coverage | n.a. | n.a. |
| IF5 | ARP USSD | Dialing subscriber belongs to ARP | Any or depending on the USSD service – only in ARP coverage (\*) | Using USSD code designated for ARP | n.a. |
| IF5 | DSP USSD | Dialing subscriber belongs to ARP | Any or depending on the USSD service – only in DSP coverage (\*) | Using USSD designated for DSP | n.a. |

(\*): in case of USSD interface is used for triggering USSD Call back service (offered by DSP or ARP), the DSP may apply a location control validating whether the roamer is in the ARP/DSP coverage.

The invocation at DSP and the control at the ARP requires at least:

* Subscriber identification
* Location information
* Event type and destination

The definition and relevant parameters are defined in the following sections.

* + - 1. The subscriber identification

The subscriber shall be identified by its MSISDN wherever possible.

The subscriber MSISDN shall be used as the primary identifier of a subscription on interfaces between DSP and ARP. Where a MSISDN is not associated with the subscription, IMSI shall be used. It shall be possible for MSISDN and IMSI to both be included in protocol messages, but it is not mandatory to include both under any circumstance.

Note: it is expected that Dual-IMSI implementation providing roaming enablement via a sponsor IMSI should not affect the decoupling implementation because:

* The primary MSISDN of the customer remains usually available;
* The HPMN is still involved in the subscriber authentication and registration procedures as well as the online charging activity. The IMSI-HPMN and IMSI-Sponsor mapping is usually applied at the Sponsor operator.
  + - 1. The location information

The DSP and the ARP shall agree on the ARP roaming coverage i.e. the set of roaming locations where the customer is controlled by the ARP.

The minimum set of locations consists of the mobile networks located in countries where the EU Regulation applies. The DSP and ARP may extend the scope of the ARP coverage.

The observable location information of the roaming customer depends on the call event and the roaming implementation at the DSP, and between the HPMN and the VPMN.

For example, the roaming arrangement using Roaming Hubs may affect the information passed to the ARP.

In the context of CS-domain, the relevant information is the MSC/VLR Global Title of the core network node serving the customer.

The Global Title (or its range) used by the VPMN is defined in the roaming agreement between the HPMN and the VPMN and is not publicly available. However, the CC/NDC usually follows the regular numbering plans and enables determining the location of the subscriber using ITU, NRA information, or private companies.

In some cases, the roaming relationship between the home and the visited network is based on a technical implementation that prevents the ARP from using publicly-available information for determining the location of its customer. In such circumstances, the DSP shall provide the relevant information for determining the location of a customer to the ARP.

This shall typically cover the cases where the GT CC/NDC does not reflect the actual location of the customer e.g.

* Alias GT of a EU network caching a non-EU actual location
* Alias GT of a non-EU network caching a EU location
* GT of a EU network used specifically for non-terrestrial service (i.e. air, satellite or maritime services)
* etc

In the context of PS-domain, the relevant information is usually the IP address or FQDN of the core network node serving the customer. Additionally, depending on the technology and the VPMN-implementation, the MCC/MNC of the VPMN may also be visible on the online interface, for example, GTP may convey optionally the MCC/MNC between the VPMN and HPMN in the RAI (Routing Area Identity).

The IP address (or its range) or FQDN used by the VPMN is defined in the roaming agreement between the HPMN and the VPMN and is not publicly available. However, the IP address or FQDN may usually be resolved for determining the owner and location of the subscriber using IANA, whois command, etc.

In some cases, the roaming relationship between the home and the visited network is based on a technical implementation that prevents the ARP from using publicly-available information for determining the location of its customer. In such circumstances, the DSP shall provide all relevant information for determining the location of a customer to the ARP.

This shall typically cover the cases where the IP address or the FQDN does not reflect the actual location of the customer e.g. an alias IP address.

Since the MCC/MNC identifies univocally the location of the subscriber, it is recommended the HPMN and VPMN supports the use of these fields on their roaming interface.

The DSP is free to put in place a location information translation mechanism providing transparent location information to the ARP within the interface instead of sharing GT/IP/FQDN information.

The location of the subscriber will be checked by the DSP and the ARP when processing the online event. Dedicated errors are defined for each interface to identify unambiguously and directly, if standard permits, the rejection due to location mismatch (ARP vs. DSP coverage).

It should be noted that out-of-ARP-coverage error includes the case where events are sent to the ARP while the end-user is not in a roaming condition.

* + - 1. Event type and destination

The minimum set of destination consists of destination for which the EU Regulation applies. The DSP and ARP may extend the scope of the ARP coverage. In such case, the DSP and the ARP shall determine the ARP destination set and type i.e. the set of destinations under the control of the ARP including the call type (voice, video-telephony, etc).

The event type is passed transparently to the ARP – e.g. Voice, video-telephony, SMS, Data, MMS. Hence there is not specific action to be taken by the parties.

The called destination for Voice, SMS and MMS services is based on the publicly available numbering plan. Hence the ARP is responsible of determining the destination of the call and hence, the associated call rate.

The call destination will be checked by the DSP and the ARP when processing the online event. Dedicated errors are defined for each interface to identify unambiguously and directly, if standard permits, the rejection due to a destination set mismatch (Call Destination not being part of the EU regulated destinations and of the DSP-ARP agreement).

* + - 1. Special use case: short codes

The call handling of short codes usually requires number translation for reaching the final call destination. The associate charging has to be configured for charging correctly these calls, too.

The use short code calls is not part of the regulation and therefore its implementation is subject to agreement between the DSP and the ARP.

* + - 1. Special use case: regulated free-of-charge numbers

The regulation requires the roaming provider to setup a free-of-charge number for obtaining more detailed personalised pricing information on the roaming charges that apply in the visited network to voice calls and SMS, and information on the transparency measures applicable by virtue of this Regulation, by means of a mobile voice call or by SMS.

The free-of-charge requirement applies only in visited networks located inside the Union.

ARP will deliver Free-of-charge number for obtaining more detailed information on the roaming charges. ARP free-of-charge number belongs to the EU numbering plan.

If the ARP coverage is limited to EU to EU, DSP has also to provide a DSP free-of-charge number for the where the customer can get the non-EU destinations tariff.

2 implementation options are possible to handle the calls towards the DSP free-of-charge number:

1. Either DSP is able to filter the DSP free-of-charge number. The ARP will not receive the corresponding triggers - ARP online charging is not impacted by the call.
2. DSP is not able to filter the DSP free-of-charge number. The DSP will inform the ARP about how to recognize the destination. The ARP will not charge at retail level the ARP customer for dialling the DSP free-of-charge number.
   * + 1. Special use case: Premium Rate and VAS services

The call handling of Premium Rate and VAS services requires specific management. These numbers are not part of the regulation and therefore the corresponding implementation is subject to the agreement in place between the DSP and the ARP.

## LBO implementation

* + 1. Subscriber identification

The subscriber shall be identified by its MSISDN wherever possible.

The subscriber MSISDN shall be used as the primary identifier of a subscription. Where a MSISDN is not associated with the subscription, IMSI shall be used. It shall be possible for MSISDN and IMSI to both be included in protocol messages, but it is not mandatory to include both under any circumstance.

* + 1. Service Usage

It is expected the LBO user will register the visited network providing the LBO service using a manual mode selection. The manual selection registration may happen after an initial automatic registration.

This ensures the subscriber will not select alternative networks because of loss of coverage, SIM parameters, etc.

The LBO design uses a new standardised APN value (standardised at European level) of "euinternet" (not case sensitive), which is known hereafter as the EUInternet APN. The EUInternet APN is specific to the LBO service and based on which the VPLMN will route Internet traffic directly to the VPLMN instead of routing via the HPLMN.

It is expected the LBO user will access the LBO service using the EU-wide dedicated APN.

# Interface definition for single imsi

## ARP – DSP Connectivity

The preferred transport layer for the Signalling is IP. With Signalling Transport over IP (SIGTRAN) the existing protocols on the higher layers can be used without changes (CAP, MAP). Also other protocols like SMPP, http/json and Diameter can be used via the same IP connection.

A separation of the protocols in VPNs or IPSec can be mutually agreed between the DSP and the ARP.



Figure 2 – Overview: IP transport for different protocols

.

## SIGTRAN

The TCAP and the SCCP provide a signaling connection between different signaling nodes and provide a transport mechanism for the upper protocol layers, e.g. Camel or MAP. The SCCP, Camel and MAP protocol layers do not require any modifications if SIGTRAN or TDM is used for the transport.

If SIGTRAN is not available, TDM based MTP and SCCP can also be used.   
If SIGTRAN is used, M2PA or M3UA shall be used.

* + - 1. SIGTRAN Option M3UA



Figure 3– M3UA stack overview

The Protocol layers in classical SS7 and in SIGTRAN M3UA.   
SCCP, CAMEL, MAP layers are unchanged.



Figure 4 – the communication between two SIGTRAN M3UA nodes in the OSI layer model

The Network Appearance Parameter (NA) in M3UA shall be agreed between the DSP and the ARP. The value of the NA can be different from the value of the NA in the private network of the DSP. This separation can improve the security.

* + - 1. SIGTRAN Option M2PA



Figure 5 – M2PA stack overview

The Protocol layers in classical SS7 and in SIGTRAN (M2PA variant).   
SCCP, CAMEL, MAP layers are unchanged.



Figure 6 – The Communication between two SIGTRAN / M2PA nodes in the OSI layer model

In this SIGTRAN option the M2PA layer emulates an MTP2 connection between the nodes.

* + - 1. MTP / M3UA Routing

For the following protocol layers an address planning between the DSP and the ARP is necessary:

* IP connection (IP addresses, Gateway, Netmask, etc.)
* SCTP Associations (number of associations, multihoming)
* M3UA: The Network Appearance Parameter (NA) . The NA shall be agreed between the DSP and the ARP. The value of the NA for the ARP connection can be different from the value of the NA in the private network of the DSP.
* Signaling Point Codes and MTP Routing Tables
* SCCP Addresses (E.164 Global Titles)

As an option, for increasing redundancy, multiple SCTP associations are recommended (Multihoming).

**Option 1:**



Figure 7 – SCTP Multihoming (IP) – option 1



MTP/M3UA Routing in A:

Destination B = Linkset A\_B, Prio 1

Figure 8 – SCTP Multihoming (SPC) – option 1

**Option 2 (more Reliability)**



Figure 9 – SCTP Multihoming (IP) – option 2



MTP/M3UA Routing in A:

Destination B = Linkset A\_B, Prio 1

Figure 10 – SCTP Multihoming (SPC) – option 2

**Option 3 (Paranoia Mode)**



Figure 11 – SCTP Multihoming (IP) – option 3



Figure 12 – SCTP Multihoming (SPC) – option 3

MTP/M3UA Routing in A:

Destination B = Linkset A\_B, Prio 1

Destination B = Linkset A\_D, Prio 2  
Destination D = Linkset A\_D, Prio 1

Destination D = Linkset A\_B, Prio 2

MTP/M3UA Routing in C:

Destination B = Linkset C\_B, Prio 1

Destination B = Linkset C\_D, Prio 2

Destination D = Linkset C\_D, Prio 1

Destination D = Linkset C\_B, Prio 2

The Signaling Point codes can be unique either in the country (national unique SPC) or can be unique worldwide (international unique SPC).

If the DSP and the ARP agree on the usage of private SPCs (not unique in different networks), the ARP shall use this private SPC only for the specific connection between the relevant ARP and the DSP. The private SPC cannot be used for other SS7 connections between different networks.

* + - 1. SCCP Routing

The nodes on the DSP side and on the ARP (Carrier) side shall act as SCCP Relay Gateways.

The SCCP Addresses (Calling Party and Called Party, E.164 Global Titles) are involved in an end-2-end Signaling Connection. They are used between the Serving PLMN and the DSP based on the existing Roaming connections. In the signaling relationship between the VPLMN and the DSP the E.164 GTs of the VPLMN and the DSP are used.

The ARP may have its own GT, or GT is provided from the DSP. However, the VPLMN does not have necessarily an SCCP Routing for this GT as the roaming relationship only exists between the HPMN and the VPMN. Hence this could result into problems in SCCP connections with multiple messages in each direction, e.g. prepaid service.

To ensure the end-2-end routing from VPLMN to the ARP, the ARP has to use a GT from the DSP range or the DSP shall use a proxy with SCCP address manipulation.

As described in the IF1 section, the SCCP Relay function or the Proxy function in place shall enable the exchange of message end-to-end between the ARP and the DSP.

The selection of the method (Route on PC, TT modification, Global Title modification, etc) depends on the DSP routing capabilities.

## Interface overview

To enable the sale of regulated roaming services the following interfaces are proposed to directly provide the basic regulated service.

* **IF1**: An online interface for voice retail billing (Camel or Diameter).
* **IF2**: An online interface for SMS retail billing (Camel or Diameter).
* **IF3**: An online interface for Data/MMS retail billing (Diameter).
* **IF4**: An interface for providing mobility information to the ARP, to inform the ARP that one of its customers has started to roam or has changed networks.
* **IF5**: real-time USSD interface to enable the ARP to provide pre-paid account queries (conditional).
* **IF9**: SMS delivery interface (optional).

The purpose of this document is to detail the specifications of each of these interfaces.

For sake of completeness, in order to manage the customer and perform proper billing and invoicing the following additional interfaces are also required. They will be defined by the Billing and Provisioning (B&P) workgroup.

* IF6: Invoicing interface, providing for example re-written TAP CDRs.
* IF7: Provisioning interface enabling the management of ARP subscriptions.
* IF8: Interface for high usage and fraud control (optional).

Domestic Service Provider

ARP awareness

Alternative Roaming Provider

Visited Network

Mobility  
Proxy

Voice  
Proxy

SMS  
Proxy

Fraud

Billing

CRM

HLR

Voice  
Mail

GMSC

SMSC

GGSN

MMSC

On line Charging System

(SCP)

Tariff notification

IF4

IF1

IF2

IF3

IF5

USSD

USSD  
Proxy

CRM

IF7

WS  
Billing

IF6

Fraud

IF8

Postpaid

Prepaid

MMS  
Proxy

Data  
Proxy

IF9

SMS  
Delivery

SMS  
Delivery

Figure 13 – Single IMSI interface definition

**Note**

ARP Awareness (terminology to be refined) logical function aims at enabling the DSP functions to determine whether customers have an ARP subscription and if yes with which ARP, whether a service used by an ARP customer has to be decoupled or not, etc.

## Generic rules for interface definition

Some functions have to be assigned to DSP or ARP, based on the interfaces defined above.

The major criteria for interface definition and function mapping are modularity, information hiding, coupling minimization and cohesion maximisation.

When defining the specifications details, the I&P group has considered:

* Interfaces (IFx) availability,
* Mapping of the functions associated to those interfaces (IFx),

following the scheme below.

ARP

DSP

**IFx**

Figure 14 – Generic rules for function mapping

## Preliminary Note

By exclusively using Diameter-based Billing interfaces between the ARP and DSP Online Charging Systems (OCS), voice could be rated and charged in Real Time at retail level by the ARP. CAMEL roaming agreement between DSP and VPMN could remain in place for Real Time Charging, but the possibility of interoperability issues between DSP and ARP CAMEL implementations could be avoided (CAMEL services have only been tested when opening CAMEL roaming relationship between VPMN and DSP implementations).

Another advantage of Diameter usage is that DSP IN service implementations are isolated from ARP connections. This would remove the need for repeated backward compatibility testing with each connected ARP following any change in service developments, version upgrades, protocols, etc. that the DSP deploys internally in its IN systems. The support of a Diameter interface is not avoidable (required for Anti bill shock measures, Real Time Data Charging), but support for a Camel interface is.

## SI-IF1 : Voice Control

## Description

This interface is designated to enable charging of ARP subscribers for voice calls. This interface shall be established between the DSP and the ARP. Figure 4 shows conceptual network architecture for SI-IF1. SI-IF1 interface between DSP and ARP shall be established over CAMEL protocol. Due to the fact that the Diameter protocol for CS voice call is currently not standardized, the use of Diameter for IF1 will be subject to future expansion and is out of the scope of this section. The use of Diameter will be described in a next version of the present document.

The transport layer implementation of IF#1 shall be as described in DSP-ARP connectivity section.

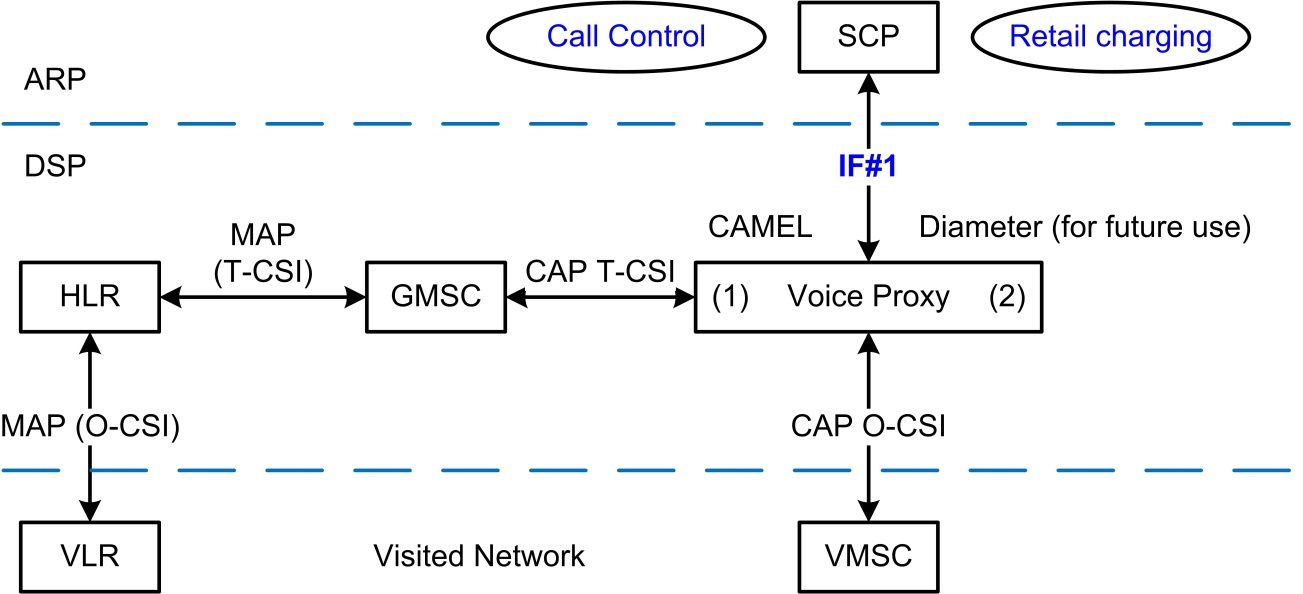


Figure 15 – Voice / CAMEL architecture and associated functions

## Detailed Procedures for MO Calls

* + - 1. Handling of MO-call at DSP

DSP may provide real-time charging interface and, optionally, real-time call control interface towards ARP. The providing of real-time charging interface and real-time call control interface is subject to the existence of CAMEL agreement between DSP and VPMN in countries that are covered by ARP. The providing of real-time charging interface and call control interface further requires that the DSP subscribers are provisioned with an O-CSI for usage in these VPMNs.

