3GPP TR 32.808 V8.0.0 (2007-06)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Study of Common Profile Storage (CPS) Framework of User Data for network services and management (Release 8)

Keywords
Object Model, management

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The present document studies the problems and potential improvements in the way user data is introduced and handled in the 3GPP based networks. Related to these studies this Technical Report investigates the need to introduce a common end-user profile storage framework into 3GPP conformant communication networks.

The introduction of a Common Profile Storage Framework of User Data ("Common" in the sense of common to all applications) for network services and management applications could significantly enhance the ability of 3GPP based networks to offer complex and combined services in the areas of:

- Multimedia.
- Data services.
- Value Added Services.
- End-to-end applications.

In light of developments both within 3GPP (e.g. IMS, MBMS, OCS, PCC) and outside 3GPP (e.g. NGN, OMA, etc.) with a growing number of physically disjoint but logically correlated user data stored in several data bases a consolidation and co-ordination of these is needed to prevent further redundancy and possible contradiction and to enable operators to administer and provision complex and combined services.

Initial study of the user related data within and outside 3GPP is necessary to assess the properties of such a Common User Profile Storage Framework based on

- the needs of Network Elements like MMS-RS, HLR, HSS, BM-SC; and
- features like Service Management, Subscription Management and Charging Management.

On-going efforts within the mobile and NGN community to define advanced services within the network (i.e. 3GPP, TISPAN) should provide valuable drive for developing the Common Profile Storage Framework functionality for 3GPP.

1 Scope

The present document investigates possibilities to introduce an end-user profile storage framework into 3GPP conformant communication networks. To this end the following topics are covered:

- Analysis of the consequences of creating one common data model structure for an end user:
  - Existing data specifications concerning an end-user or a subscriber in 3GPP, TISPAN, OMA and other relevant standardization groups are listed and used as a basis for the proposal of a structure for a common end-user data model.
  - Topics connected to the fact that one common data model exists, like minimizing data redundancy, access control, providing views for applications are highlighted.
  - The relationship between an end user and a subscriber as defined by 3GPP is revisited in light of the fact that the relations between subscribers (contract holders) and end-users can be n:m.
- Current initiatives connected to subscription information carried out inside and outside 3GPP are covered.
- Analysis of differences and deficiencies concerning 3GPP's current status of specifications (e.g. GUP, SuM, etc.) in comparison to existing/emerging solutions with centralized or distributed storage models.
- Identification of items for standardization as a result of the analysis described in the bullet above.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.008 (V7.2.0): "Organization of subscriber data (Release 7)".

[3] 3GPP TS 23.003 (V7.0.0): "Numbering, addressing and identification (Release 7)".

[4] 3GPP TS 23.097 (V6.0.0): "Multiple Subscriber Profile (MSP) (Phase 1) - Stage 2 (Release 6)".

[5] 3GPP TS 23.016 (V6.1.0): "Subscriber data management; Stage 2 (Release 6)".

[6] 3GPP TS 32.140 (V6.3.0): "Telecommunication management; Subscription Management (SuM) requirements (Release 6)".

[7] 3GPP TS 32.141 (V6.1.0): "Telecommunication management; Subscription Management (SuM) architecture (Release 6)".

[8] 3GPP TS 32.171 (V6.1.0): "Telecommunication management; Subscription Management (SuM) Network Resource Model (NRM) Integration Reference Point (IRP): Requirements (Release 6)".

[9] 3GPP TS 32.172 (V6.3.0): "Telecommunication management; Subscription Management (SuM) Network Resource Model (NRM) Integration Reference Point (IRP): Information Service (IS) (Release 6)".

[10] 3GPP TS 32.175 (V6.2.0): "Telecommunication management; Subscription Management (SuM) Network Resource Model (NRM) Integration Reference Point (IRP): eXtensible Markup Language (XML) definition (Release 6)".

[11] 3GPP TS 23.240 (V6.7.0): "3GPP Generic User Profile (GUP) requirements; Architecture (Stage 2) (Release 6)".

[12] 3GPP TR 23.941 (V6.0.0): "3GPP Generic User Profile (GUP); Stage 2; Data Description Method (DDM) (Release 6)".

[13] 3GPP TS 23.002 (V7.1.0): "Network architecture (Release 7)".

[14] 3GPP TS 23.101 (V6.0.0): "General Universal Mobile Telecommunications System (UMTS) architecture (Release 6)".

[15] 3GPP TS 33.102 V7.0.0 (2005-12): "3G Security; Security architecture (Release 7)".

[16] 3GPP TS 43.020 V6.4.0 (2006-06): "Security related network functions (Release 6)".