The CAMEL-IDP forwarding from DSP to ARP may be handled in the following methods (options):

1. Implementation Option 1 : Relaying the IDP message, and further CAMEL messages within the CAMEL dialogue, between DSP and ARP by means of SCCP routing;
2. Implementation Option 2 - Managing two CAMEL dialogs: One between the VPMN’s MSC/gsmSSF and the DSP’s SCP and another one between the DSP’s SCP and the ARP’s SCP.

DSP shall forward the CAP-MO-IDP (for Mobile Originated (MO) call or Mobile Forwarded (MF) call) received from VPMN to ARP’s SCP when all of the following conditions are fulfilled:

1. The Calling Party Number (for MO call) or Redirecting Party Id (for MF call) contained in the IDP operation is related to an ARP subscriber – or based on OCSI definition if specific per ARP;
2. The ARP subscriber is, as derived from the Location Information contained in the IDP operation, located in ARP coverage, as specified in the working assumption section.

It is observed that the present condition can’t be fulfilled when Implementation Option 1 is used, unless the OCSI associated with a customer varies per location. It results, when Implementation Option 1 is used, all MO calls from the ARP subscriber might be forwarded from DSP to ARP.

1. The Called Party BCD Number (for MO call) or Called Party Number (for MF call) contained in the IDP operation is related to a ARP destination as specified working assumption section.

It is observed that the present condition can’t be fulfilled when Option 1 is used. When Option 1 is used, all MO calls from the ARP subscriber may be forwarded from DSP to ARP.

The DSP is not obliged to convert the CAMEL phase, as used between VPMN and DSP, for the ARP. The CAMEL phase offered to the ARP may be the same one as is used between the VPMN and the DSP.

The CAMEL signalling between DSP and ARP shall comply with GSM TS 03.78 and GSM TS 09.78 (for CAMEL Phase 1 or CAMEL Phase 2) or 3GPP TS 23.078 and 3GPP TS 29.078 (for CAMEL Phase 3 or CAMEL Phase 4), depending on which CAMEL phase is used.

**Implementation Option 1: Relaying CAMEL to ARP by SCCP routing** – A CAMEL dialogue will be established between VPMN and ARP, whereby the CAMEL dialogue is routed through the voice proxy of the DSP. The voice proxy shall apply manipulation in the SCCP layer in order to facilitate that the messages replied from the ARP will be routed to the DSP network. For the remainder of the CAMEL dialogue, the CAMEL operations are sent between VPMN and ARP via the voice proxy.

The voice proxy for option 1 entails a functional entity in the DSP’s network that handles CAP signalling related to voice call establishment to/from ARP subscriber. The voice proxy determines whether the criteria are fulfilled for relaying the CAP signalling towards ARP. In the affirmative case, the voice proxy relays the CAP signalling, for this call to/from the ARP subscriber, between VPMN and DSP. This implies that the TCAP relationship is established between VPMN and ARP.

Examples of SCCP relaying methods are (i) replacing the SCCP Destination Address and SCCP Origination address and (ii) replacing the SCCP Destination Address and adapting the Translation Type (TT) of the SCCP Origination Address.

In this option the DSP only inspects upper layer (TCAP/CAP) and no modification or manipulation is done.

This has the following implications:

1. DSP will not have full control of the call session.
2. DSP will not be able to produce CDRs. This fact may complicate failure investigation, dispute resolution and wholesale management between DSP and ARP.

(e.g. ARP subscriber complains that a call failed. Without CDR in DSP, the investigation will be more difficult).

1. DSP will not be able to apply restrictions on CAMEL operations that are generated from ARP.

(e.g. ARP can connect the call to destinations that are not agreed by DSP or ARP SCP may arm the Answer DP or the Disconnect DP in interrupt mode when that is not agreed by DSP).

1. DSP may mandate the ARP to perform CAMEL integration to VPMNs.

The following figure depicts the basic MO-call signaling flow for option 1.

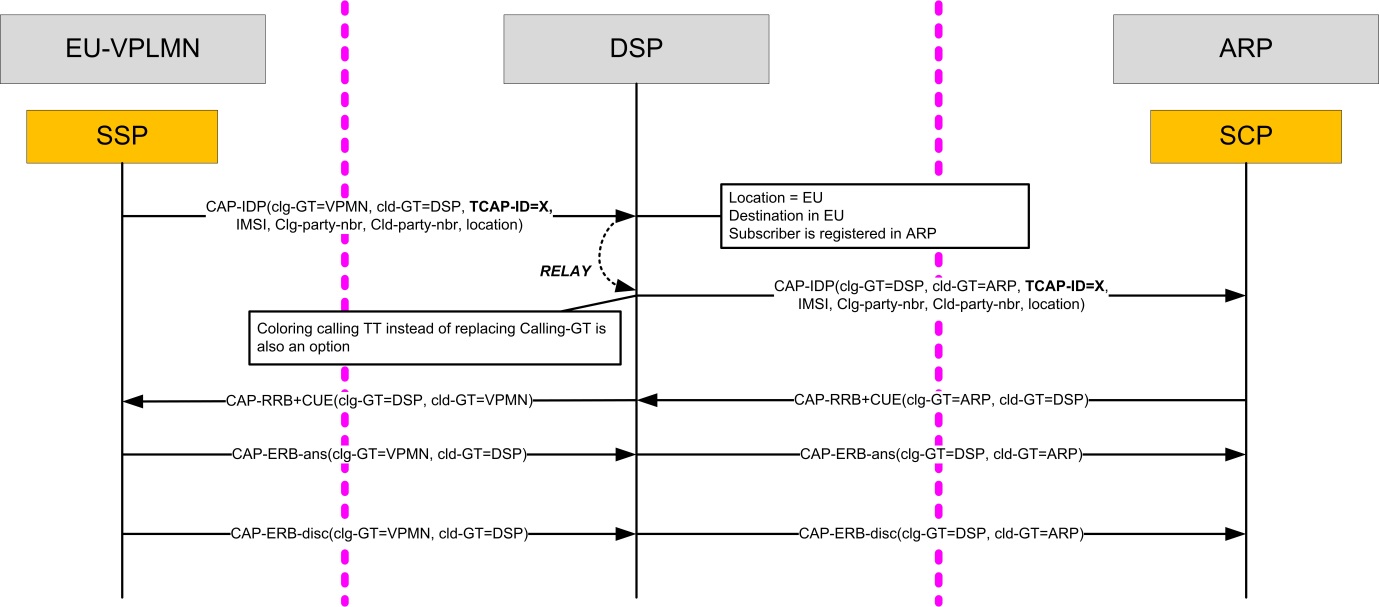


Figure 16 – Sequence diagram for SCCP level relay of CAMEL operations (option 1)

**Option 2: Managing two CAMEL dialogs**:

The voice proxy for option 2 entails a functional entity in the DSP’s network that comprises a gsmSCF and a gsmSSF. The gsmSCF in the voice proxy terminates the CAP dialogue that is initiated from the MSC/gsmSSF in the VPMN’s network or that is initiated from the GMSC/gsmSSF in the DSP’s network. The gsmSSF in the voice proxy initiates the CAP dialogue towards ARP. The voice proxy further contains service logic that handles the CAMEL dialogue towards the VPMN and the CAMEL dialogue towards the ARP and that maps information between these two dialogues.

This option has the following aspects:

1. DSP will have full control of the call session.
2. DSP will be able to produce CDRs, which facilitates investigation and dispute resolution in reasonable timeline. DSP will also be able to perform full wholesale management.
3. DSP will be able to apply restrictions on CAMEL operations that are generated from ARP.
4. DSP will perform separate CAMEL integration with VPMNs and CAMEL integration with ARPs. CAMEL integration to VPMNs, in so far as such integration had already been applied, will not have to be re-performed for each ARP.
5. DSP and ARP may agree on a unique CAMEL phase for the IF1 interface, independent of the CAMEL phase between VPMN and DSP.

The following figure depicts the basic MO-call signaling flow for option 2.

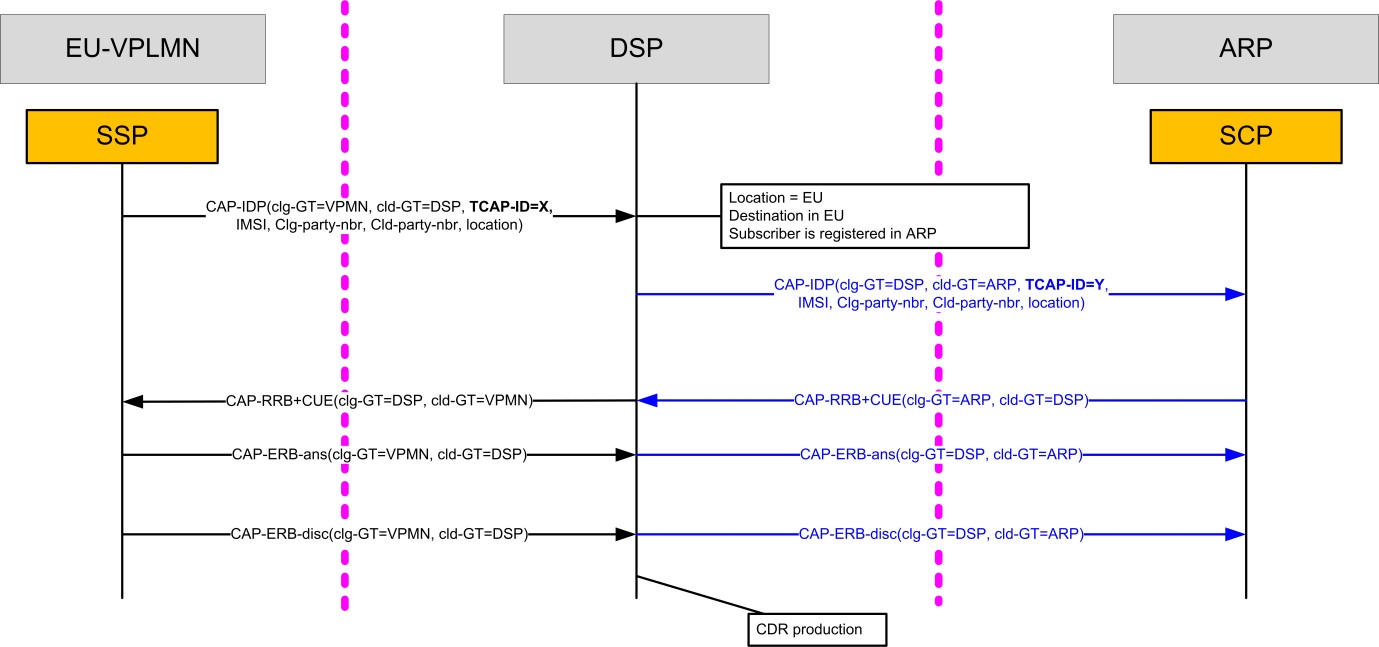


Figure 17 – Sequence diagram for MO call handling with separate CAMEL dialogues

The DSP shall provide, in the CAP IDP operation, all mandatory parameters to ARP. In addition, the DSP may perform the following manipulations on the CAP IDP operation:

1. Replace the SK value.
2. Adapt the Location Information. The CAMEL standard specificies the following mandatory sub-parameters for the Location Information:
   1. VLR number;
   2. Age of location information; and
   3. Cell ID or LAI.

Due to the fact that the tariff information is based on VPMN network, DSP shall provide the VLR number in the Location Information. The DSP may, however, hide the CellIdOrLAI and/or the Age-of-location parameters from the Location Information.

**Call diversion**

By selecting option 2, the DSP will have the capability to perform screening on DRA (Destination Routing Address) number present in CAP Connect operation replied from ARP. DSP may, resulting from analysing the DRA, reject the Connect operation.

**Call event arming**

By selecting option 2, the DSP will have the capability to perform screening on BCSM event arming mode (Notify and Continue or Interrupt), present in the CAP-RRB (Request-Report-BCSM) messages replied from the ARP. Arming BCSM events by ARP shall be done in conformance to agreement between DSP and ARP. The following options are identified:

* ARP may arm events in interrupt mode; this mode of event arming results in the establishment of a control relationship between DSP and ARP. A control relationship allows ARP to provide on-line charging and provides ARP with call control capability.
* ARP may arm events in Notify and Continue mode; this mode of event arming results in the establishment of a monitor relationship between DSP and ARP. A monitor mode enables ARP to monitor the call, but does not provide on-line charging and call control capability, apart form modifying the destination of the call or disallowing the call establishment.

**Announcement playing**

The playing of announcement is supported in CAMEL Phase 2 and higher. For option 2, the ability for playing announcements by ARP is subject to agreement between DSP and ARP. In addition, the ability for playing announcements by ARP is subject to the existence of CAMEL Phase 2, or higher, agreement between DSP and the VPMN where ARP subscriber roams. The ability for playing announcements by ARP is further subject to the support, by DSP, of this capability.

* + - 1. Handling of MO-call at ARP

Based on agreement between DSP and ARP, ARP may perform call diversion for certain call cases.

Based on agreement between DSP and ARP, ARP may arm BCSM DPs in “notify and continue mode” or in “interrupt” mode.

For CAMEL Phase 1, the ARP may apply charging based on Request Report BCSM (RRB) and Event Report BCSM (ERB). The use of Activity Test may also be possible for checking the transaction status.

For CAMEL phase 2 and higher, the ARP may use the following charging related operations:

* Apply charging (ACH) and Apply charging report (ACR);
* Call information request (CIRq) and Call information report (CIRp); and
* Furnish charging information (FCI).

The use of call control operations (including the use of the Connect operation and the arming of DPs in interrupt mode) must be agreed between DSP and ARP.

**Note** The arming of at least one DP in interrupt mode is required for the use of the Apply Charging operation.

## Detailed Procedures for MT Calls

* + - 1. Handling of MT-call at DSP

CAMEL control of MT calls may be done through interaction with the GMSC or through interaction with the VMSC. Interaction with GMSC for MT calls is done through T-CSI. Interaction with VMSC for MT calls is done through VT-CSI. When VT-CSI is used for MT call control, this is generally restricted to Home network. MT calls in home network do not qualify for control by ARP. Therefore, VT-CSI based control of MT call is considered to be out of scope of the present document.

When CAMEL is used for Mobile Terminating (MT) call in the DSP, DSP shall use the same CAMEL phase for the interface between the DSP SCP and the ARP as between the GMSC and the DSP SCP.

**Note** Conversion of CAMEL phase for this call case is not prohibited but is deemed to fall outside the scope of the present document.

There is no dependency between the CAMEL phase used for MO and MT scenario.

When the DSP uses non-CAMEL IN, such as INAP, for MT control, conversion to CAMEL phase 2 shall be applied by the DSP network.

**Note** Conversion to other CAMEL phase than CAMEL phase 2 is not prohibited but is deemed to fall outside the scope of the present document.

For charging of MT call, an IDP shall be sent from DSP to ARP SCP. DSP shall populate all parameters in the IDP operation, in accordance with the CAMEL standard.

DSP shall send IDP (MT call) to ARP’s SCP when all of the following conditions are fulfilled:

1. The recipient number (Called Party Number) contained in the IDP operation is related to an ARP subscriber;
2. The recipient subscriber (ARP subscriber) is, as derived from the Location Information contained in the IDP operation, located in ARP coverage, as specified in working assumptions section;

It is observed that the present condition can’t be fulfilled when Implementation Option 1 is used. When Option 1 is used, all MT calls to the ARP subscriber may be forwarded from DSP to ARP.

The following figure depicts the basic MT-call signaling flow for option 2.

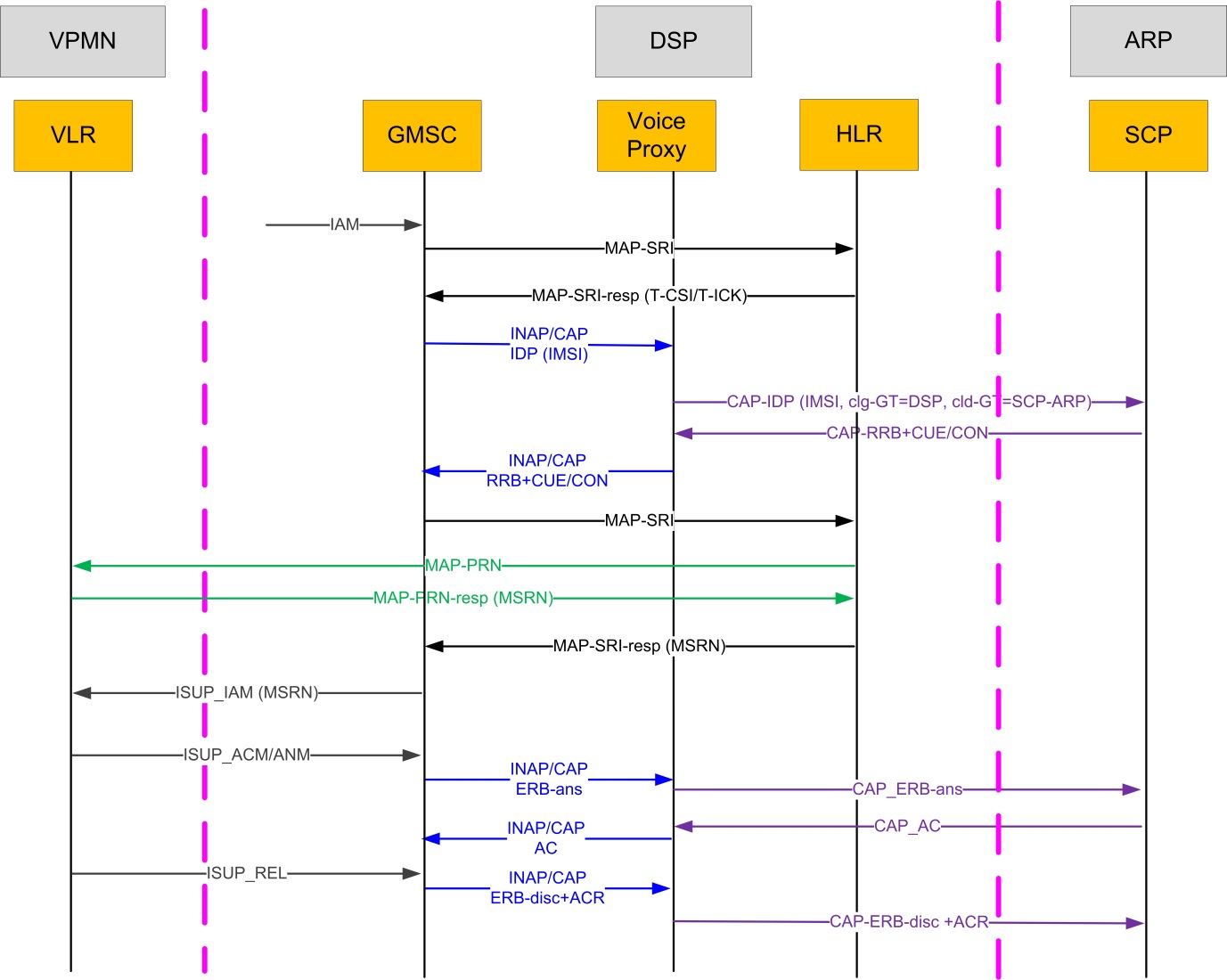


Figure 18 – Sequence diagram for MT call handling with separate CAMEL dialogues

A terminating call for a roaming ARP subscriber may lead to call forwarding in the VPMN. When CAMEL agreement between DSP and VPMN operator is present, the call forwarding in the VPMN may result in the invocation of a CAMEL service for the forwarded call. The DSP shall forward the IDP operation related to this forwarded call, to ARP. ARP may in this case apply its own ‘anti trombone solution’.