[17] 3GPP TS 23.060 V7 .1.0 (2006-06): "General Packet Radio Service (GPRS); Service description; Stage 2 (Release 7)".

[18] 3GPP TS 23.271 V6.13.0 (2005-09): "Functional stage 2 description of Location Services (LCS) (Release 6)".

[19] 3GPP TS 25.305: "User Equipment (UE) positioning in Universal Terrestrial Radio Access Network (UTRAN); Stage 2".

[20] 3GPP TS 43.059: "Functional stage 2 description of Location Services (LCS) in GERAN".

[21] 3GPP TS 23.141 (V6.9.0): "Presence service; Architecture and functional description; Stage 2 (Release 6)".

[22] 3GPP TS 23.228 (V7.4.0): "IP Multimedia Subsystem (IMS); Stage 2 (Release 7)".

[23] 3GPP TS 33.222 (V7.1.0):"Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (Release 7)".

[24] 3GPP TS 33.102 (V7.0.0): "3G Security; Security architecture (Release 7)".

[25] Draft ETSI TS 188 002-1 (V0.0.7): "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Subscription Management; Part 1: Requirements".

[26] Draft ETSI TS 188 002-2 (V0.0.3): "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Subscription Management; Part 2: Information Model".

[27] TISPAN WG8 interim meeting WG8TD08 Sophia Antipolis, 3 - 5 May 2006: "Remaining Comments".

[28] 3GPP2 S.R0037-0 v3.0 Version Date: August 21, 2003 Version 3.0: "IP Network Architecture Model for cdma2000 Spread Spectrum Systems".

[29] 3GPP2 X.S0027-001-0 Version 1.0 Date: September, 2004: "Presence Service: Architecture and Functional Description".

[30] OMA-TS-Presence_SIMPLE-V1_0-20060418-C Candidate Version 1.0 - 18 Apr 2006: "Presence SIMPLE Specification".

[31] OMA-AD-Presence_SIMPLE-V1_0-20060110-C Candidate Version 1.0 - 10 Jan 2006: "Presence SIMPLE Architecture Document".

[32] OMA-AD_IMS-V1_0-20040420-D Draft Version 1.0 - 20 Apr 2004: "Utilization of IMS capabilities Architecture".

[33] OMA-TS-MLP-V3_2-20051124-C Candidate Version 3.2 - 24 Nov 200:5 "Mobile Location Protocol 3.2".

[34] OMA-AD-MLS-V1_0-20050607-C Candidate Version 1.0 - 07 June 2005: "OMA Mobile Location Service Architecture".

[35] OMA-TS-XDM_Core-V1_0-20060612-A Approved Version 1.0 - 12 Jun 2006: "XML Document Management (XDM) Specification".

[36] OMA-TS-DM_StdObj-V1_2-20060602-C Candidate Version 1.2 - 02 Jun 2006: "OMA Device Management Standardized Objects".

[37] OMA-SyncML-DMStdObj-V1_1_2-20031203-A Approved version 03-December-2003: "SyncML Device Management Standardized Objects, Version 1.1.2".

[38] OMA-Security-CertProf-V1_1-20040615-C Candidate Version 1.1 - 15 Jun 2004: "Certificate and CRL Profiles".

[39] IETF RFC 2778 (February 2000): "A Model for Presence and Instant Messaging", M. Day, J. Rosenberg, H. Sugano.

[40] IETF RFC 2924 (September 2000): "Accounting Attributes and Record Formats", N. Brownlee, A. Blount.

[41] IETF RFC 3588 (September 2003): "Diameter Based Protocol", P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko.

[42] IETF RFC 3280 (April 2002): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", R. Housley, W. Polk, W. Ford, D. Solo.

[43] IETF RFC 2560 (June 1999): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams.

[44] ITU-T Recommendation X.509 (08/2005): "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks" 08/2005.

[45] ITU-T Recommendation Q.822 (04/1994): "Stage 1, stage 2 and stage 3 description for the Q3 interface - Performance management.

[46] Identity Management Systems (IMS): Identification and Comparison Study Independent Centre for Privacy Protection (ICPP) /Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein and Studio Notarile Genghini (SNG) 2003-09-07 Contract N°19960-2002-10 F1ED SEV DE.

[47] 3GPP TS 32.240 (V6.3.0): "Telecommunication management; Charging management; Charging architecture and principles (Release 6)".

[48] 3GPP TS 22.115 (V6.7.0): "Service aspects; Charging and billing (Release 7)".

[49] 3GPP TS 22.140 (V6.7.0): "Multimedia Messaging Service (MMS); Stage 1 (Release 6)".

[50] 3GPP TS 23.140 (V6.9.0): "Multimedia Messaging Service (MMS); Functional description; Stage 2 (Release 6)".