**Note** ‘Anti trombone solution’ is a term commonly used to refer to the method of converting call forwarding in the VPMN into call forwarding in the Home PLMN. Such method prevents additional roaming cost for the operator and/or the end-user.

The following figure shows the signaling associated with a particular implementation of Anti trombone solution.

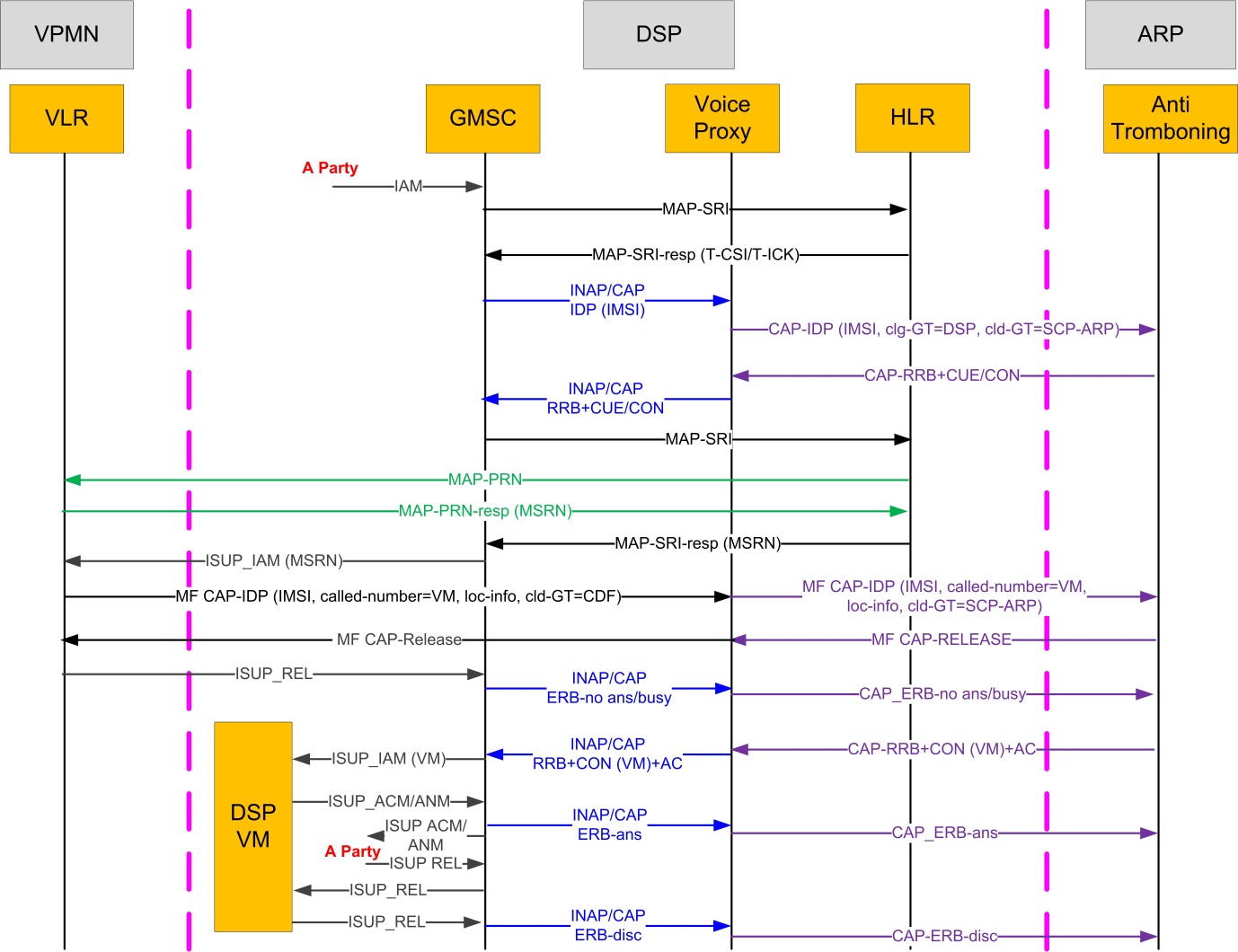


Figure 19 – Sequence diagram for Anti trombone solution

In hybrid scenario, comprising a mix of non-CAMEL based service invocation (in Home PLMN) and CAMEL based service invocation (in VPMN), anti-trombone solution may be implemented by DSP as defined in the High level specifications document.

* + - 1. Handling of MT-call at ARP

The CAMEL interface between DSP and ARP comprises both call control capability and charging control capability. The use of call control operations (e.g. CONNECT and the arming of DPs in interrupt mode) must be agreed between DSP and ARP. The use of CONTINUE or RELEASE is by default allowed.

When CAMEL agreement between VPMN operator and ARP is present, ARP may apply its own anti-trombone solution.

In hybrid scenario when non-CAMEL and CAMEL are present, ARP shall not be allowed to implement anti-trombone solution of its own as defined in the High level specifications document.

## Interface Primitives

The CAMEL operations that may be used for enabling the decoupling of roaming retail service for voice control are:

DSP to ARP

* Initial DP (IDP)
* Event Report BCSM (ERB)
* Apply Charging Report (ACR)
* Call Information Report (CIRp)

ARP to DSP

* Activity Test (AT)
* Apply Charging (ACH)
* Call Information Request (CIRq)
* Continue (CUE)
* Furnish Charging Information (FCI)
* Release Call (RC)
* Request Report BCSM (RRB)
* Reset Timer (RT)

The actual availability and support of these operations depends on the HPMN CAMEL roaming agreements (e.g. CAMEL phase) and DSP capability (e.g. capability of brokering the message, interworking limitations with actual protocol being used (INAP for MT Call), etc).

The support of other CAMEL operations (e.g. Connect (CON)) providing call control or operations for user interactions (e.g. Play Announcement) goes beyond the decoupling requirement and hence, shall be defined as part of the DSP-ARP agreement.

## Parameters, Definitions and Use

The parameters of the primitives are as specified in GSM TS 03.78 and GSM TS 09.78 (for CAMEL Phase 1 and CAMEL Phase 2) and 3GPP TS 23.078 and 3GPP TS 29.078 (for CAMEL Phase 3 and CAMEL Phase 4).

## Error handling

* + - 1. System related errors

The following errors can occur when forwarding (option 1) or sending (option 2) call control and/or charging control to ARP:

* The ARP’s SCP does not respond to IDP sent by DSP.
* The signalling connection between DSP and ARP is not operational.
* Proxy device deployed between ARP and DSP is not operational.

In all of the above scenarios, the DSP shall reject the call establishment by returning an IDP Error to MSC of the VPMN, for MO calls or MF calls, or to the GMSC of DSP, for MT calls or MF calls.

As a corollary of the above requirements, the DCH (Default-Call-Handling) in the O-CSI that is sent to the VLR in VPMN or to the GMSC of DSP, as well as the DCH in the T-CSI that is sent to the GMSC of DSP, shall be set to “RELEASE”.

* + - 1. Error handling in MO calls

When the calling subscriber does not belong to this ARP, ARP shall reject the CAMEL service invocation by returning an IDP Error with error code MissingCustomerRecord.

When the ARP subscriber is currently not within ARP coverage, ARP shall reject the CAMEL service invocation by returning an IDP Error with error code UnexpectedDataValue.

When ARP determines from the Called Party BCD Number in the CAP IDP operation that the destination of the call does not represent a destination within ARP destination set, then ARP shall reject the CAMEL service invocation by returning an IDP Error with error code ParameterOutOfRange.

**Note** The above cases constitute ‘error cases’, in which DSP should not have invoked the CAMEL service at ARP.

When the ARP subscriber doesn’t have sufficient credit for the call at hand, ARP shall the reject the call establishment through the use of ReleaseCall. The cause value used in this call case shall be agreed between ARP and DSP.

* + - 1. Error handling in MT calls

When the called subscriber does not belong to this ARP, ARP shall reject the CAMEL service invocation by returning an IDP Error with error code MissingCustomerRecord.

When the ARP subscriber is currently not within ARP coverage, ARP shall reject the CAMEL service invocation by returning an IDP Error with error code UnexpectedDataValue.

**Note** The above cases constitute ‘error cases’, in which DSP should not have invoked the CAMEL service at ARP.

When subscriber doesn’t have sufficient credit for the call at hand, ARP shall the reject the call establishment through the use of ReleaseCall. The cause value used in this call case shall be agreed between ARP and DSP.

## SI-IF2 : SMS Control

## Context

The observation of the current implementation of online charging methods for SMS roaming has shown a lack of a single common approach in the industry.

While it is fully available in the standards, the adoption of CAMEL phase 3 in the roaming context remains anecdotic. However, if a roaming agreement using CAMEL phase 3 (SMS control) exists between the visited network and the home PLMN, it is likely that the DSP will leverage its existence for decoupling the roaming service with the ARP.

The “home-routed” nature of the SMS has rather led operators to develop alternative techniques to avoid the operational burden of roaming tests. This is based on intercepting the MAP SMS-MO operations and subsequently allowing its process after interacting with the OCS.

There are typically multiple available approaches for interacting with the OCS and charge the customer:

* using a SS7 signalling (CAMEL phase 1,2 or 3, MAP, etc)
* using Diameter
* using near-realtime CDR for a “hot” billing approach

The recommended approach shall focus on using CAMEL phase 3 directly, a “MAP to CAMEL” interworking function or “MAP to Diameter” interworking function.

The *hot billing* methodis not recommended and shall only be used under mutual agreement. Indeed, in the context of ARP roaming, there might dispute due to conflicting decision (SMS-C accepts the SMS-MO leading to wholesale charges while the customer might be actually out of credit).

A private dispute resolution process should be put in place in case of such near-realtime scenario is applied.

Since the purpose of these guidelines is to define a **common** **online** interface for any DSP to any ARP, it is assumed the DSP will enhance its current implementation in order to comply with the proposed interface based on CAMEL for SMS control or Diameter.

It is expected that most of DSPs may have to implement additional conversion/interworking function in their network; hence, the applied recommendation is expected to follow the most “natural” or future-proof evolution from the existing DSP implementation.

## Description

SMS real-time charging shall be based on standard protocol for online charging of SMS i.e. CAMEL for SMS control (CAMEL phase3 onwards) or Diameter.

ARP

OCS

SMS Proxy

VMSC/SGSN

Diameter

DSP

Visited Network

CAMEL

For SMS control

For

**IF2a**

**IF2b**

**OR**

SCP

Figure 20 – SMS architecture and associated functions

The “home-routed” nature of the SMS has led operators to develop alternative techniques to avoid the operational burden of roaming tests. This is based on intercepting the MAP SMS-MO operations and to trigger the OCS before acknowledging the message.

This is depicted in the figure below.

In the context of decoupling roaming service, the MAP intercept function and SMS-C reside in the DSP network while the OCS resides at the ARP.

When there isn’t any CAMEL agreement for SMS control in place between the HPMN and the VPMN, the DSP shall ensure a real-time interface based on a MAP intercept function to be in place.

The call flow below illustrates the sought mechanism – however it is an implementation choice to define where to implement the MAP intercept and the relevant protocol to reach the SMS-proxy on the DSP side.



Figure 21 – Generic SMS interception mechanism for online charging

The MAP intercept function and the SMS-C function are shown as different entities for clarity reasons; they could be located with the same network element i.e. within the SMSC platform.

The SMS/MAP intercept will be responsible for verifying that the user has credit on the account by initiating a CAMEL dialogue or Diameter credit control session.

Additionally, it may run a format check verifying that the destination number is part of the ARP coverage, identifying the sending party is an ARP customer, etc.

Depending on the actual DSP implementation, the interface used for credit checks is recommended to contain different level of functionality to ensure correct retail as well as wholesale charging. This shall ensures that the decoupling method does not introduce any caveat: the SMSC may, for example, not process the SMS-MO although the ARP OCS allowed it.

* When the interface is based on Diameter and the credit check is done
  + Prior to MO process then additional functionality is recommended in the interface in order to ensure the retail process is in line with the actual SMS processing at the SMSC. This can be done by a credit reservation and arming processing events or an immediate charging with refund capability.
  + After MO process of the SMS is done then Immediate Event Charging (IEC) without refunding capability is enough to ensure correct charging.
* Similarly, for a Camel based interface,
  + In case credit check is done prior to the SMS process the mentioned procedure with credit reservation and arming event is recommended to be implemented.
  + if the credit check is done after the actual MO SMS processing, then there is no need to use the Request Report SMS and Event Report SMS procedure ; the direct process of the credit control based on the IDP is sufficient.

When a subscriber sends an SMS that exceeds the permissible length for SMS, then the UE may offer the subscriber to send the SMS as “concatenated SMS”.

The concatenated SMS is sent as two or more individual SM’s through the network.

In general, each SMS of a concatenated SMS will trigger its own online charging service.

## CAMEL for SMS Control

Sample call flows are mentioned below.

Their purpose is to illustrate the principles and only relevant parameters are shown.

The actual implementation remains operator-specific.

The sending of SMS from SGSN is similar and can be deducted easily.

The initial purpose of the IF2 interface is to deliver online charging control.

Because CAMEL provides both call and charging control facilities jointly, the use of call control operations (e.g. CONNECT-SMS and event report with interrupt mode) must be mutually agreed.

Beyond the ability of using the CONNECT-SMS operations, the set of modified destination subscriber number and the arming of specific event shall be mutually agreed by the DSP and ARP.

This would prevent from abusing the DSP with the call control facilities provided (e.g. rerouting number to fraudulent destinations).

The use of CONTINUE-SMS or RELEASE-SMS shall always be supported.

*Existing roaming agreement allowing SMS control over CAMEL*

Roaming agreement using CAP3 may exist, DSP shall detect that IDP-SMS shall be passed to the ARP instead of its own OCS, when relevant.

Similarly to the implementation options presented in the IF1, the DSP may provide the CAMEL messages:

* Relaying at SCCP level;
* Relaying at CAP Application level.

The reader should refer to IF1 section for getting an overview of the implications of choosing one or the other method.



Figure 22 – SMS control over CAMEL (existing roaming agreement)

CAP IDP-SMS does not contain any indication that the SMS is part of a concatenated SMS.

The DSP shall preferably use a Default Call Handling – RELEASE in the SMS-CSI.

It is recommended to use the SMS Event Report in this scenario.

*Non-Existing roaming agreement allowing SMS control over CAMEL*

When there isn’t any CAMEL agreement for SMS control in place between the HPMN and the VPMN, the DSP shall ensure a real-time interface based on a MAP intercept function is in place.

The call flow below illustrates the sought mechanism – however it is an operator decision to define where to implement the MAP intercept and the relevant protocol to reach the SMS-proxy on the DSP side.

However, the protocol between the SMS-Proxy and the ARP-OCS shall be CAP3 for SMS-control.



Figure 23 – SMS control over CAMEL (MAP intercept)

As indicated previously, the use of event reports depends on the actual implementation as stated above.

* + - 1. CAMEL Control Limitations

The use SMS Submission and Failure event report is optional, but recommended when the interaction with the OCS happens before the actual SMS processing.

This enables the alignment between the retail control and the wholesale activity: if the SMSC cannot process the MO-SMS request, the actual retail charging shall not happen as a failure report will be received at the ARP side.

In case the ARP does not support the use of these events, the DSP shall not be liable for any inconsistencies between the SMS retail mechanism and the SMS wholesale mechanism (e.g. SMSC processing).

In case the DSP does not support the use of these events, the DSP shall ensure a mutually agreed dispute resolution procedure is in place for solving the cases where the ARP customer is charged while the SMS is not processed by SMSC.

* + - 1. CAMEL Control Restrictions

The ARP shall not be allowed to modify the SMS-C being used by the subscriber as the roaming relationship (VPMN-HPMN) should remain under the full control of the DSP.

## DIAMETER

In case of using Diameter the DSP will perform unit determination and the ARP will be responsible for charging determination, referred to as Decentralized Unit Determination and Centralized Rating in 3GPP TS 32.299.

Two cases for control of user credit for online charging are possible when charging SMS:

• Immediate Event Charging (IEC) and

• Event Charging with Unit Reservation (ECUR).

In the case of *Immediate Event Charging* (IEC), the credit control process for events is controlled by the corresponding *CC-Requested-Type EVENT\_REQUEST* that is sent with *Credit-Control-Request (CCR)* for a given credit control event.

A refund using *Direct debiting operation* should be performed, when the service charged previously through Direct Debiting Operation is finally proved to be unsuccessfully delivered.



Figure 24 – SMS control over Diameter (MAP intercept and IEC mode)

In the case of *Event Charging with Unit Reservation (*ECUR) the *CC-Request-Type INITIAL /*

*TERMINATION\_REQUEST* are used for charging for a given credit control event, however, where a reservation is made prior to service delivery and committed on execution of a successful delivery.



Figure 25 – SMS control over Diameter (MAP intercept and ECUR mode)

The decision whether to apply IEC or ECUR is based on DSP capabilities.

## Detailed Procedures at DSP

In the absence of CAP3 roaming agreement the SMSC or other network element involved in the MO-SMS data path will have to initiate a credit / charging control session to the OCS of the ARP.

Hence a MAP to CAP or DIAMETER translation has to be performed.

The corresponding mapping table can be found in section 1.1.5.