[51] 3GPP TS 22.242 (V6.3.0): "Digital Rights Management (DRM); Stage 1 (Release 6)".

[52] 3GPP TS 22.146 (V8.1.0): "Multimedia Broadcast/Multicast Service (MBMS); Stage 1 (Release 8)".

[53] 3GPP TS 22.246 (V8.1.0): "Multimedia Broadcast/Multicast Service (MBMS) user services; Stage 1 (Release 8)".

[54] 3GPP TS 22.240 V6.5.0 (2005-01): "Service requirement for the 3GPP Generic User Profile (GUP); Stage 1 (Release 6)".

[55] 3GPP TS 29.240 V6.1.0 (2005-06): "3GPP Generic User Profile (GUP); Stage 3; Network; (Release 6)".

[56] 3GPP TS 23.228 V7.4.0 (2006-06): "IP Multimedia Subsystem (IMS); Stage 2 (Release 7)".

[57] 3GPP TR 23.979 V6.2.0 (2005-06): "3GPP enablers for Open Mobile Alliance (OMA); Push-to-talk over Cellular (PoC) services; Stage 2 (Release 6)".

[58] 3GPP TR 25.zyx V0.0.1 Draft2(2006-0x): "Improved support of gaming over HSDPA/EDCH (Release 7)".

[59] 3GPP TS 29.078 (V7.3.0): "Customised Applications for Mobile network Enhanced Logic (CAMEL); CAMEL Application Part (CAP) specification (Release 7)".

[60] 3GPP TS 32.104 (V4.0.0): "Telecommunication Management; 3G Performance Management (Release 4)".

[61] 3GPP TS 22.259 (V8.1.0): "Service requirements for Personal Network Management (PNM); Stage 1 (Release 8)".

[62] 3GPP TR 23.818 (V0.8.0): "Optimisations and Enhancements for Realtime IMS communication (Release 7)".

[63] ETSI ETS 300 374-1 (1994): "Intelligent Network (IN); Intelligent Network Capability Set 1 (CS1); Core Intelligent Network Application Protocol (INAP); Part 1: Protocol specification".

[64] ETSI EN 301 140-1 (V1.3.4): "Intelligent Network (IN); Intelligent Network Application Protocol (INAP); Capability Set 2 (CS2); Part 1: Protocol specification".

[65] ETSI EN 301 931-1 (V1.1.2): "Intelligent Network (IN); Intelligent Network Capability Set 3 (CS3); Intelligent Network Application Protocol (INAP); Protocol specification; Part 1: Common aspects".

[66] 3GPP2 S.R0064-0, Version 1.0, Version Date: 30 October 2002:" Multimedia Messaging Services (MMS); Stage 1 Requirements".

[67] OMA-TS-PoC_XDM-V1_0-20060609-A Approved Version 1.0 - 09 June 2006: "PoC XDM Specification".

[68] OMA-RD-CPv12-V1_0-20050825-D, Draft Version 1.0 -25 Aug 2005: "Client Provisioning v1.2 Requirements".

[69] OMA-RD-GPM-V1_0-20060824-D, Draft Version 1.0 - 24 Aug 2006: "Global Permissions Management Requirements".

[70] OMA-AD-GPM-V1_0-20060828-D, Draft Version 1.0 - 28 Aug 2006: " Global Permissions Management Architecture".

[71] OMA-AD-Policy_Evaluation_Enforcement_Management-V1_0 - 2006625-D, Draft Version 1.0 - 25 June 2006: "Policy Evaluation, Enforcement and Management Architecture".

[72] OMA-MMS-ARCH-V1_2-20050301-A, Approved Version 1.2 - 01 Mar 2005: "Multimedia Messaging Service, Architecture Overview".

[73] OMA-MMS-ENC-V1_2-20050301-A, Approved Version 1.2 - 01 Mar 2005: "Multimedia Messaging Service Encapsulation Protocol".

[74] OMA-AD-Charging-V1_0-20060825-D, Draft Version 1.0 - 25 Aug 2006: "Charging Architecture".

[75] OMA-RD_Charging-V1_0-20041118-C, Candidate Version 1.0 - 18 Nov 2004: "Charging Requirements".

[76] OMA-AD-BCAST-V1_0-20060329-D, Draft Version 1.0 -29 March 2006: "Mobile Broadcast Services Architecture".

[77] OMA-RD-DCD-V1_0-20060530-C, Candidate Version 1.0 - 30 May 2006: " Dynamic Content Delivery Requirements".

[78] OMA-AD-DCD-V1_0-20061014-D, Draft Version 1.0 - 14 October 2006: "Dynamic Content Delivery Architecture".

[79] OMA-AD-IMS-V1_0-20050809-A, Approved Version 1.0 - 9 Aug 2005: "Utilization of IMS capabilities Architecture".

[80] OMA-AD-IMPS-V1_3-20051011-C, Candidate Version 1.3 - 11 Oct 2005: "IMPS Architecture".

[81] OMA-AD_PoC-V1_0-20060609-A, Approved Version 1.0 - 09 Jun 2006: "Push to talk over Cellular (PoC) - Architecture".

[82] OMA-AD-DS-V2_0-20061011-D, Draft Version 2.0 - 11 Oct 2006: "DS 2.0 Architecture"

[83] OMA-AD-Game-Services-V1_0-20060307-C, Candidate Version 1.0 - 03 Mar 2006: "Game Services Architecture".

[84] WID: General Service Subscription Management (GSSM) 0136.

[85] OMA-RD-GSSM-V1_0-20061005-D, Draft Version 1.0 - 5 Oct 2006: " General Service Subscription Management Requirements".

[86] OMA-RD-Identity_Management_Framework-V1_0-20050202-C, Candidate Version 1.0 - 02 Feb 2005: "Identity Management Framework Requirements".

[87] IETF RFC 3060 (February 2001): "Policy Core Information Model - Version 1 Specification", B. Moore, E. Ellesson, J. Strassner, A. Westerinen.

[88] IETF RFC 2251 (December 1997): "Lightweight Directory Access Protocol (v3)", M. Wahl, T. Howes, S. Kille.

[89] ITU-T Recommendation X.500 (02/2001): "Informations technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services".

[90] ITU-T Recommendation Q.1211 (03/1993): "Introduction to intelligent network capability set 1".

[91] ITU-T Recommendation Q.1231 (09/1997): "Introduction to Intelligent Network Capability Set 3".

[92] ITU-T Recommendation Q.1221 (12/1997): "Introduction to Intelligent Network Capability Set 2".

[94] ITU-T Recommendation M.3400 (02/2000): "TMN management functions".

[95] TMF Annex TMF053D, Release 4.0, Approved Version 1.1, August 2004: "NGOSS Architecture, Technology Neutral Specification, Metamodel".

[96] TMF Annex TMF053B, Release 4.0, Approved Version 4.5, August 2004: "NGOSS Architecture, Technology Neutral Specification, Contract Description: Business and System Views".

[97] TMF Annex TMF053C, Release 4.0, Approved Version 1.1, August 2004: "NGOSS Architecture, Technology Neutral Specification, Contract Description: Behaviour and Control Services".

[98] TMF 053, Release 4.0, Approved Version 4.1, August 2004: "The NGOSS Technology Neutral Architecture".

[99] GB922, Release 4.0, Approved Version 3.2, August 2004: "Shared Information Data (SID) Model; Concepts, Principles, and Domains".

[100] GB922 Addendum 2, Release 4.0, Approved Version 3.2, August 2004: "Customer Business Entity Definitions".

[101] IETF RFC 3856: "A Presence Event Package for the Session Initiation Protocol (SIP)".

[102] IETF RFC 2141: "URN Syntax".

[103] IETF RFC 1766: "Tags for the Identification of Languages".

[104] ISO 639: "Codes for the representation of names of languages".

[105] IETF RFC 2822: "Internet Message Format".

[106] IETF RFC 2486: "The Network Access Identifier".

[107] 3GPP TS 22.228: "Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1".

[108] IETF RFC 3966: "The tel URI for Telephone Numbers".

[109] ITU-T Recommendation I.356: "B-ISDN ATM layer cell transfer performance".

[110] ITU-T Recommendation I.371: "Traffic control and congestion control in B-ISDN".

[111] 3GPP TS 32.251: "Telecommunication management; Charging management; Packet Switched (PS) domain charging".

[112] ITU-T Recommendation M.20: "Maintenance philosophy for telecommunication networks".

[113] 3GPP TS 32.111-1 V6.0.1 (2005-06) "Technical Specification Group Services and System Aspects; Telecommunication management; Fault Management; Part 1: 3G fault management requirements; (Release 6)"

[114] GB921, Release 5.0, Enhanced Telecom Operations Map (eTOM): The Business Process Framework; April 2005: "For the Information and Communications Services Industry"

[115] GB921 F, Release 4.5, Addendum F, Enhanced Telecom Operations Map (eTOM): The Business Process Framework; November 2004: "Process Flow Examples"

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply:

NOTE: A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

adaptation layer function: function provided by the Common Profile Storage Framework to decouple any application from the actual data store

application: this notion is only used in the contexts of the respective standard documents
This means that the explanation can be found in the cited reference documents.