Before initiating the credit control procedure, the DSP will check:

* The subscriber type: ARP or DSP
* The subscriber status: Realtime or offline charging
* The ARP subscriber is under the ARP coverage :
  + the recipient number is a ARP-served number (e.g. a regulated destination or any other destination mutually agreed)
  + the sender is located within the ARP footprint (e.g. in the Union or any location mutually agreed).

The DSP will await ARP answer and process:

* The positive / negative answer, as provided by the ARP
* The DSP will time-out the transaction in case of no answer from the ARP
  + Time Out is based on CAMEL timers i.e. 1 to 20sec.
  + The value of the timer is a DSP implementation should be based on an internal standard implementation policy.
* Error handling
  + See the detailed ARP procedures for possible returned errors.

## Detailed Procedures at ARP

Upon IDP trigger or CCR request, the ARP will validate the sender of the SMS is an ARP customer and eligible for service (w.r.t its current location and the recipient number).

The ARP will respond with the errors for the

|  |  |  |
| --- | --- | --- |
|  | CAMEL | DIAMETER |
| Subscriber does not belong to ARP | missingCustomerRecord | DIAMETER\_USER\_UNKNOWN 5030 |
| Subscriber is not within ARP served footprint | unexpectedDataValue | DIAMETER\_END\_USER\_SERVICE\_DENIED 4010 |
| Recipient number of the SMS is not within ARP destination set | parameterOutOfRange | DIAMETER\_END\_USER\_SERVICE\_DENIED 4010 |

In case the ARP subscriber is not a prepaid customer and the online charging interface was used by the HPMN, the ARP may respond with:

* CAMEL CONTINUE-SMS
* DIAMETER\_CREDIT\_CONTROL\_NOT\_APPLICABLE 4011
  + The OCF determines that the service can be granted to the end user but no further credit control needed for the service (e.g. service is free of charge or is treated for offline charging).

## Interface primitives

The CAMEL operations that may be used for enabling the decoupling of roaming retail service for SMS control are:

From DSP to ARP:

Initial DP SMS,

Event Report SMS,

From ARP to DSP:

Continue SMS,

Release SMS,

Request Report SMS Event,

Furnish Charging Information SMS,

Reset Timer SMS.

The actual availability and support of these operations depends on the HPMN CAMEL roaming agreements (e.g. CAMEL phase) and DSP capability (e.g. capability of brokering the message, interworking limitations with actual protocol being used, etc).

The support of other operations (e.g. connect SMS) providing SMS control or other function shall be defined as part of the DSP-ARP agreement.

The details of the primitives can be found in the relevant 3GPP standards for CAMEL – 22.078, 23.078 and 29.078.

DIAMETER primitives for Credit Control are:

Credit-Control-Request [CCR]

Credit-Control-Answer [CCA]

The details of the primitives can be found in the relevant 3GPP standards for DIAMETER – 32.299 (General) and 32.274 (SMS case).

## Parameters Definitions and Use

The 3GPP standards define the mandatory and optional parameters of the primitives.

For CAMEL, the MAP -> CAMEL ph3 mapping table can be found as follows.

The table is based on 3GPP 29.078, 23.040 and 29.002 and shows the relevant parameters to be matched between the MAP operation and the CAP operation.

|  |  |  |
| --- | --- | --- |
| SCCP parameters | CAMEL parameters | Comments |
| Cg-SCCP Address | MSC number | Per standard, only present if SMS reference number present |
| Cg-SCCP Address | Location Information/VLR number | Best effort – copy of MSC field into VLR |
| MAP parameters | CAMEL parameters | Comments |
| IMSI | IMSI |  |
| n.a. | Service Key | *Determined by mutual agreement between the DSP and ARP* |
| SM-RP-DA | SMS-C |  |
| SM-RP-OA | Calling Party Number | MSISDN of the ARP customer |
| TP-Destination-Address (TP-DA) | Destination Subscriber Number |  |
| n.a. | Event Type | *SMS\_Collected\_Info* |
| n.a. | Time Zone and Timestamp | *Timestamp and Time Zone at the DSP – at the time of intercepting the MAP message* |
| 1st octet of the SMS-SUBMIT TPDU | TP Short Message Submission  Specific Information |  |
| TP Protocol Identifier | TP Protocol Identifier |  |
| TP Data Coding Scheme | TP Data Coding Scheme |  |
| TP Validity Period | TP Validity Period |  |
| n.a. | SMS Reference Number | *Determined by the MAP intercept function* |

In case Diameter is the chosen interface, the following MAP -> Diameter translation shall be done.

Detailed information can be found in 3GPP TS 32.274: "Telecommunication management; Charging management; Short Message Service (SMS) charging".

The following table is based on 3GPP 32.299, 32.274, 23.040 and 29.002.

|  |  |  |
| --- | --- | --- |
| SCCP/MAP parameter | Diameter SMS-Information AVP | Comments |
| n.a. | SMS-Node | The SMS-Node AVP (AVP code 2016) is of type Enumerated and identifies the role which the SMS node performs in relation to the charging event. |
| Cg-SCCP Address | Originator-SCCP-Address | This is usually the address of the MSC or SGSN/Serving Node that was serving the UE when it submitted the SM. It contains the Global Title, where Global Title represents an E.164 number. |
| SM-RP-DA | SMSC-Address | The SMSC-Address AVP (AVP code 2017) is of type Address and carries the address of the SMSC, as contained in the  SM. |
| TP Data Coding Scheme | Data-Coding-Scheme |  |
| n.a. | SM-Message-Type | The SM-Message-Type AVP (AVP code 2007) indicates the type of the message which  caused the charging interaction. In the SMS-MO case, the value is “0” (SUBMISSION) |
| TP Protocol Identifier | SM-Protocol-ID |  |
| TP-User-Data-Header-Indicator | SM-User-Data-Header |  |
| TP-Destination-Address (TP-DA)  Or  A modified address (in case of optional service rendered by the DSP) | Recipient-Info / Recipient-Address | This field holds the address of the recipient of the SM. This will typically be an E.164 number or a shortcode. |
| TP-Destination-Address (TP-DA) | Recipient Received Address | This field holds the original, unmodified address of the recipient of the SM, as received by the SMS node, in case address manipulation (such as number plan corrections) have been applied in the SMS node. This will typically be an E.164 number or a shortcode |
| SM-RP-OA | Subscription-Id |  |

## Error Handling

The error scenarios can be split into 2 major scenario sets:

Service Implementation Related:

1. ARP decision to reject the SMS because the subscriber doesn’t have any credit on the account;
2. ARP decision to reject the SMS because the subscriber is not an ARP subscriber;
3. ARP decision to reject the SMS because the subscriber is not located within the ARP coverage.
4. ARP decision to reject the SMS because the recipient number is not part of the ARP destination set.

Breakdown / Failure Related:

1. Communication problem between DSP and ARP i.e. the ARP doesn’t respond to credit control requests but the application layer is up ;
2. Connection (peer or signaling point) is down, it’s not possible to perform a credit control;
3. DSP failure in delivering the SMS from the ‘intercept’ function to the SMSC ;
4. Normal error handling by the DSP according to 3GPP 29.002 ;

There are no mechanisms / procedures available to deliver the SMS and do the retail charging a posteriori. Hence, in all the above scenarios, the DSP shall reject the SMS-MO and return error to MSC/SGSN of the Visited MNO. The actual reject can be sent by the SMSC or the MAP-interception function.

## Limitations

This usual architecture, leveraging the “home-routed” principle of the SMS-MO, can be subject to Fraud cases, when the end-user or a 3rd party manipulates the destination SMSC address, making it different from the DSP SMSC address. This is inherent to the architecture and can be minimized:

* using CAMEL ph3 between Visited and Home networks,
* applying SMS call barring.

The ARP should benefit from the protection mechanisms put in place by the DSP or the VPMN in order to minimize these risks.

## Special Use Case: Short Code

In case the DSP uses short codes for controlling its own pricing transparency solution (i.e. the STOP/START mechanism), the DSP shall provide:

- the ARP with long number value of the short code for applying the appropriate retail charges or,

- filter the online triggers to the ARP for avoiding charging the customer for this message.

The use of short codes by ARP is out of scope of the regulation.

Therefore its implementation is subject to agreement between the DSP and the ARP.

The activation/deactivation of the transparency mechanism may happen when located in domestic network or roaming in the ARP or DSP coverage.

## Summary table

The following table summarizes the information shared between the ARP and DSP for the purpose of setting up the interface. The actual connectivity items are out of scope.

|  |  |  |
| --- | --- | --- |
| Information | Information Provider | Purpose |
| Protocol  CAP3/DIAMETER | DSP | Identify the interfacing model |
| Operational Model  Immediate Event Charging  Or  Reservation | DSP | Identify the interface implementation model |
| In case of CAMEL, the list of allowed operations (beyond the roaming decoupling requirements) | Mutually agreed | Identify the operations (call and event control) |
| In case of allowed CAMEL Connect operations, the list of agreed destination subscriber number | Mutually agreed | Identify the rerouting possibilties |
| Short Codes | ARP and DSP | Enable the continuation of the pricing information mechanisms of each roaming provider under ARP/DSP coverage. |

## SI-IF3 : Data Control

## Architecture, Description and Definitions

Data charging is based on Diameter signalling. The same interface is designed to provide retail charging and could also deliver Anti Bill Shock function.



Figure 26 – Data architecture and associated functions

MMS charging can be based on event or volumes: two different architectures are proposed.

1. MMS charging on Volume is based on the same principle and interface as data charging (SI-IF3a using Diameter signalling)
2. MMS charging on Event (per message) is based on an interface between the MMS proxy and the ARP OCS (SI-IF3b using Diameter signalling).



Figure 27 – MMS architecture and associated functions

Interfaces 3a and 3b between DSP and ARP for credit control, which includes bill shock function, shall be based on standard 3GPP interfaces.

The Diameter Credit Control Application (DCCA) is a Diameter based application that can be used to implement real-time credit control for a variety of end user services such as network access and messaging services.

The following standard specifications shall apply:

* RfC 3588: Diameter Base Protocol
* RfC 6733 is replacing RFC 3588. The DSP will decide which RfC that is implemented.
* RfC 4006: Diameter Credit-Control Application
* 3GPP TS 32.251: Telecommunication management; Charging management; Packet Switched (PS) domain charging
* 3GPP TS 32.270: Telecommunication management; Charging management; Multimedia Messaging Service (MMS) charging
* 3GPP TS 32.299 Telecommunication management; Charging management; Diameter charging applications (Gy)
* 3GPP TS 32.240: Telecommunication management; Charging management; Charging architecture and principles

Further description below shall give a subset of the standard necessary to implement the minimum set of functions enabling ARP with the charging management facilities for data services including MMS. Additional functionality may be implemented on commercial terms. The used version of a particular interface protocol specification is subject to mutual agreement between the DSP and ARP.

The quota management is unit based, units are measured in either volume or events. The DSP needs to categorize the traffic using different Rating Groups, e.g. normal charging, zero-priced charging (MMS event, ARP landing page). Each RG will create its own credit instance within a Gy session, the different credit instance are handled separately from each other.

The DSP traffic categorization can be done using RG as the granularity i.e. several service data flows with the same charging principle are belongs to the same RG and quota management is performed on the RG. The other option of categorization introduces more granularity where quota management is made on the combination of RG and the service data flow (service-identifier avp.

The DSP will state the level of granularity used to the ARP.

For data services session based charging with central unit determination and centralized rating shall apply. The units are measured in volume.

For MMS charging scenario, if event based MMS charging applies; immediate event charging with local unit determination and centralized rating shall apply.

## Definitions

Depending on existing DSP implementations, the ARP has to support two possible methods, according to 3GPP standard, to distinguish traffic for different purpose in DSP GGSN.

1. **Multi APN strategy:** If a DSP uses the multi APN strategy, the differentiation on different services is generally determined by the APN. The DSP may make the APN usage visible to the ARP. Charging of MMS can at the DSP based on dedicated APN or RG. Depending on the implementation, the use of specific RG for the Quota management of MMS traffic volume may be required in the Gy interface towards the ARP. Alternately, Quota management may not be used for a dedicated APN, if e.g. MMS is not charged by volume.
2. **Single APN strategy:** A DSP using a single APN strategy (no dedicated APN for different services) has to differentiate services by using rating groups: for example, in the case of MMS, the DSP shall provide a second rating group to the ARP allowing charging MMS based on events. In such case, the volume is accounted using a second rating group, which potentially could be zero-rated in retail charging. The DSP may have additional RG configured, depending on its implementation. They have to be supported by the ARP.

The Rating-Group AVP is of type Unsigned32 (AVP Code 432) and contains the identifier of a rating group. The specific rating group the request relates to, is uniquely identified by the combination of Service-Context-Id and Rating-Group AVPs. The definition of a rating group is DSP implementation-dependant and will be given by the DSP to the ARP.

To allow sufficient operation, giving a good balance between charged volume and number of Gy transactions, the DSP will define the size of

* 1. Default quota size per RG, used by the OCS when subscriber’s account has credit enough the quota
  2. Minimum quota size per RG, the minimum quota the OCS is allowed to provide when the subscriber’s account doesn’t cover the default quota,
  3. Quota threshold, when reporting shall be done.
  4. Validity time, the time from when the quota is granted until GGSN will update the OCS with the usage
  5. Quota Holding Time, the time a credit instance are allowed to be idle i.e. no packets are sent before the credit instance is terminated and GGSN will report the usage

As the standard roaming service will be offered, the charging control dialog will not include possibilities to the ARP of setting or changing triggers in the GGSN of the DSP.

## Detailed Procedures at DSP

The DSP will deliver all services to the customer, using GGSN and MMSC functionality.

The DSP will provide an online interface to the ARP OCS, acting as a client for direct charging control using an event based charging interface, if event based MMS charging applies.

The DSP will provide an online interface to the ARP OCS, acting as a client for session charging control using a session based charging interface.

The DSP sets parameters for data transmission to standard values, avoiding any discrimination in terms of QoS offered to roamers.

The DSP will deliver only service to customers after successful authorization by the ARP. The DSP will not allow transfer of payload packets to go through GGSN in case of quota hasn’t been granted by ARP.

The DSP will deliver service differentiation (Data / MMS) either by APN or by Rating Group method dependant on existing implemented methods.

Detailed Procedures at ARP

The ARP acts as OCS server for all data services.

The ARP has to grant volume quota for all chargeable services prior to usage i.e. responding to the CCR.

## Interface primitives

The charging control is based on Diameter Credit Control (DCC) using pairs of request and answer messages (CREDIT-CONTROL-REQUEST (CCR) – CREDIT-CONTROL-ANSWER (CCA)). The use cases are start, mid-session and termination control (it corresponds to the request type: Initial, Update and Terminate).

For immediate event charging also event type ‘event’ is also used.

Details on content for the messages can be found in the Parameters Definitions and Use sections.

For termination of data session, either the customer or the OCS of ARP terminates the session. The ARP can terminate the session using temporary or permanent error codes on command level. Error codes on the MSCC level is only valid for the credit instance and will not lead to a disconnect of the data session

Optionally the DSP may give ARP the possibility, depending on markets and commercial agreements, to redirect traffic to Top-up Server of ARP.

MMS event charging is controlled by DCC messages between MMS proxy and ARP OCS.

* + - 1. Start of Data session

The DSP will state whether the CCR (I) will be sent prior to establishing the PDP session or if it will be sent upon receiving the first payload packet.

Authentication and quota management can be combined within the CCR initial. If the DSP is splitting the OCS authorization and quota management then a two-steps handling takes place.

The implementation of the Diameter dialog depends on needs for getting minimum quota together with the PDP context establishment.

The three following scenarios are depicted hereafter and work without changes in ARP implementations.

The following figure illustrates the scenario when the CCR (I) is sent during establishing the PDP session and authentication and quota management is combined within the CCR (I). A default quota is requested during the authentication.



Figure 28 – Start of Data Session call flow: control at PDP context creation

1. End User initiates a PDP context request
2. The DSP prepare a data session e.g.
   1. authenticates the user request
   2. turn on Gy interfaces for this user and ARP
   3. assigned an IP address is to the user
   4. bitrate is set to standard, no dynamic bitrate is supported
3. DSP sends a quota request via Data Proxy using in the **CREDIT-CONTROL-REQUEST ( INITIAL\_REQUEST)** message to the ARP OCS.
4. ARP OCS receive a quota request via Data Proxy using in the **CREDIT-CONTROL-REQUEST ( INITIAL\_REQUEST )** message from DSP.
5. ARP checks customer account
6. The ARP OCS responds with the **Credit-Control-Answer (INITIAL\_REQUEST )** message to Data Proxy granting the requested quota.
7. The DSP receive the **Credit-Control-Answer (INITIAL\_REQUEST)** message via DATA Proxy granting the requested quota. The DSP will if applicable setup the PDP context and will allow service usage.

The following figure illustrates the scenario when the CCR (I) is sent after establishing the PDP session and authentication and quota management is combined within the CCR (I) and triggered by the start of the data transmission.



Figure 29 – Start of Data Session call flow: control at first packet received

1. End User initiates a PDP context request
2. The DSP prepares a data session e.g.
   1. authenticates the user request
   2. turns on Gy interfaces for this user and ARP
   3. assigns an IP address to the user
   4. bitrate is set to standard, no dynamic bitrate is supported
3. The DSP may decide to accept PDP context request at this stage and trigger charging control at first usage or can authenticate already the PDP context request against the OCS of ARP.
4. DSP sends a quota request via Data Proxy using in the **CREDIT-CONTROL-REQUEST (INITIAL\_REQUEST)** message to the ARP OCS.
5. ARP OCS receives a quota request via Data Proxy using in the **CREDIT-CONTROL-REQUEST (INITIAL\_REQUEST)** message from DSP.
6. ARP checks customer account.
7. The ARP OCS responds with the **Credit-Control-Answer (INITIAL\_REQUEST)** message to Data Proxy granting the requested quota.
8. The DSP receives the **Credit-Control-Answer (INITIAL\_REQUEST)** message via DATA Proxy granting the requested quota. The DSP will, if applicable, setup the PDP context and will allow service usage.

The following figure illustrates the scenario when the CCR (I) for authentication is sent during establishing the PDP session and the quota management is done afterwards by CCR (U) triggered by the start of the data transmission.



Figure 30 – Start of Data Session call flow: split authentication and quota management

1. End User initiates a PDP context request
2. The DSP prepares a data session e.g.
   1. authenticates the user request;
   2. turns on Gy interfaces for this user and ARP;
   3. assigns an IP address to the user;
   4. bitrate is set to standard, no dynamic bitrate is supported.
3. The DSP may decide to accept PDP context request at this stage and trigger charging control at first usage or can authenticate already the PDP context request against the OCS of ARP.
4. DSP sends a **CREDIT-CONTROL-REQUEST (INITIAL\_REQUEST)** message to the ARP OCS.
5. ARP OCS receives **CREDIT-CONTROL-REQUEST (INITIAL\_REQUEST)** message from DSP.
6. ARP checks customer account.
7. The ARP OCS responds with the **Credit-Control-Answer (INITIAL\_REQUEST)** message to the Data Proxy to allow further proceeding.
8. The DSP receive the **Credit-Control-Answer (INITIAL\_REQUEST)** message via DATA Proxy.
9. The DSP will if applicable setup the PDP context and will allow service usage.
10. If the DSP detects the beginning of Data transmission, DSP sends the **CREDIT-CONTROL-REQUEST (UPDATE\_REQUEST, “Rating Group”)** message via Data Proxy to ARP OCS.
11. ARP OCS receives **CREDIT-CONTROL-REQUEST (UPDATE\_REQUEST )** messages and grant volume
12. ARP OCS responds with **CREDIT-Control-Answer ( UPDATE\_REQUEST )** message to grant quota.
13. The DSP receives the **CREDIT-Control-Answer ( UPDATE\_REQUEST, “Rating Group” )** message via Data Proxy granting quota.
    * + 1. Data Mid-session update and control



Figure 31 – Middle of Data Session call flow

**Note** The procedure is used for CCR update (e.g. Quota or time period expires) procedures.

In case of quota or time period expires no Update PDP Context Update Procedure between the SGSN and GGSN applies.

1. DSP operates data session on given quota, quota threshold and optional set guard time period.
2. If either quota or the optional time period expires, DSP sends the **CREDIT-CONTROL-REQUEST (UPDATE\_REQUEST, “Rating Group”)** message via Data Proxy with used volume to ARP OCS.
3. ARP OCS receives **CREDIT-CONTROL-REQUEST (UPDATE\_REQUEST)** messages as report of used volume and request to grant additional volume.
4. ARP OCS responds with **CREDIT-Control-Answer ( UPDATE\_REQUEST)** message to grant additional quota.
5. The DSP receives the **CREDIT-Control-Answer ( UPDATE\_REQUEST, “Rating Group” )** message via Data Proxy granting additional quota.
   * + 1. Data session termination by user



Figure 32 – Termination of Data Session call flow (user-termination)

1. The user terminates a PDP context.
2. The DSP sends a **CREDIT-CONTROL-REQUEST (TERMINATION\_REQUEST)** via Data Proxy to ARP OCS to report session termination including final volume used.
3. ARP OCS receives **CREDIT-CONTROL-REQUEST (TERMINATION\_REQUEST)** message on PDP context termination.
4. ARP OCS sends **CREDIT-CONTROL-ANSWER (TERMINATION REQUEST)** message to DSP.
5. ARP updates customer account.
6. DSP receives the **CREDIT-CONTROL-ANSWER (TERMINATION REQUEST)** message via DATA Proxy
   * + 1. Credit session terminated by ARP OCS with FINAL-UNIT-ACTION=TERMINATE



Figure 33 – Termination of Data Session call flow (ARP-termination)- case 1

1. The DSP may receive as answer, either on INITIAL-REQUEST or UPDATE, the **Credit-Control-Answer (Update\_Request (Final-Unit-Indication (Final-Unit-Indication (Final-Unit-Action= Terminate))** message.
2. DSP sends **Credit-Control-Request (Update\_Request, Used\_Units)** to ARP OCS.
3. ARP OCS responds with **Credit-Control-Answer (Update\_Request)** message

**Note** Other possibilities to terminate the session including deleting the PDP Context on Diameter Command level are not excluded.

* + - 1. Data session terminated by ARP OCS with CC-Session Failover (result code 4012, DIAMETER\_CREDIT\_LIMIT\_REACHED)



Figure 34 – Termination of Data Session call flow (ARP-termination) - case 2

1. The DSP may receive as answer, either on INITIAL-REQUEST or UPDATE, the **Credit-Control-Answer (Update\_Request (CC-Session Failover DIAMETER-CREDIT-LIMIT-REACHED (Result Code 4012))** message.
2. The DSP terminates the data session by sending Delete PDP Context Request towards the customer,
   * + 1. Credit control MMS

The event based credit control dialog will be between MMS Proxy and OCS of ARP. Data quota handling for the plain data transmission part of a MMS within the GGSN depends on DSP implementations.

If destination rules should apply for MMS, quota management of plain data transmission has to be excluded: the ARP cannot be charged for MMS data volume while the message is not under his own control due to a destination rule.

Multiple destination MMS will, DSP implementation dependant, either create a single CC session for each recipient or request for multi-event Quota CC session.

The handling of Multiple Destination MMS where the destinations are shared between ARP and DSP depends on the technical DSP capabilities and DSP/ARP agreement. It is not discussed further in this document.

DSP standard retransmission policy for MMS will apply. No additional delivery reporting will be setup to ARP.

* + - 1. MMS MO using IEC (Immediate Event Charging) without quota management for data volume at GGSN

In the following case, the charging of the plain data transmission of the MMS is excluded, i.e. there is no quota management applied. This is depicted in the figure hereafter.



Figure 35 – MMS MO using IEC without quota management for data volume

* + - 1. MMS MO using IEC (Immediate Event Charging) with separate quota management for data volume at GGSN

In this case the charging of the plain data transmission of the MMS is done by using a separate Diameter dialog between the OCS Data Proxy and the ARP OCS before the MMS is sent. This case is only applicable when there is no destination rules applied for MMS.



Figure 36 – MMS MO using IEC with quota management for data volume

**Note 1**: In case the requested APN is generic (MMS or Data is not differentiated on APN basis), the GGSN gets quota for the global volume, including potential MMS Traffic - even if the customer will never send a MMS.

**Note 2:** In case a dedicated APN is used for MMS, the GGSN gets quota for MMS. If the GGSN des not support quota management for MMS, it is expected no CCR will be sent by the GGSN.

**Note 3:** Conditionally, in the case where no quota was assigned before, the GGSN detects the MMS Relay access and initiate a CREDIT-CONTROL-REQUEST towards the ARP, the GGSN gets only quota for MMS.

1. End user requests to send a Multimedia Message (MMS).
2. The DSP send **Credit-Control-Request** **(EVENT\_REQUEST with Requested-Action DIRECT\_DEBITING)** via MMS Proxy to ARP OCS
3. ARP OCS receive **Credit- Control-Request** **(EVENT\_REQUEST with Requested-Action DIRECT\_DEBITING)** via MMS Proxy to ARP OCS
4. ARP checks the end user’s account balance, rates the service, and debits the service from the end user’s account
5. ARP OCS sends **Credit-Control-Answer (Event Request)** via MMS Proxy.
6. DSP receive **Credit-Control-Answer (Event Request)** via MMS Proxy.
   * + 1. MMS MT using IEC (Immediate Event Charging)

If a destination rules applies in MMS MO case then the quota management of plain data transmission has to be excluded. It is not possible to have different quota rules for MMS MO and MMS MT.



Figure 37 – MMS MT using IEC

**Note 4:** In case the requested APN is generic (MMS or Data is not differentiated on APN basis), the GGSN gets quota for the global volume, including potential MMS Traffic.

**Note 5:** In case a dedicated APN is used for MMS, the GGSN gets quota for MMS. If the GGSN des not support quota management for MMS, it is expected no CCR will be sent by the GGSN.

**Note 6:** Conditionally, in case of no quota assigned before; the behaviour is expected to be inline with Note 3. The charging control remains initiated by the UE in order to receive the announced MMS (SMS-push).

* + - 1. MMS MT using ECUR (Event Charging with Unit Reservation)

If a destination rules applies in MMS MO case then the quota management of plain data transmission has to be excluded.



Figure 38 – MMS MT using ECUR

**Note 7:** In case the requested APN is generic (MMS or Data is not differentiated on APN basis), the GGSN gets quota for the global volume, including potential MMS Traffic.

**Note 8:** In case a dedicated APN is used for MMS, the GGSN gets quota for MMS. If the GGSN des not support quota management for MMS, it is expected no CCR will be sent by the GGSN.

**Note 9:** Conditionally, in case of no quota assigned before; the behaviour is expected to be inline with Note 3. The charging control remains initiated by the UE in order to receive the announced MMS (SMS-push).

* + - 1. Generation and Handling of Call Data Records

The interfaces 3a and 3b will deliver all necessary information to the ARP to allow detailed retail billing for data and event based MMS services. A volume based MMS billing will be included in the normal Data volume. As regulation defines that prices for MMS volume is treated like for data traffic. Even if all necessary information is already provided the DSP may have a mutual agreement with an ARP to provide additional CDR’s on an offline interface (may be together with wholesale information).

* + - 1. Handling of non ARP traffic

MMS to and from a non EU regulated country/network are handled locally within the DSP. In this case no quota management (neither for Data nor for the MMS event as such) applies between DSP and ARP.

## Parameters Definitions and Use

* + - 1. CCR/CCA fields

The AVP’s in the CCR / CCA are specified in 3GPP TS 32.299. In addition to this the Packet Switched (PS) Domain charging is specified in 3GPP TS 32.251 and 3GG TS 32.270 describes the charging management for the Multimedia Messaging Service (MMS).

## Error Handling

The principle error handling has to follow the rules described in the Diameter Base Protocol (IETF RFC 4006 and RFC 6733) and the related 3GPP specifications.

Especially the following procedures and actions are defined:

3GPP TS 32.299: Telecommunication management; Charging management; Diameter charging applications (Gy)

3GPP TS 32.251: Telecommunication management; Charging management; Packet Switched (PS) domain charging (Annex B: Tx expiration; Failure Handling procedure and session failover mechanism description)

Generally the error scenarios can be split into 2 major scenario sets:

Service Implementation Related:

1. ARP decision to reject the Data traffic or the MMS because the subscriber doesn’t have any credit on the account. (DIAMETER\_CREDIT\_LIMIT\_REACHED 4012)
2. ARP decision to reject the Data traffic or the MMS because the subscriber is not an ARP subscriber. ( DIAMETER\_AUTHORIZATION\_REJECTED 5003)
3. ARP decision to reject the Data traffic or the MMS because the subscriber is not located within the ARP coverage. ( DIAMETER\_AUTHORIZATION\_REJECTED 5003)
4. ARP decision to reject Data traffic or the MMS because the subscriber not subscribed to a detectable service, currently only “any Data” or MMS. (DIAMETER UNABLE TO COMPLY 5012)
5. ARP decision to reject Data traffic or the MMS because wrong AVP’s, Service parameters (like APN) or messages received. (DIAMETER UNABLE TO COMPLY 5012)
6. DSP decision to reject service if the assigned Quota by the ARP is outside agreed limits. (Undersized/ Oversized quota) .

Breakdown / Failure Related:

For all the following cases the DSP will not provide service to customers anymore.

1. Communication problem between DSP and ARP i.e. the ARP doesn’t respond to credit controls but the application layer is up ;
2. Connection (peer or signalling point) is down, it’s not possible for the DSP to do a credit control ;
3. Normal error handling by the DSP according to IETF and 3GPP Specifications as mentioned above.

## Summary table

The following table summarizes the information shared between the ARP and DSP for the purpose of setting up the interface. The actual connectivity items are out of scope.

|  |  |  |
| --- | --- | --- |
| Information | Information Provider | Purpose |
| Protocol  DIAMETER | DSP | Identify the interfacing model  Information elements out of 3GPP standard are used. |
| DCCA | DSP | Application according 3GPP |
| Rating Groups | DSP | The DSP defines the structure and values ranges the ARP has to commit |
| Operational mode at DSP  single / multi APN Operation  Quota management | DSP | The DSP has to deliver the implemented interface coding structure for ARP to follow the implementation |
| Operational mode at DSP for MMS | DSP | Information if event based charging is available or not |
| Quota (minimum, default, etc.) | DSP | ARP to follow |

## SI-IF4 : Mobility Control

## Description

Through this interface the DSP will inform the ARP on the subscriber’s roaming status while travelling within the EU.

The roaming status information must be provided in near-real-time based on the mobility observation between the VLR/SGSN and the HLR.

ARP

Subscriber location

Mobility Proxy

VLR/SGSN

DSP

Visited Network

**IF4**

Figure 39 – Mobility management architecture and associated functions

This interface is based on OMA RESTful Network API for Terminal Status (Candidate Version 1.0 – 08 Oct 2013), which can be found in RESTful Network API for Terminal Status V1.0 Enabler Release Package: <http://technical.openmobilealliance.org/Technical/release_program/TerminalStatusREST_v1_0.aspx>

In case of discrepancy, the OMA specifications take precedence.

## Detailed Procedures at DSP

The DSP will act as a notification server for this interface provided to the ARP.

The DSP will send notifications one every successful update location on networks inside ARP coverage.

The DSP will not retry sending notifications which previously failed to send, or for which it has not received a response.

## Detailed Procedures at ARP

The ARP will act as the notification client for this interface provided by the DSP.

The ARP must respond upon reception of the notification from the DSP.

The ARP will not receive notifications when subscribers attach to networks outside ARP coverage.

The ARP will not receive notifications when subscribers attach to DSP network or other home country’s network in case of national roaming.

**Note** Only the actual registration events in a network are passed to the ARP. It results a possible limitation on distinguishing when subscriber comes back to last ARP coverage network from outside ARP coverage. Example: a customer coming back and forth EU and non EU location may be seen as doing registration procedures in a network.

## Interface primitives

The Subscriber’s Roaming Status may be provided via a RESTful web API. Usually RESTful web API utilizes HTTP commands POST, GET, PUT, and DELETE in order to perform an operation on a resource at the server. This resource is addressed by a URI; and what is returned by the server is a representation of that resource depending on its current state.

The HTTP method POST is used to provide the Subscriber’s Roaming Status.

|  |  |
| --- | --- |
| Resource URI | http://{arp\_host}/terminalstatus/{version}/notifications/RoamingChangeNotification |
| HTTP Method | POST |
| Operation | Provide notification about the roaming status of the subscribers. |

Where:

{arp\_host} is replaced by the fully qualified domain name (FQDN) of the ARP server being accessed.

{version} optionally indicates the version of the interface being accessed, the current version is ‘v1’.

This figure below shows a scenario to send notifications about subscriber roaming status change:



Figure 40 - Roaming status change notification

Outline of flow:

An ARP notification client subscription process:

1. An application creates a new subscription to roaming status change notification by using POST.
2. The DSP responds with the resulting resource URL containing the subscriptionId.

**Note**

The subscription step is defined as a mandatory stage in the OMA specifications as it enables both parties to exchange data.

This procedure is usually applied at runtime (online subscription) or implicitly applied in the first transaction for accessing a resource.

However, in the current context, the industry believes the number of subscription will be low (say dozens).

So it is “expected” the DSP may configure the ARP subscription manually rather than having a runtime process in place.

Therefore, the subscription procedure may be replaced by a static configuration at the DSP side, in case it is not supported by the DSP.

1. A subscriber registers into a VPLMN and VLR/SGSN starts the Location Update procedure.
2. The DSP ends the procedure by sending current subscriber information to the requesting VLR.
3. The DSP detects the subscriber roaming status changes of an ARP subscriber.
4. The DSP server notifies the ARP using HTTP POST about the roaming status changes.
5. The ARP will respond to the HTTP request acknowledging the roaming status received.

This sequence [1-5] will continue executing as far as the subscriber register into any VPLMN while roaming within EU.

## Parameters Definitions and Use

The content type for the interface is ‘**application/json**’.

The subsections of this section define the data structures used in this interface. Some of the structures can be instantiated as so-called root elements.

For structures that contain elements which describe a user identifier, the statements in OMA RESTful Network API for Terminal Status (Candidate Version 1.0 – 08 Oct 2013) section 6 regarding 'tel', 'sip' and 'acr' URI schemes apply.

If a network element identifier (e.g. Visitor Location Register, Serving GPRS Support Node, etc.) of type anyURI is in the form of a Global Title (GT), it MUST be defined as a global number according to [RFC3966] (e.g. tel:+32476000011). The use of characters other than digits and the leading “+” sign SHOULD be avoided in order to ensure uniqueness of the resource URL. This applies regardless of whether the identifier appears in a URL variable or in a parameter in the body of an HTTP message.

If a network element identifier (e.g. Mobility Management Entity, etc.) of type anyURI is in the form of an Fully Qualified Domain Names (FQDN), it MUST be defined according to [3GPP TS 23.003], and it MUST include the protocol prefix 'tel:' followed by the FQDN (e.g. tel:mmegi32799.mme.epc.mnc001.mcc206.3gppnetwork.org).

If a subscriber identifier (e.g. subscriberId, etc.) of type string is in the form of an International Mobile Subscriber Identity (IMSI), it MUST be defined according to [ITU-T E.212].

If a terminal identifier (e.g. deviceId, etc.) of type string is in the form of an International Mobile Equipment Identity (IMEI), it MUST be defined according to [3GPP TS 23.003] and it SHOULD consist of 14 digits (e.g. 49015420323751), including the 8-digit Type Allocation Code (TAC) and the 6-digit Serial Number (SNR).

* + - 1. Type: RoamingChangeNotification

A type containing terminal roaming status for change notification:

|  |  |  |  |
| --- | --- | --- | --- |
| Element | Type | Optional | Description |
| callbackData | xsd:string | Yes | CallbackData if passed by the application during the associated startNotification operation.  See [REST\_NetAPI\_Common]. |
| roaming. | TerminalRoamingStatus  [1..unbounded] | No | Collection of the terminal roaming status |
| isFinalNotification | xsd:boolean | Yes | Will be set to true if it is a final notification about roaming status change. |
| link | common:Link  [0..unbounded] | Yes | Link to other resources that are in relationship with the resource. |

A root element named roamingChangeNotification of type RoamingChangeNotification is allowed in request and/or response bodies.