application front end: data access part of an application of the Common Profile Storage (CPS) Framework

contract holder: A Contract Holder is a Subscriber that makes a (sub-)set of his subscribed services available to the End-Users that are assiciated with the Subscriber

data entities: logical data model is an abstract DBMS-independent representation of a set of data entities and their relationships within the scope of a system
A logical data model typically includes all the entities and their attributes that correspond to a set of specified information requirements, which includes the definition of logical constraints on these attributes.

end user: person actually consuming a service, in 3GPP defined as user in opposition to a subscriber

network function: function within the 3GPP or OMA, etc., service Architecture or Management Network making use of the Common Profile Storage (CPS) Framework

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply:

NOTE: An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

AAA	Authentication, Authorization and Accounting
AAB	Automatic Alternative Billing
ABD	Abbreviated Dialling
ABMF	Account Balance Management Function
ACC	Account Card Calling
ACE	Agnostic Charging Entity
ACID	Atomicity - Consistency - Isolation - Durability
AKA	Authentication and Key Agreement
ALF	Adaptation Layer Function
APN	Access Point Name
ARAP	Appletalk Remote Access Protocol
AS	Application Server
ASN.1	Abstract Syntax Notation Number One
AuC	Authentication Center
AUID	Application Unique ID
AVP	Attribute Value Pair
BCAST	Mobile Broadcast
BD	Billing Domain

NOTE: This may also be a billing system/ billing mediation device.

BDS	Broadcast Distribution System
B2BUA	Bach-to-Back User Agent
BSF	Bootstrapping Server Function
BSG	Basic Service Group
CA	Certification Authority
CAMEL	Customized Application for Mobile Networks Enhanced Logic
CAP	CAMEL Application Part
CC	Call Control
CCBS	Completion of Calls to Busy Subscriber
CCC	Credit Card Calling
CD	Call Distribution
CDF	Charging Data Function
CDMA	Code Division Multiple Access
CDR	Call Detail Record (ITU-T) Charging Data Record (3GPP)
CF	Call Forwarding
CGF	Charging Gateway Function
CGI	Cell Global Identification
CHAP	Challenge-Handshake Authentication Protocol
CLF	Connectivity Session Location Function
CN	Core Network
CPE	Customer Premises Equipment
CRM	Customer Relationship Management
CON	CONference calling
CPS	Common Profile Storage
CPSF	Common Pofile Storage Framework
CRL	Certificate Revocation List
CS	Circuit Switched
CS-x	Capability Set x
CRD	Call Rerouting Distribution
CTF	Charging Trigger Function

CUG	Closed User Group
DAP	Directory Access Protocol
DBMS	Data Base Management System
DCD	Dynamic Content Delivery
DCR	Destination Call Routing
DER	Distinguished Encoding Rules
DISP	Directory Information Shadowing Protocol
DIT	Directory Information Tree
DM	Device Management
DOP	Directory Operational Binding Management Protocol (DOP)
DRM	Digital Right Management
DSA	Directory Server Agent
DSP	Directory System Protocol
DUA	Directory User Agent
EBSG	Elementary Basic Service Group
EIR	Equipment Identity Register
eTOM	enhanced Telecom Operations Map
FE	Front End
FMD	Follow-Me Diversion
GBA	Generic Bootstrapping Architecture
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GPM	Global Permission Management
GPRS	General Packet Radio System
GPRS NAM	GPRS Network Access Mode
GPS	Global Positioning System
GSSM	General Service Subscription Management
GUP	Generic User Profile
GUSS	GBA User Security Settings
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
HSDPA	High Speed Downlink Packet Access
HSUPA	High Speed Uplink Packet Access
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Taskforce
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMEISV	IMEI Software Version
IMPS	Instant Messaging and Presence Service
IM-SSF	IP Multimedia Service Switching Function
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
INAP	IN Application Part
IP	Internet Protocol
IPX	Internetwork Packet eXchange
IR	Infrared
IRP	Integration Reference Point
ISC	IMS Service Control
ISDN	Integrated Services Digital Network
ISIM	IM Services Identity Module
ISO	International Organisation for Standardisation
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LAI	Local Area Identification
LAT	LDAP Radius Termination Action
LCS	Location Services
LDR	Location Deferred Request.
LIR	Location Immediate Request
LMSI	Local Mobile Station Identity
LMU	Location Measurement Unit

LSA	Localised Service Area
MAP	Mobile Application Part
MBMS	Multimedia Broadcast and Multicast Service
MCI	Malicious Call Identification
MIME	Multipurpose Internet Mail Extensions
MLS	Mobile Location Service
MMD	Multimedia Domain
MMS	Multimedia Messaging Service
MNP	Mobile Number Portability
MS	Mobile Station
MSC	Mobile Switching Center
MSCF	Messaging Service Control Function
MSISDN	Mobile Subscriber ISDN Number
NACF	Network Access Configuration Function
NAF	Network Application Function
NAS	Network Access Server
NE	Network Element
NGN	Next Generation Networks
NGOSS	New Generation Operations System and Software
NRM	Network Resource Model
OCF	Online Charging Function
OCS	Online Charging System
OCS	Originating Call Screening
ODB	Operator Determined Barring
OMA	Open Mobile Alliance
OSA	Open Service Architecture
OSE	OMA Service Environment
PAN	Personal Aera Network
PCC	Personal Computing and Communications
PDA	Personal Digital Assistant
PDBF	Profile Database Function
PDG	Packet Data Gateway
PDP	Packet Data Protocol
PEEM	Policy Evaluation, Enforcement and Management
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMI	Privilege Management Infrastructure
PNA	Presence Network Architecture
PNE	Personal Network Element
PNM	Personal Network Management
PNP	Private Numbering Plans
PoC	Push to talk over Cellular
POP	Post Office Protocol
POTS	Plain Old Telefone Service
PS	Packet Switched
	Presence Server
QoS	Quality of Service
PTN	Personal Telecommunication Number
RADIUS	Remote Authentication Dial In User Service
RAF	Repository Access Function
RAI	Routing Area Identification
RAN	Radio Access Network
RAS	Reliability, Availability and Survivability
RF	Rating Function
RLS	Resource List Server
RSA	Algorithm invented by Rivest, Adleman and Shamir
SAI	Service Area Identity
SCE	Service Creation Environment
SCP	Service Control Point
S-CSCF	Serving Call Session Control Function

SDP	Session Description Protocol
	Service Data Point
SGSN	Serving GPRS Support Node
SLF	Subscription Locator Function
SID	Shared Information Model
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SN	Switching Network
SS	Supplementary Services
SS7	Signalling System Number 7
SuM	Subscription Management
TAN	Transaction Number
TBSCertificate	To Be Signed Certificate
TCS	Terminating Call Screening
TDR	Time Dependent Routing
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TMF	Tele Management Forum
TMSI	Temporary Mobile Station Identity
UAC	User Agent Client
UAS	User Gent Server
UDR	User-Defined Routing
UE	User Equipment
UICC	USIM Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
UPSF	User Profile Server Function
UPT	Universal Personal Telecommunications
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIM	Universal Subscriber ID Module
USS	User Security Settings
UTRAN	Universal Terrestrial Radio Access Network
UUID	Universally Unique Identifier
VAS	Value Added Services
VASP	VAS Provider
VBS	Voice Broadcast Service
VGCS	Voice Group Call Service
VLR	Visitor Location Register
VMSC	Visited Mobile Switching Center
VPN	Virtual Private Network
VPN	Virtual Private Network
VPLMN	Visited Public Land Mobile Network
WAG	WLAN Access Gateway
WAP	Wireless Application Protocol
W-LAN	Wireless Local Area Network
WSDL	Web Service Definition Language
XCAP	XML Configuration Access Protocol
XDM	XML Document Management
XDMS	XDM Server
XML	eXtensible Markup Language

4 Rationale for the Analysis of a Common User Model and of the Basic Structure of a Common Profile Storage Framework

This clause provides motivation for:

- the analysis of a common end-user model; and
- the analysis of a Common Profile Storage Framework.

All aspects are dealt with in two steps. The first step is the statement of motivating ideas corroborated by use cases and the second step is the formulation of required steps of investigation following from the motivation part.

4.1 Motivation - Use Cases

Motivating Statement 1: Characterizing an end-user versus a contract holder

Looking at 3GPP's data definitions in [2] it focuses on the subscription of services. It is organized into the following blocks:

- Definition of subscriber data for CS and PS domain:
  - Data related to subscription, identification and numbering.
  - Data related to Mobile Station types.
  - Data related to authentication and ciphering.
  - Data related to roaming.
  - Data related to basic services.
  - Data related to supplementary services.
  - Mobile station status data.
  - Data related to Operator Determined Barring.
  - Data related to handover.
  - Data related to short message support.
  - Data related to subscriber trace.
  - Data related to the support of voice group and broadcast calls.
  - Data related to GPRS NAM.
  - Data related to CAMEL.
  - Data related to IST.
  - Data related to Location Services.
  - Data related to Super-Charger.
  - Data related to bearer service priority.
  - Data related to charging.