* + - 1. Type: TerminalRoamingStatus

A type containing current terminal roaming status:

|  |  |  |  |
| --- | --- | --- | --- |
| Element | Type | Optional | Description |
| address | xsd:anyURI | No | Address of the terminal device (e.g. 'sip' URI, 'tel' URI, 'acr' URI) to which the roaming status information applies. |
| subcriberId | xsd:string | Yes | The International Mobile Subscriber Identity (IMSI) to which the roaming status information applies. Must be included when the address of the terminal device is unknown i.e. ‘tel:+000000000000’. |
| deviceId | xsd:string | Yes | The unique International Mobile Equipment Identity (IMEI) of this terminal device. |
| retrievalStatus | common:RetrievalStatus | No | Status of retrieval for this terminal device address. |
| retrievalTime | xsd:dateTime | Yes | Indicates the time when the status was retrieved |
| currentRoaming | RoamingStatus | Yes | Roaming status of terminal. Must be included when retrievalStatus=Retrieved. |
| servingMccMnc | MobileCountryNetworkCode | Choice | Mobile Country Code / Mobile Network Code couple for the serving network.  Must be included when currentRoaming=DomesticRoaming  or  currentRoaming=InternationalRoaming. |
| servingNode | MobileServingNetworkNode | Choice | Address of the mobile network node serving the terminal device. |
| errorInformation | common:ServiceError | Yes | Must be included when retrievalStatus=Error. This is the reason for the error |

**Note:** XSD modelling uses a “choice” to select either “servingMccMnc” or “servingNode” or none of them, but not both.

* + - 1. Type: MobileServingNetworkNode

A type containing the type and the address of the network node serving the terminal device

|  |  |  |  |
| --- | --- | --- | --- |
| Element | Type | Optional | Description |
| type | ServingNetworkNodeType | No | Type of the network node serving the terminal device. |
| node | xsd:string | No | Address of the network node serving the terminal device (e.g. 'sip' URI, 'tel' URI, FQDN). |

* + - 1. Enumeration: RoamingStatus

An enumeration, defining the roaming status of a terminal:

|  |  |
| --- | --- |
| Element | Description |
| InternationalRoaming | Terminal is roaming internationally, i.e., in a country different from that in which it is registered for service with its home MNO/MVNO |
| DomesticRoaming | Terminal is roaming domestically, i.e., in the same country in which it is registered for service with its home MNO/MVNO. |
| NotRoaming | Terminal is not roaming, i.e., is connected to its home MNO/MVNO. |

* + - 1. Enumeration: ServingNetworkNodeType

An enumeration, defining the serving network node types:

|  |  |
| --- | --- |
| Element | Description |
| VLR | Terminal is attached to a Visitor Location Register. |
| SGSN | Terminal is attached to a Serving GPRS Service Node. |
| MME | Terminal is attached to a Mobility Management Entity. |

* + - 1. Enumeration: RetrievalStatus

|  |  |
| --- | --- |
| Enumeration | Description |
| Retrieved | Data retrieved. Current data is provided |
| NotRetrieved | Data not retrieved, current data is not provided (does not indicate an error, no attempt may have been made). Note that this field is useful in case a list of addresses are requested, some items could be marked as "NotRetrieved" in case retrieval could not be attempted for some reason, e.g. to avoid time outs |
| Error | Error retrieving data |

Roaming status change notification for single network-connected subscriber

This shows an example roaming status notification for two mobile devices:

* ***Notification by MSISDN:***

|  |  |
| --- | --- |
| POST /notifications/RoamingStatusNotification HTTP/1.1  Content-Type: application/json  Accept: application/xml  Content-Length: nnnn  Host: application.arp.com  Date: Thu, 01 Jul 2014 13:51:59 GMT  {"roamingChangeNotification ": {  "roaming": [  {  "address": "tel:+19585550100",  "subscriberId": "299011234567890",  "deviceId": "12315420323751"  "retrievalStatus": "Retrieved",  "retrievalTime": "2014-10-26T21:32:52",  "currentRoaming": "InternationalRoaming",  "servingNode": {  "type": "VLR",  "node": tel:+19585550199"  }  }  ]  }} | The JSON response contains a ***roamingChangeNotification*** object.  As the notification was for more than one mobile device the notification contain a ***roaming*** array.  ***retrievalStatus*** value is one of “Retrieved” or “Error” |

* ***Notification by IMSI:***

|  |  |
| --- | --- |
| POST /notifications/RoamingStatusNotification HTTP/1.1  Content-Type: application/json  Accept: application/xml  Content-Length: nnnn  Host: application.arp.com  Date: Thu, 01 Jul 2014 13:51:59 GMT  {"roamingChangeNotification ": {  "roaming": [  {  "address": "tel:+000000000000",  "subscriberId": "299011234567890",  "deviceId": "12315420323751"  "retrievalStatus": "Retrieved",  "retrievalTime": "2014-10-26T21:32:52",  "currentRoaming": "InternationalRoaming",  "servingNode": {  "type": "VLR",  "node": "tel:+19585550166"  }  }  ]  }} | The JSON response contains a ***roamingChangeNotification*** object.  As the notification was for more than one mobile device the notification contain a ***roaming*** array.  ***retrievalStatus*** value is one of “Retrieved” or “Error” |

* ***Response:***

|  |  |
| --- | --- |
| HTTP/1.1 204 No Content  Date: Thu, 01 Jul 2014 13:51:59 GMT | Indicates request processed successfully but no data is returned |

## Error Handling

Response Codes

HTTP response codes are used to indicate:

204 – No Content; the server has fulfilled the request but does not need to return an entity-body

400 – Bad request; check the error message and correct the request syntax.

401 – Authentication failure, check your provider’s authentication requirements.

403 – Forbidden; please provide authentication credentials.

404 – Not found: mistake in the host or path of the service URI.

405 – Method not supported: in the interface, only POST is supported.

503 – Server busy and service unavailable. Please retry the request.

More details on these at <http://www.ietf.org/rfc/rfc2616.txt>

* + - 1. Exceptions

SVC0004: No valid address

|  |  |
| --- | --- |
| HTTP/1.1 400 Bad Request  Content-Type: application/json  Content-Length: 1234  Date: Thu, 01 Jul 2014 13:51:59 GMT  {"requestError": {  "serviceException": {  "messageId": "SVC0004",  "text": "No valid addresses provided in message part %1",  "variables": "%1 - request URI"  }  }} | **400** indicates an error  A ***serviceException*** describes the reason why the service cannot accept the request; for example if the request URI was incorrect.  A ***policyException*** object means that the request syntax is valid, however an operator policy has been broken: in this example because the operator cannot support the batch size requested.  ***serviceException*** and ***policyException*** share the same body: an identifier pair for the exception (***messageId***), a text pair to describe it consistently (***text***), and a variables pair to indicate any specific cause of the error (***variables***). The ***variables*** relate to the %1 placeholder(s) in the ***text***. |

* + - 1. SVC2000: Service Error

The following exception will be received in case the subscriber is not registered in the ARP systems, and such will not be served by the ARP:

|  |  |
| --- | --- |
| HTTP/1.1 400 Bad Request  Content-Type: application/json  Content-Length: 1234  Date: Thu, 01 Jul 2014 13:51:59 GMT  {"requestError": {  "serviceException": {  "messageId": "SVC2000",  "text": "The following service error occurred: %1. Error code is %2.",  "variables": [  "%1 – Not a subscriber",  "%2 – ARP001",  ]  }  }} | **400** indicates an error  A ***serviceException*** describes the reason why the service cannot accept the request; for example if the subscriber was incorrect (not an APR subscriber). |

The following exception will be received in case the subscriber is not roaming under the ARP coverage, and such will not be served by the ARP:

|  |  |
| --- | --- |
| HTTP/1.1 400 Bad Request  Content-Type: application/json  Content-Length: 1234  Date: Thu, 01 Jul 2014 13:51:59 GMT  {"requestError": {  "serviceException": {  "messageId": "SVC2000",  "text": "The following service error occurred: %1. Error code is %2.",  "variables": [  "%1 – Not under coverage",  "%2 – ARP002",  ]  }  }} | **400** indicates an error  A ***serviceException*** describes the reason why the service cannot accept the request; for example if the location was incorrect (not under APR coverage). |

## SI-IF5 : USSD Control

## Description

The major goal of this interface is to relay USSD signalling between subscriber and ARP services USSD (Unstructured Supplementary Services Data) allows bi-directional and half-duplex connections between a handset and a USSD application server, exchanging plain text messages with each other.

Each USSD message can contain up to 182 user characters and is completely transparent for the handset and the mobile network.

There are two types of USSD, corresponding with its two phases of development in standard:

* USSD phase 1: the USSD service platform sends a response and the session is closed. So, only one request and its response are exchanged per session in USSD Phase 1.
* USSD phase 2: a session in USSD Phase 2 may be composed of many USSD messages (request and response messages). USSD Phase 2 can provide interactive services with a user-friendly ergonomic interface.

The USSD service code has to follow a given format: A [A] [A]1X(Y)[\*<STRING>]#

Where:

* A = \* or #
* X = 0 – 9 where X = 0 – 4 for services of the HPLMN & X = 5 – 9 for services of the VPLMN
* Y = 0 – 9
* [ ] indicates an optional element.

In a roaming decoupling situation, only HPLMN range could be used:

100…149 for International use i.e. used in the VPMN: the Visited PMN sends the USSD back to the Home PMN.

USSD services rely mainly on a USSD Center (USSD-C) which routes USSD messages from handsets to USSD application servers and vice-versa. A synthetic architecture is defined below:

VMSC

HLR

USSD-C

Applications

handset

MAP

MAP

Figure 41 – Architecture of USSD Services

Sessions are opened by using service codes (like a short number combining \* and #). After dialling on the handset a USSD service code (#121# for instance), a USSD request is sent to the USSD-C which identifies, thanks to the service code, the adequate application server which will process the request and send the response: a text message displaying a menu for instance. The user may continue the session by choosing an item of the menu or may decide to close it.

To support ARP related USSD services, minimizing the impact to existing infrastructure the following principal solution shall be implemented:

* USSD proxy with ARP awareness functionality,
* Allocation of USSD service code for ARP services,
* Routing of all ARP service code requests from HLR to USSD proxy and back.
* Routing of all ARP related USSD signalling from USSD proxy to ARP and back.

VMSC

HLR

USSD  
proxy

ARP  
SCP

handset

MAP

MAP

IF5

Figure 42 – IF5 USSD interface

The DSP shall allocate at least one USSD service code for ARP services in the 100-149 range, which does not overlap with existing DSP USSD service codes, but can be shared between different ARP.

IF5 USSD proxy / ARP interface shall be based on the SS7/MAP protocol.

There are 3 types of usage scenarios:

* Mobile initiated USSD – when the network relays information from mobile user to application entity in order to allow USSD operation.
* Network initiated USSD request - when the invoking application entity requires information from the mobile user, in connection with USSD handling;
* Network initiated USSD notification - when the invoking application entity requires a notification to be sent to the mobile user, in connection with USSD handling;

When interface 5 (IF5) is made available by the DSP then the mobile originated USSD is supported, the network initiated requests are depending on HLR capability.

## Detailed Procedures at DSP

* + - 1. General

Support of USSD signalling depends on the agreement between DSP and VPMN. DSP shall offer the relay of USSD signalling on all the networks where it is used by DSP’s own subscribers.

* + - 1. Mobile-initiated USSD

DSP shall forward USSD requests initiated by subscriber and received from DSP network or VPMN to ARP’s SCP when the three conditions below are met:

1. The number of USSD initiator corresponds to an ARP subscriber;
2. The USSD code belongs to ARP services;
3. The service requested is according to the agreement between DSP and ARP at the current location of subscriber – the location is not limited to the EU, but particular services may be limited to EU.

DSP shall ensure that subscriber identification (MSISDN) as well as the address of the VLR is included in the signalling to ARP.

MSISDN-less subscriptions are out of scope and for further study.

No protocol conversion will be done between different MAP operations, the USSD proxy will transparently pass the message relayed from the HLR.

* + - 1. Network-initiated USSD

DSP shall relay USSD notifications initiated by ARP SCP to VPMN in the following conditions:

1. The destination number of USSD corresponds to an ARP subscriber;
2. The service requested is according to the agreement between DSP and ARP at the current location of subscriber;

## Detailed Procedures at ARP

* + - 1. General

ARP is responsible for the provisioning of USSD based services and usage of USSD signalling transferred between subscriber and ARP shall be in accordance to the standards.

The capacity of the MAP is limited. Heavy traffic between the SCP and the HLR will delay other MAP transactions, for example, location updates. ARP shall ensure the reasonable usage of USSD signalling and shall take into account capacity considerations.

* + - 1. Mobile-initiated USSD

ARP shall reply to all USSD requests initiated by subscriber and received via DSP:

1. The reply shall be performed related to the same Origination Transaction ID
2. The reply shall be forwarded to the Calling Party Address in the SCCP level of the USSD request.
   * + 1. Network-initiated USSD

ARP may initiate USSD requests or notifications in the following conditions:

1. The destination number of USSD corresponds to an ARP subscriber;
2. The service used is according to the agreement between DSP and ARP at the current location of subscriber;

## Interface primitives

The interface is the standard MAP protocol according to 3GPP TS 29.002.

USSD signalling shall comply with the following standards:

* 3GPP TS 23.090, Unstructured Supplementary Service Data (USSD)-Stage 2 version 4.1.0,
* 3GPP TS 24.090, Unstructured Supplementary Service Data (USSD)-Stage 3.

The MMI for USSD shall be according to TS 22.030 and TS 22.090. The alphabet indicator and the data coding scheme shall be according TS 23.038.

***Common MAP-OPEN service primitives***

MAP-OPEN confirmed service is used for establishing MAP dialogues between two MAP service entities.

***The following parameters are relevant for USSD:***

Destination address:

A valid SCCP address identifying the destination peer entity.

Destination reference:

This parameter is a reference that refines the identification of the called process. It shall be either IMSI or MSISDN.

Originating reference:

This parameter is a reference that refines the identification of the calling process. It shall be the ISDN-Address-String on MAP-PROCESS-UNSTRUCTURED-SS-REQUEST, but can be omitted on other application contexts.

Application context name:

This parameter identifies the type of application context being established. If the dialogue is accepted the received application context name shall be echoed.

The following MAP services (application contexts) are relevant for USSD:

* MAP-PROCESS-UNSTRUCTURED-SS-REQUEST (processUnstructuredSS-Request);
* MAP-UNSTRUCTURED-SS-REQUEST (unstructuredSS-Request);
* MAP-UNSTRUCTURED-SS-NOTIFY (unstructuredSS-Notify).

***USSD MAP service primitives***

The MAP\_PROCESS\_UNSTRUCTURED\_SS\_REQUEST confirmed service is used for Mobile initiated USSD with the following relevant primitives:

* Invoke id
* USSD Data Coding Scheme
* USSD String
* MSISDN - included as an operator option, e.g. to allow addressing the subscriber’s data in the gsmSCF with the MSISDN

The MAP\_UNSTRUCTURED\_SS\_REQUEST confirmed service is used for Network initiated USSD request with the following relevant primitives:

* Invoke id
* USSD Data Coding Scheme
* USSD String

The MAP\_UNSTRUCTURED\_SS\_NOTIFY confirmed service used for Network initiated USSD notification with the following relevant primitives:

* Invoke id
* USSD Data Coding Scheme
* USSD String

## Parameters Definitions and Use

The following parameters shall be used for provisioning of USSD services for subscribers:

* Destination reference - subscriber number used for subscriber identification:
  + MSISDN number
  + IMSI number, especially if MSISDN is not available.
* Originating Reference - Location information (VMSC) – used for Mobile-initiated USSD requests to distinguish location for services where location information is relevant.
* USSD string – used for identification of ARP service.

MTP routing parameters shall be exchanged between ARP and DSP:

* Signalling Point Codes

Specific SCCP routing parameters, which shall be exchanged and harmonised between ARP and DSP:

* The SSN used in this interface will be based on the existing DSP implementation and will be provided by the DSP to the ARP

## Error Handling

The following failure related errors can occur during USSD usage between VPMN, DSP and ARP:

* The ARP’s SCP does not respond to USSD message sent by DSP.
* The signalling connection between DSP and ARP is not operational.
* Proxy device deployed between ARP and DSP is not operational.

In all of the above scenarios, the DSP shall reject the USSD by returning an MAP Error to MSC of the VPMN.

All such error cases shall be handled in according to the MAP specification TS 29.002. For definition of errors see 3GPP TS 24.080, for example, usually TC-U-ABORT message is sent back to the VPMN.

USSD service related errors are handled in the following way.

**Mobile-originated USSD:**

* When the subscriber does not belong to this ARP, error cause "Invalid Destination Reference" is returned by ARP to the HLR in the MAP-Refuse-PDU.
* When the service requested by the subscriber is not according to the agreement between DSP and ARP at the current location of subscriber, error cause "Invalid Destination Reference" is returned by ARP to the HLR in the MAP-Refuse-PDU. Additionally DSP may reject such a request, sending similar error to VPMN.

**Network initiated USSD notification or USSD request:**

* When the subscriber does not belong to this ARP, error cause "Invalid Destination Reference" is returned by ARP to the HLR in the MAP-Refuse-PDU.
* When the subscriber use the USSD service which does not belong to ARP coverage, error cause "Invalid Destination Reference" is returned by ARP to the HLR in the MAP-Refuse-PDU, Additionally DSP may reject such a request, sending simlar error to VPMN.
* If the VLR Address is not known in the HLR for the subsriber of ARP, the error cause "Absent Subscriber" is returned to the USSD application.
* If the VPMN does not support MAP version 2, the transaction is released.

## SI-IF9 : SMS Wholesale Interface (MO+MT)

The following interface implementation shall be considered as an example. The IF9 is an optional interface which requires mutual agreements between a DSP and an ARP.

## Description

The interface IF9 is an optional interface between the ARP and DSP. It can provide an ARP the possibility to instruct the DSP to generate a short message (SMS) for an ARP subscriber. The content of such a SMS might be for example tariff data, bill shock prevention, emergency or hotline numbers. Additional the ARP can receive SMS for own services.

ARP

ESME

SMSC

VLR/SGSN

DSP

Visited Network

**IF9**

HLR

MAP

Proxy

Figure 43 – MO/MT SMS architecture and associated functions

## Detailed Procedures at ARP

The ARP is connected to the DSP via an IP interface. This IP connection shall protect against misuse (fraud, address spoofing). It is requested to establish a secure connection between both entities (e.g. VPN connection or IPSec tunnel).

The interface IF 9 shall be usually based on the protocol SMPP. The DSP can also propose other methods available and commonly acknowledged as part of the state of the art in the DSP country. Although valid, these techniques are not discussed in this document.

The ARP shall act as a SMPP Client (External Short Message Entity - ESME) and the SMSC of the DSP as a SMPP server (SMSC).

The ARP has the responsibility to setup the connection to the SMSC with a “bind\_transmitter” request. This request considers authentication data. Detail information about this data is described in the SMPP standard and must be mutually agreed between the ARP and DSP.

The bind connection can be established for a single SMS transmission or can be active all the time (mutable agreed between the ARP and DSP).

## Detailed Procedures at DSP

Dependent on the authentication data the SMSC, the DSP acknowledges the bind request of the ARP.

The Receiver of a SMS confirms with a (SMPP) ACK the received SMS from the Sender.

An optional SMS proxy could check an external database. The primary parameter for this check is the MSISDN of the receiving party. The SMSC-proxy can check if the receiving subscriber belongs to the sending ARP.

Further verification can be performed if the subscriber is served by the VPLMN (outbound roaming).

MT SMS:

The SMSC uses the MAP procedures to terminate the SMS in the VLR (VPLMN) after a HLR inquiry. If the SMS cannot be delivered (e.g. absent subscriber), the SMSC keeps the SMS in a database.

According the configured retry schema the SMSC tries to deliver the SMS to the recipient.

The SMSC shall store CDRs for each successful MT\_SMS for the Wholesale-Billing between the ARP and the DSP.

MO SMS:

The Visiting MSC uses the MAP procedures to send the SMS to the SMSC.

The SMSC shall store CDRs for each MO\_SMS for the Wholesale-Billing between the ARP and the DSP.

## Interface primitives

The exchange of SMS between the ARP and the DSP is defined in the Short Message Peer to Peer Protocol Specification (SMPP).

The connection between the ARP and the DSP is made after a binding process. Each SMS shall be acknowledged.

The figure below illustrates the bind, unbind and the SMS delivery more in detail.

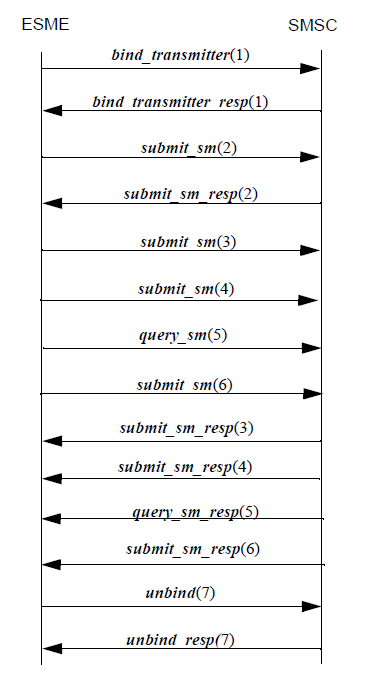


Figure 44 – Typical SMPP request/response sequence for an SMS from ARP to DSP

Source: SMPP protocol specification V 3.4, SMPP Developers Forum

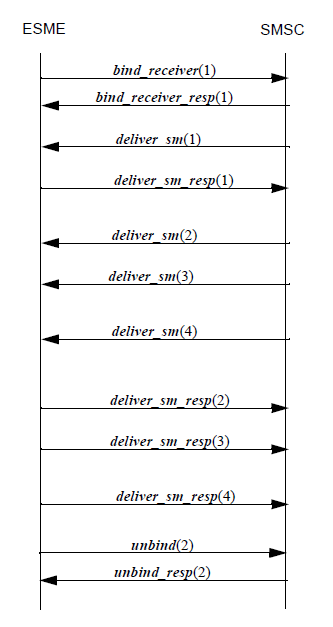


Figure 45 – Typical SMPP request/response sequence for an SMS from DSP to ARP

Source: SMPP protocol specification V 3.4 , SMPP Developers Forum

## Parameters Definitions and Use

The address of the sender and the receiver shall be formatted according to the E.164 standard. The used Type of number (TON) and Numbering Plan Indicator (NPI) shall be agreed between the ARP and the DSP.

The coding schema for special characters in the SMPP payload (e.g. umlauts like ä,ö,ü,ß) shall be agreed between the ARP and the DSP.

The SMSC shall store CDRs for each SMS for the Wholesale-Billing between the ARP and the DSP.

The maximum length of the SMPP messages shall be agreed between the ARP and the DSP. For a single SMS the SMPP standard supports up to 254 octets but on SMSC (MAP/MTP) only 160 octets per SMS are supported.

## Error Handling

If the SMSC of the DSP cannot properly store the received SMS of the ARP in the own database, the SMSC shall send an error on the SMPP interface according to the SMPP specification.

The SMSC does not send a delivery receipt to the ESME after an unsuccessful delivery of a SMS.

# Interface definition for LBO

## Assumptions

No new interfaces are needed between LBO and HPMN to launch LBO offer, except a conditional notification interface.

## Interface overview

The following interfaces will be included in the LBO architecture:

* IF1: existing MAP mobility interface, which will be impacted for customer profile and traffic steering.
* IF2: an NEW on-line notification interface provided by the LBO provider to inform Home operators of the start/end of an LBO subscription (conditional).
* IF3: existing TAP file interface. No TAP files are to be sent from LBO providers for LBO APN usage.

HPMN

LBO provider

Visited Network

SGSN

WS  
Billing

Notification

IF1(\*)

Notification

IF2

WS  
Billing

IF3(\*)

Traffic  
Steering

HLR

(\*) IF1 & IF3 are EXISTING interfaces, while IF2 is really a NEW interface.

Figure 46 – LBO interface definition

The purpose of this document is to detail the specifications of each of the IF1 and IF2 interfaces.

For sake of completeness, in order to manage the customer and perform proper billing and invoicing the IF3 interface is also required. It will be defined by the Billing and Provisioning (B&P) workgroup.

## LBO-IF1 : Mobility / Profile Control

## Description

IF1 interface (MAP) is an existing interface which will be impacted for

• Customer profile management: a standard EU Internet APN for regulated LBO service has to be configured by default from the DSP, at least for the LBO networks and preferably (recommended) for all the European countries. The sending of this APN to the rest of the world is an implementation choice of the DSP.

The new standardised APN value (standardised at European level) is "euinternet" (not case sensitive), which is known hereafter as the EUInternet APN. The EUInternet APN is specific to the LBO service and based on which the VPLMN will route Internet traffic directly to the VPLMN instead of routing via the HPLMN.

It is expected the LBO user will access the LBO service using the EU-wide dedicated APN

• Traffic steering (using SS7) has to be defined clearly to be compliant with the regulation “Obligation of DSPs not to bar or steer away outbound roaming customers having manually selected a LBO/VPMN network”, according to the following conditions:

* In order to assure customer experience, manual mode network selection shall be used by LBO customers to choose the LBO network.
* DSP SoR mechanism shall not interfere with manual selection

It is noted that some devices automatically switch back to “automatic network selection” without user interaction and some handsets do not allow access to change the APN, which may impair the user experience of the LBO customer

The version of MAP protocol in use within IF-1 interface is MAPv3.

The Network Identifier part of the APN used for EU Regulated services is: “euinternet”.

The full EU APN name is built accordingly by network elements as follows:

euinternet.mncxxx.mccxxx.gprs, where mncxxx.mccxxx.gprs is the Operator Identifier part of the APN belonging to the LBO.

Mobility procedures at LTE/EPC Network elements are out of scope of this version of the document.

However it is expected the basic principles governing them remain similar.

## Detailed Procedures at HPMN

The DSP must ensure an LBO-eligible roamer profile contains the EU Internet APN profile with VPAA flag set to ON when roaming in a LBO network. VPAA stands for Visited PLMN Access Allowed and gives right to a visited SGSN to deliver the whole S-G chain for packet data services.

Limitation of the usage of EU Internet APN within EU Countries may result in a definition, for example, of specific service areas into the HLR, containing the list of PLMN allowed to receive this profile. The detail to be listed will be the E.164 Global Title of the SGSN elements in a VPLMN. This information can be retrieved from GSMA PRD IR.21 from each operator, assisted by RAEX Application, where available.

Provisioning and de-provisioning to ARP LBO customers of this APN is an action in charge of the Provisioning group.

To be noted that up today there may be HPMN that are applying Steering mechanisms only to Mobility Procedures coming from visited MSC/VLR, considering the Circuit Switched preference for Location Updating against GPRS Location Updating. The HPMN shall ensure its steering methods are inline with the regulatory requirements.

In addition to the insertion and modification of general subscription data for a PS subscriber, the HLR may request the insertion or modification of one or several new or existing PDP subscription contexts in the SGSN. In particular, the following PDP context parameters may be modified by the HLR:

- QoS Profile Subscribed

- VPLMN Address Allowed

In the case of LBO, the HPMN shall provide the EUinternet APN with the same QoS settings as the internet service for his roaming subscribers using the usual HPMN APN for accessing the internet.

* + - 1. Impacts on usage of Single IMSI+LBO

The HPMN, when acting as DSP, may decide to offer only real-time decoupling facilities (also called convergent mode) to the connected ARP. This approach imposes the ARP service is only available in the CAMEL roaming footprint of the DSP.

Impacts on LBO:

1. Since barring LBO networks is not allowed the following points should be noted:
2. In order for the LBO VPLMN to be able to provide full services (voice, SMS per traditional roaming in addition to LBO Data) to a real-time controlled customer (whether ARP or DSP) the LBO may request a CAMEL agreement with the DSP.
3. The LBO may choose not to ask for CAMEL agreement and therefore the prepaid/ real-time subscriber will have only DATA services (and any other services allowed by the DSP for CAMEL subscribers on non-CAMEL networks) in that network.
4. In such a case the LBO shall inform the LBO subscriber that there may be a loss of service (i.e. MO call), this is to avoid an overload of customer care requests on the DSP.

**Note** Article 3 could enable CAMEL opening obligation for the VPMN (LBO provider) if requested by HPMN.

## Detailed Procedures at LBO

The LBO provider shall be able to receive the proper Internet EU APN with VPAA flag set to Allowed into the MAP Primitive “Insert Subscriber Data”.

Configuration of EU Internet APN into SGSN, DNS, GGSN and Radius are out of scope of this interface and will be detailed in the Whitepaper.

APN Restriction

The support for APN Restriction and Maximum APN Restriction at the SGSN is optional and an APN Restriction value may be configured for each APN in the GGSN or P-GW. The support for reception, storage, and transfer of APN Restriction is required for an S4-SGSN. It is used to determine, on a per MS basis, whether it is allowed to establish PDP Contexts or EPS bearers to other APNs.

APN selection and DNS usage

Preconditions: the customer has EU Internet APN configured in the handset, customer SGSN Profile contains a EU Internet APN and VPAA flag set to TRUE, LBO DNS contains record resolution for APN to one or more LBO GGSN.

APN selection at LBO SGSN steps:

- EUInternet APN (APN (r)) is sent from customer MS to the SGSN [APN(r) is the requested APN]

- SGSN has stored the EuInternet APN (APN (s)) from the ISD subscription procedure [APN(s) is the subscribed APN]

- match verification from SGSN between APN(r) and APN(s)

- VPAA flag verification

- DNS query composition as per above

- PDP Context Activation

GPRS Subscription Data Withdraw with MAP-DELETE-SUBSCRIBER-DATA service from DSP:

This parameter is used to indicate whether all GPRS Subscription Data for the subscriber shall be deleted or if only a subset of the stored GPRS Subscription Data for the subscriber shall be deleted. In the latter case only those PDP contexts whose identifiers are included in the subsequent identifier list will be deleted.

Considerations on GLR implementation in a LBO provider

In case a visited PLMN has implemented a GLR (Global Location Register), the signalling interface between DSP and LBO becomes GLa-interface and it is the same as that between the SGSN and the HLR (see TS 29.002 [26]). The HLR regards the GLR as the SGSN via this interface.



Figure 47 – GLR – HLR interface

## Interface primitives

The IF1 interface is a standard MAP interface that refers to SGSN Gr interface of a Visited PLMN (or GLa interface in case of GLR at the visited PLMN).

The Gr interface is defined between the SGSN and HLR. It allows retrieving or updating GPRS subscription and GPRS location information in the HLR during location-management or authentication procedures.

This interface is used to exchange the data related to the location of the mobile station and to the management of the subscriber. The main service provided to the mobile subscriber is the capability to transfer packet data within a Packet Data Network.

MAP-Update-GPRS-Location service

The SGSN informs the HLR of the location of a mobile station managed by the latter. The HLR sends to the SGSN all the data needed to support the service to the mobile subscriber. Exchanges of data may occur when the mobile subscriber requires a particular service, when he wants to change some data attached to his subscription or when some parameters of the subscription are modified by administrative means.

Signalling on this interface uses the Mobile Application Part (MAP), which in turn uses the services of Transaction Capabilities (TCAP). See TS 29.002.

The mobility management of the roaming customer in a Visited PLMN is handled by the application context gprsLocationUpdateContext, with the following two MAP operations: updateGprsLocation and insertSubscriberData.

MAP-INSERT-SUBSCRIBER-DATA service

This service is used by an HLR to update an SGSN with certain subscriber data in the following occasions:

- if the GPRS subscription has changed;

- if the network access mode is changed;

- the operator has applied, changed or removed Operator Determined Barring;

- the subscriber has changed data concerning one or more supplementary services by using a subscriber procedure;

- the HLR provides the SGSN with subscriber parameters at GPRS location updating of a subscriber

MAP-DELETE-SUBSCRIBER-DATA service

This service is used by an HLR to remove certain subscriber data from an SGSN if the subscription of one or more services is withdrawn.

## Parameters Definitions and Use

Relevant parameters to be considered regarding the Profile Management, transmitted within Location Updating Procedures or Standalone ISD Procedures:

Subscriber Status

It is included either at location updating or when it is changed.

Operator Determined Barring information may be present according to DSP restriction applied to the customer.

GPRS Subscription Data

This parameter contains a list of PDP-contexts a user has subscribed to and it shall contain the EU Internet APN with proper VPAA flag, according to the LBO service selected by the customer.

At GPRS location updating, the HLR shall include the complete GPRS Subscription Data.

When there is a change in GPRS subscriber data the HLR shall include only the new and/or modified PDP contexts and this will be applied during subscription and un-subscription of LBO services. When the SGSN receives GPRS Subscription Data within a dialogue it shall check if the received data has to be considered as the entire GPRS subscription data. If so, it shall replace the stored GPRS Subscription Data with the received data set, otherwise it shall replace the data only for the modified PDP contexts (if any) and add the new PDP contexts (if any) to the stored GPRS Subscription Data.

If the SGSN detects that there is overlapping in the information received within a dialogue, it shall send the error Unexpected Data Value.

Access Restriction Data

This parameter indicates the allowed RAT according to subscription data. It is supposed no Access Restriction is sent by the HLR within this procedure.

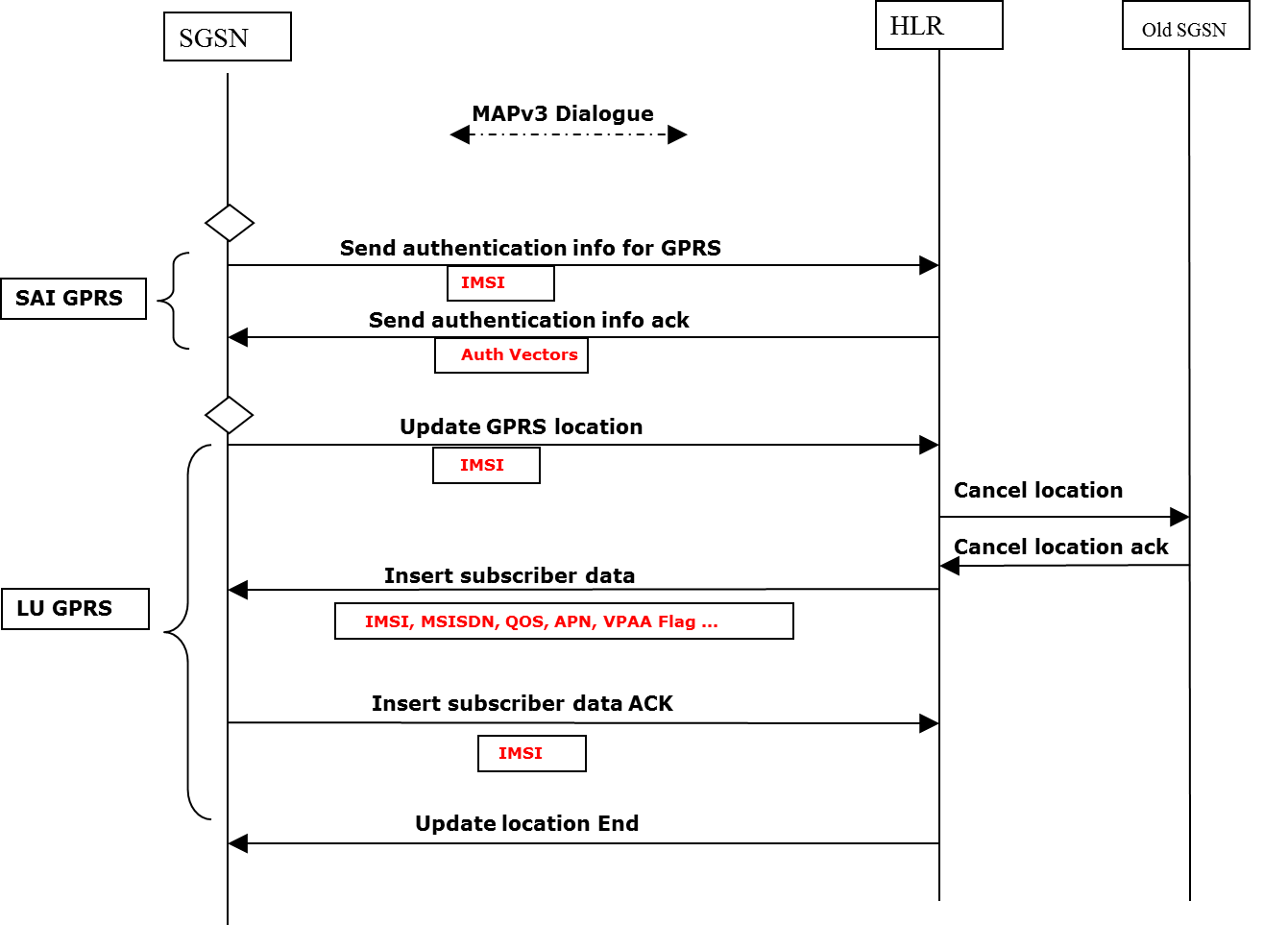


Figure 48 – Update GPRS Location call flow

## Error Handling

Error Handling is implemented according to 3GPP TS 29.002

Implementation errors to be handled as per the roaming agreement.

## LBO-IF2 : LBO notification interface

## Description

The IF2 interface is a NEW interface to provide notification to the HPMN about the subscription and usage of LBO service. The main purpose of the notification is to possibly adjust the traffic steering policy, based on a dynamic subscriber profile management.

**Note** The HPMN refers to the IMSI range owner. The customer may only know his domestic provider, which could be a MNO or a MVNO. It results a HPMN may convey messages for multiple DSP’s – the MNO and its hosted MVNO.

The interface is:

* **Conditional to LBO provider**: LBO provider should send notifications to HPMN if requested to do so. The function sending the notification at the LBO provider is denoted *LBO-V*.

The LBO Provider shall share with the HPMN the LBO-V Application MSISDN/GT used for sending the notifications.