- Definition of subscriber data for IP Multimedia domain:
  - Data related to subscription, identification and numbering.
  - Data related to registration.
  - Data related to authentication and ciphering.
  - Data related S-CSCF selection information.
  - Data related to Application and service triggers.
  - Data related to Core Network Services Authorization.
  - Data related to Charging.
  - Data related to CAMEL Support of IMS Services.

In [2] these data are not organized into any specific structure. It is [5], which standardizes 3GPP's view of the interdependencies between the data entities defined in [2]. The root entity is the IMSI, which characterizes a subscriber as can be seen in the following figure1 in the non-GPRS case:

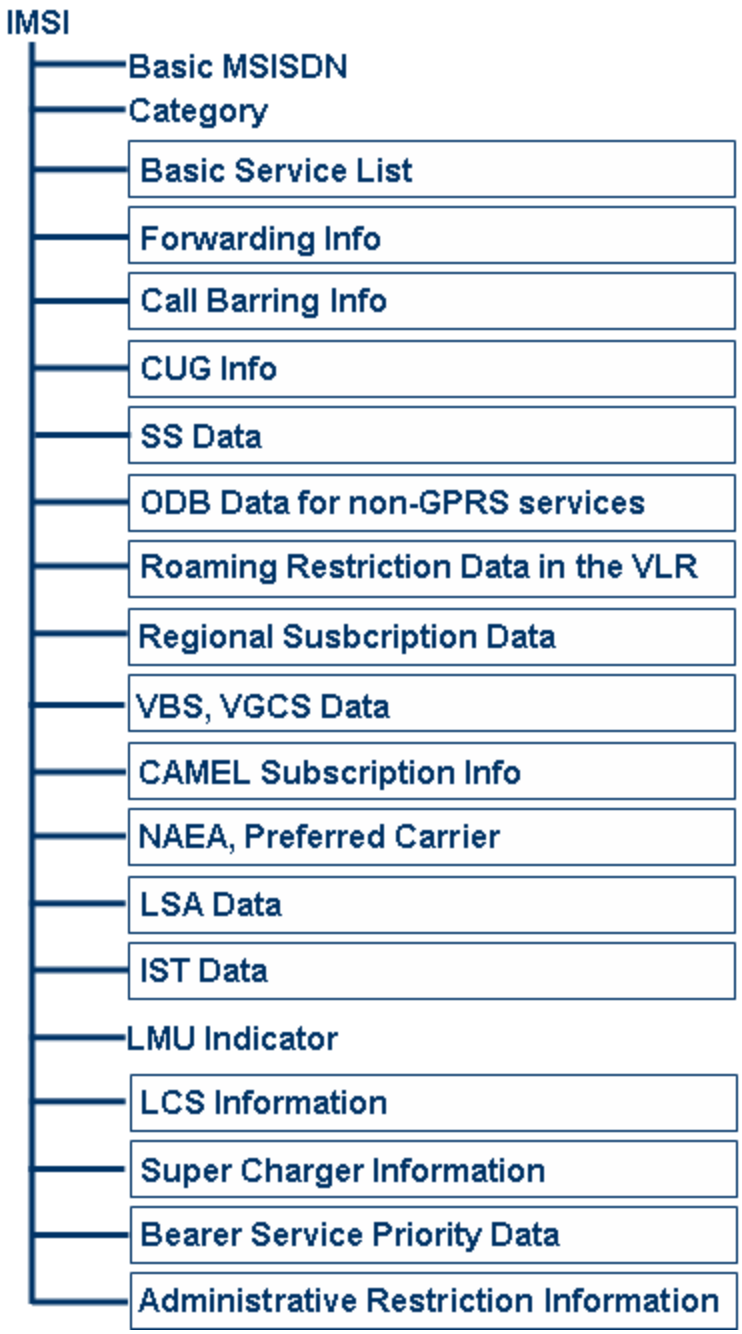


Figure 4.1.1: Organization of subscriber data in the non-GPRS case according to [5]

In the GPRS case, 3GPP defines the following structure [5].