* **Optional to HPMN:** it is up to the HPMN to decide whether it wants to receive or not the notifications. The function receiving the notification at the HPMN side is denoted *LBO-H*.

A HPLMN shall share with LBO provider the LBO-H Application MSISDN/GT where the notifications shall be sent to.

The HPMN shall acknowledge the receipt of the notification; the notification request cannot be used solely for complicating the LBO implementation. However, the corresponding SoR policy adjustments remain at the HPMN’s discretion.

While the notification is designed to address a steering of roaming requirement, the HPMN may use the notification for other purposes. The description of the other possible usage of the notification information is out of scope of this document.

## Interface Setup Description

Since IF2 is a conditional/optional interface, investment reduction and design simplification has been considered while defining this interface.

Accordingly, the following principles are applied:

1. The LBO-V function informs the LBO-H by sending a SMS with a standardized information payload. The delivery of the SMS to the defined MSISDN associated to the LBO-H function happens in a conventional manner i.e. via an SMSC platform, whether owned or 3rd party or via an embedded function at the LBO-V.
2. The HPLMN who has requested notifications must route the SRISM towards LBO-H MSISDN to the LBO-H function and return an 'IMSI' and 'MSC Address'.

The returned IMSI is virtual and may be assigned dynamically, enabling a possible validation of the notification service.

The returned 'MSC-Address' corresponds to the LBO-H GT and ensures the notification is sent to the LBO-H function.

**Note** that this MSISDN need not be in the HPLMN or HPLMN country: any HPLMN using a roaming hub provider may choose to outsource the support of LBO steering modification to that roaming hub provider and supply an MSISDN in the hub's range instead.

It results the interface delivers information towards the HPMN in a quasi-real time fashion.

## Information Exchange Description

The information exchange happens when the customer subscribes to the LBO Offer (before or during its roaming activity) and when he actually activates the LBO service for the first time with the current subscription while roaming in the LBO network.



Figure 49 – Notification flow between LBO-V and LBO-H

1. At subscription time:

The LBO subscriber shall be invited at subscription time to identify its Domestic Service Provider.

For example, the LBO provider may provide a drop-down list of DSP provider, by country.

Subsequently, the LBO provider will use, for this inbound roamer, the DSP information and the associated LBO-H details.

The SMS payload shall include the following information:

1. Type of event: subscription
2. Domestic Service provider (i.e. HPLMN or MVNO name) TADIG Code
3. The customer’s MSISDN
4. The start time of the subscription
5. The validity of the LBO offer taken by the subscriber e.g. the subscriber buys a prepaid voucher, to be used within 7 days.
6. The VPMN MCC/MNC

The maximum duration of the validity period is 1 year (i.e. 365 days).

In the case, the actual expiry date of the voucher goes beyond 1 year, the LBO provider shall resend Subscription notification.

1. At usage time:

The LBO-V function uses the registration information and informs the LBO-H function without end-user intervention.

SMS payload in this case will contain:

1. Type of Message: Usage
2. Domestic Service provider (i.e HPLMN or MVNO name) TADIG Code
3. The customer’s MSISDN
4. The customer’s IMSI.

This is an optional field and can be retrieved during the establishment of the LBO session e.g. using *“Create PDP context request”* message, the *Credit Control Message, etc*. The advantage of sending the IMSI is that it can be directly interpreted by the HPLMN steering platforms. In case not available, HPLMNs are able correlate customers’ MSISDNs with IMSIs

1. The remaining time-credit of the LBO offer taken by the subscriber.
2. The VPMN MCC/MNC

The maximum duration of the time-credit is two weeks (i.e. 14 days).

In case the actually permitted usage goes beyond this period, the LBO shall resend a Usage notification at the end of the period.

## Implementation Details

The LBO-IF2 consists of a dialogue between the LBO-V and LBO-H functions.

The information exchange is based on the exchanged of a SMS whose payload is standardized.

The actual implementation of the LBO-IF2 dialogue is a LBO provider choice under the condition it respects the MT SMS procedure i.e.

1. sending a MAP SRI-SM and
2. a MAP MT-FORWARD-SM (MAPv3) or MAP FORWARD-SM (SMS Deliver) (MAP v1 or MAP v2).

## Prerequisites

**At the LBO side:**

* The LBO-V solution shall emit the notification message to the HPMN using the LBO-V GT communicated during the information exchange as SCCP Calling Party.

The notification procedure being based on a SMS exchange, the LBO-V must set the destination number of the SM and the DSP of the subscriber. This is based on technical information shared by the HPMN when requesting the LBO-IF2 establishment.

It results the request shall include the following offline exchange of information e.g. using the International Roaming agreement documents (IR.21)[[1]](#footnote-1).

* The MSISDN belonging to HPMN pointing to the LBO-H function ;
* A list of the hosted MVNOs

**Note** Hosted MVNOs have no direct relation with LBO providers as MVNOs leverage the existing host network roaming footprint.

**Note** It is worth highlighting that in very exceptional cases where an MVNO is hosted by several MNOs, the request shall include as well an LBO-H/MVNO function GT associated to this exceptional MVNO.

The DSP of the subscriber shall be identified by requesting the subscriber to provide the information at subscription time.

**Note** It is possible the subscriber is ported out from his DSP to another DSP after subscribing the LBO offer but before actually using the LBO offer. In such case, the LBO notification will go to the wrong DSP. The LBO-H will return an error informing the LBO-V solution.

In case of subscriber-DSP identification error, the LBO may either ask the end-user to re-enter its DSP details or rather retry to send then notification to other DSP in the same country (trial and error).

**At the HPMN side:**

* The HPMN shall ensure the processing of SRI-SM messages for the LBO-H MSISDN.
* The LBO-H function shall receive and acknowledge the SM message containing the notification.

The following call flows shows two typical implementation options.

## Implementation Approach Samples

**Implementation Approach 1: LBO-V submits a request to an SMSC platform**

The internal dialogue between the LBO-V and SMSC is based on SMPP in the present call flow and is given for illustration purpose.

The use of alternative protocols is possible and out of scope of this document.

Similarly, the SMSC is shown as part of the VPMN but alternative implementations are possible and are out of scope of this document.



Figure 50 – Implementation example: LBO-V using a SMS-C to communicate with LBO-H

**Implementation Approach 2: LBO sends the SRI-SM and MT-Forward-SM directly**



Figure 51 – Implementation example: LBO-V communicating directly with LBO-H

## Detailed Procedures at HPMN

The Home PLMN LBO-H function shall answer the SRI-SM with

* A virtual IMSI. This IMSI can be fixed or dynamically assigned. In the latter case, it can be used for validating the actual request.
* A virtual MSC. This MSC GT is the actual LBO-H GT for receiving the actual SM.

The Home PLMN LBO-H function shall acknowledged the received MT-FWD-SM received from the LBO provider or return an error to the LBO provider.

## Detailed Procedures at LBO

The LBO provider shall maintain a look-up table: of the DSP and the corresponding MSISDN of the node holding the LBO-H function. The maintenance principles of this table are out of scope of this document.

The LBO provider shall then issue a MAP SRI-SM message using the LBO-H MSISDN.

The subsequent MT-FWD-SM will be sent to receive virtual IMSI and the virtual MSC address. The payload will be built as indicated below.

It is up to the LBO provider to decide the retry mechanism when the HPMN returns an error associated to these operations.

## Interface primitives

The interface LBO-IF2 is based on the standard MAP protocol according to 3GPP TS 29.002 for MAPv1, MAPv2 or MAPv3.

The interface LBO-IF2 relies on the exchange of the following MAP messages between the LBO provider and the HPMN.

* MAP Send Routing Info for SM (MAP v1, v2, or v3)
* MAP MT-Forward SM (MAP v3) or MAP-Forward SM (SMS Deliver) (MAP v1 or MAP v2)

The use of MAP messages was dictated by the following reasons:

* The recipient application (SoR solution) is a SS7 MAP-based solution,
* The VPMN acting as LBO provider and the HPMN have an existing SS7 MAP relationship,

## Message Details

## MAP SRI-SM

|  |  |  |
| --- | --- | --- |
| SCCP parameters | Value | Comments |
| Cg-SCCP Address | LBO-V GT | The SMSC may support the LBO-V function |
| Cd-SCCP Address | LBO-H MSISDN | The SRI-SM will be routed to the LBO-H function. |
| MAP parameters | Value | Comments |
| MSISDN | LBO-H MSISDN | As received by HPMN when requesting the LBO IF2 establishment for his outbound roamers. |
| SM-RP-PRI | True or False | at LBO discretion. |
| Service Centre Address | LBO-V GT | The SMSC may support the LBO-V function |

## MAP SRI-SM ACK

|  |  |  |
| --- | --- | --- |
| SCCP parameters | Value | Comments |
| Cg-SCCP Address | LBO-H GT |  |
| Cd-SCCP Address | LBO-V GT |  |
| MAP parameters | Value | Comments |
| IMSI | Virtual IMSI | Fixed value or dynamic value for validation |
| MSC Number | LBO-H GT |  |

## MAP MT-FWD-SM or FWD-SM

The exchange of the notification is based on 2 layers:

* a transport layer : the Short Message
* a payload layer : the actual information about the LBO subscription

The transport layer parameters are:

|  |  |  |
| --- | --- | --- |
| SCCP parameters | Value | Comments |
| Cg-SCCP Address | LBO-V GT | The SMSC may support the LBO-V function |
| Cd-SCCP Address | LBO-H GT | As received by the SRI-SM operation |
| MAP parameters | Value | Comments |
| SM-RP-DA | IMSI | As received by the SRI-SM operation |
| SM-RP-OA | LBO-V GT |  |
| SM-RP-UI |  |  |
| TP-Reply-Path (TP-RP) | 0 | No Reply-Path set (*irrelevant field*) |
| TP-User-Data-Header-Indicator (TP-UDHI) | 0 | The TP-UD field contains only the short message (*irrelevant field*) |
| TP-Status-Report-Indication (TP-SRI) | 0 | No Status Report required (*irrelevant field*) |
| TP-More Message to Send (TP-MMS) | 1 | No More message (*irrelevant field*) |
| TP-Message Type Indicator (TP-MTI) | SMS DELIVER |  |
| TP-Destination-Address (TP-DA) | LBO-H GT |  |
| TP-Protocol-Identifier (TP-PID) | 0 | (*irrelevant field*) |
| TP-Data Coding Scheme (TP-DCS) | 0 | Default |
| TP-Service-Centre-Time-Stamp (TP-SCTS) | Date and Timestamp and Time Zone of LBO provider |  |
| TP-User-Data-Length (TP-UDL) | Length of the user data |  |
| TP-User-Data | **Notification Message** | ***See below for details*** |

The payload parameters:

The Notification message is a comma-delimited string that is built using the following parameters:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Parameter | M/O/C | Format | Value | Description |
| 1 | Start Code (Subscription / Usage) | M | String | “S” or “U” | S – subscription  U – usage |
| 2 | Validity Period – Days | M | Integer |  | Number of days  max: 365 for subscription  max:7 for usage |
| 3 | Start Date | M | String | YYYYMMDDhhmmss | The given time is given UTC timezone. |
| 4 | LBO Customer MSISDN | C | String |  | MSISDN (international format) of the LBO subscriber  e.g. “32495123456”  Must be present except for MSISDN-less customers |
| 5 | LBO Customer IMSI | C | String |  | Must be present for MSISDN-less customers |
| 6 | VPMN ID | M | String | MCCMNC | MCC/MNC e.g. “20610” |
| 7 | DSP ID | M | String | TADIG | TADIG Code of DSP (e.g. HPMN or MVNO) |

**Note**: The VPMN ID is given in MCC/MNC for simplifying the Steering of Roaming Platform configuration.

In case the LBO provider uses multiple MCC/MNC for inbound roaming (e.g. a 2G MCC/MNC and a 3G MCC/MNC), it shall send multiple notifications.

The maximum size of the payload is 160 characters.

Examples:

S,365,20140702000000,32495123456**,,**20801,BELMO

U,1,20140702140000,32495123456,206101234512345,20801,BELMO

Or, in case of usage message without IMSI or MSISDN:

U,1, 20140702140000**,,**206101234512345,20801,BELMO

U,1, 20140702140000,32495123456**,,**20801,BELMO

## Error Handling

The error handling concerning the IMSI information retrieval and the transport of the notification is implemented according to 3GPP TS 29.002.

Errors could be returned online (using the error codes as defined below) or using existing offline communication channels between the parties.

The LBO-H implementation will determine whether online or offline error handling will be used i.e. whether the SM payload is verified prior to acknowledging the MT-FWD-SM / FWD-SM.

**Notification Validation error**

The LBO-H function shall return the following errors when the MT-FWD-SM / FWD-SM cannot be validated against the SRI-SM operation i.e. the IMSI received does not correspond to the IMSI returned from the SRI-SM operation

* *Illegal Subscriber*: the SM-RP-DA does not correspond to the IMSI provided in the SRI-SM ACK.

**Notification Content errors**

The LBO-H function shall return the following errors when the notification content is erroneous:

* *Unidentified subscriber*: the MSISDN/IMSI is not belonging to the HPMN.
* *Unexpected Data Value*: the content of the message does not respect the content rule.
* *Data Missing*: fields are missing in the notification string.

**Note** In case of an implementation of the LBO-V function using an SMSC, the LBO provider should to check how the MAP error is passed from the SMSC to the LBO-V function, in case of a LBO-H rejection.

This may happen transparently, for example, using SMPP v3.4 – as the sm\_deliver message contains the network\_error\_code, which corresponds directly to the MAP error.

Alternately, for other protocols e.g. CIMD or UCP, a mapping table may be required between the MAP error code and the error code.

## Security Note

Security concerns were raised during the design phase of the interface.

Concerns were mainly related to the following items:

- The introduction of the LBO-IF2 interface should not provide facilities for subscriber look-up at HLR;

- Any party should not be able to fool an HPMN with fake notifications, spoofing the LBO-V parameters.

The proposed implementation covers these items:

- No subscriber look-up is performed as the SRI-SM only reaches the LBO-H function;

- Notification is received after a LBO-H interrogation (2-step approach) meaning,

In case of spoofing method, the SRI4SM answer will get back to the “spoofed” GT not to the actual sender (spoofing party). Hence the spoofing party cannot see the virtual IMSI returned by the LBO-H function.

If the spoofer sends the MT-FWD, the notification will be discarded as it will fail containing the virtual IMSI.

Additionally, the exchange of LBO-H and LBO-V GT between the LBO and HPMN enables the configuration of SCCP filters based on SCCP Calling Party.

While the proposed scenario offers a minimal security, it does not pretend to be perfect. However it should provide sufficient confidence in the context of the LBO business.

## ANNEX - Study on Home Routing and Legal interception cases

## DSP Home Routing – CAP v1

The figure below illustrates the scenarios when the DSP administrates the re-routing number ranges in a separate network entity/proxy. The re-routing number range does not affect the signaling and the service of the ARP. The DSP has the exclusive responsibility about this number range.

Next to the re-routing numbers the proxy has the responsibility to setup a CAP IDP operation (5) to the dedicated ARP network element (NE). This IDP operation (5) must contain at least the original calling and called party numbers and the location information (VLR address of the EU Visited MSC) from the first IDP operation (1).



Figure 52 – DSP Home Routing with CAP v1 interface to ARP

Pros:

* DSP has the responsibility about the administration of the re-routing numbers. This number range need to be not considered in the IR.21 document.
* DSP is aware about signaling and the Proxy or the Gateway MSC generates IN CDRs for Wholesale Billing.

Cons:

* The proxy requires a service logic for identification of the two correlated trigger (1 and 4). A new CAP IDP operation (5) for the ARP NE must be setup by the proxy.
* Because of the limited CAP v1 operations no announcements are supported (ConnectToResource, EstablishTemporaryConnection).
* The ARP has to inform a customer about e.g. low credit with a SMS or USSD string (both interfaces are optional).

## DSP Home Routing – CAP v2

This scenario is comparable with the scenario in previous chapter. The difference is a CAP v2 interface between the DSP and ARP. The advantage of CAP v2 is the support of announcement operations except the mid call announcement. The EDP (8) is available since Camel v4.



Figure 53 – DSP Home Routing with CAP v2 interface to ARP

Pros:

* DSP has the responsibility about the administration of the re-routing numbers. This number range need to be not considered in the IR.21 document.
* DSP is aware about signaling and the Proxy or the Gateway MSC generates IN CDRs for Wholesale Billing.
* ARP can initiate announcements (ConnectToResource, EstablishTemporaryConnection) for his subscribers, e.g. low credit.

Cons:

* The proxy requires a service logic for identification of the two correlated trigger (1 and 4). A new CAP IDP operation (5) for the ARP NE must be setup by the proxy.

## ARP Home Routing – CAP v1

In this scenario the ARP disposes of an own re-routing number range. The owner of this range is the DSP but the usage is restricted for the ARP.



Figure 54 – ARP Home Routing with CAP v1 interface to ARP

Pros:

* Dependent of the calling party number the proxy has to forward the trigger to the dedicated ARP. The administration of correlated IDP operations is not in the proxy but in the ARP NE required.
* DSP is aware about signaling and the Gateway MSC is able to generate CDRs for Wholesale Billing.

Cons:

* The DSP has to reserve for every ARP a unique re-routing number range.
* For an ARP additional development effort is required for identification of the correlated IDP operations.
* Because of the limited CAP v1 operations no announcements are supported (ConnectToResource, EstablishTemporaryConnection).
* The ARP has to inform a customer about e.g. low credit with a SMS or USSD string (both interfaces are optional).

## ARP Home Routing – CAP v2

This scenario is comparable with the previous CAP V1 – ARP Home routing scenario. The difference is only the CAP v2 interface between the Proxy and the ARP.



Figure 55 – ARP Home Routing with CAP v2 interface to ARP

Pros:

* Dependent of the calling party number the proxy has to forward the trigger to the dedicated ARP. The administration of correlated IDP operations is not in the proxy but in the ARP NE required.
* DSP is aware about signaling and charging of ARP subscribers. The Gateway MSC is able to generate CDRs for Wholesale Billing.
* ARP can initiate announcements (ConnectToResource, EstablishTemporaryConnection) for his subscribers, e.g. low credit except the mid call announcement. The EDP (8) is available since Camel v4.

Cons:

* The DSP has to reserve for every ARP a unique re-routing number range.
* For an ARP additional development effort is required for identification of the correlated IDP operations.

## Legal Interception

Dependent on the national legal requirement it has to be investigated if an interception of the ARP subscribers is required in the HPLMN of the DSP.

## Summary of the solutions



(\*) Since CAP v2 announcement operations are supported

**End of Document**

1. The actual information exchange process shall be described in the EU regulation III Process document. [↑](#footnote-ref-1)