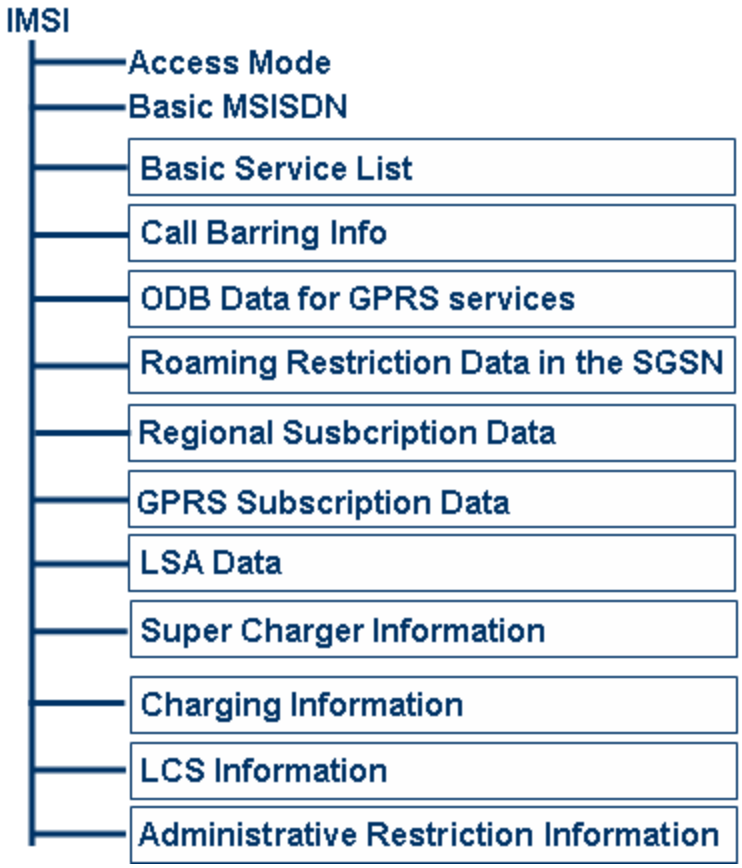


Figure 4.1.2: Organization of subscriber data in the GPRS case according to [5]

In both cases (non-GPRS and GPRS) the IMSI is the root for all further data concerning the properties of subscribed services.

In order to describe the end user as opposed to a subscriber 3GPP provides a model in the SuM specification [7].

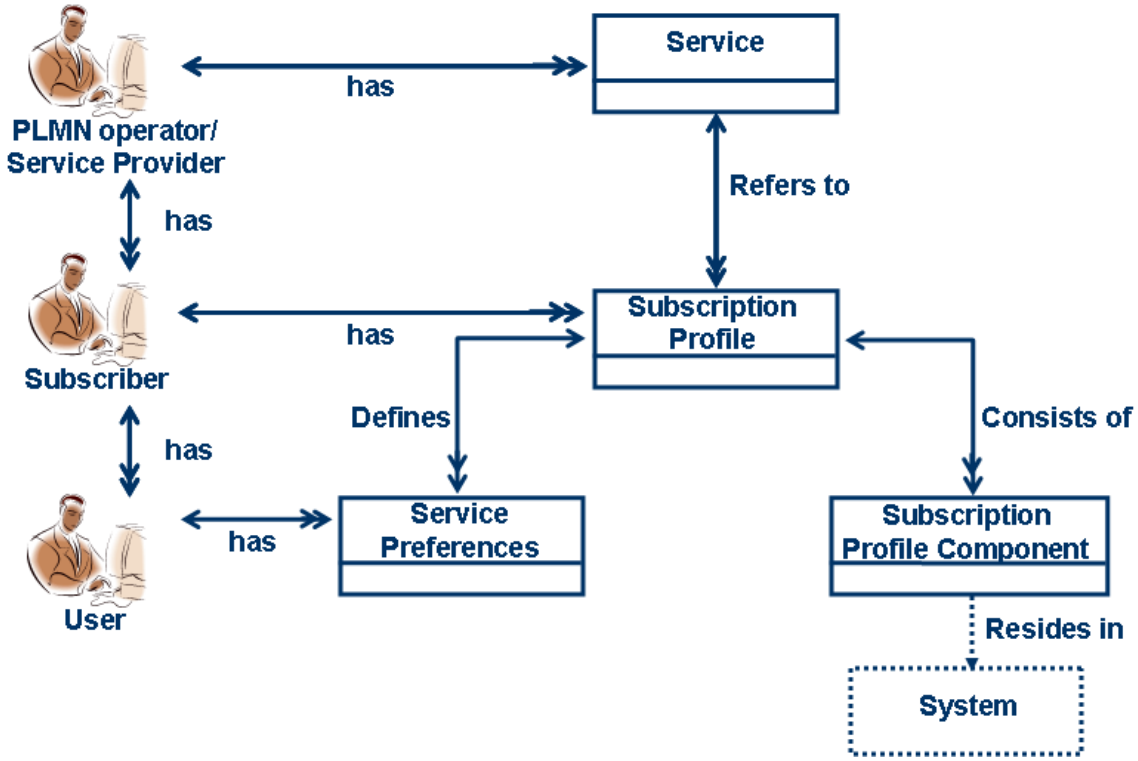


Figure 4.1.3: Organization of SuM data according to [7]

The user, in the present document also called "end user", is defined in 3GPP [1]: **User:** *An entity, not part of the 3GPP System, which uses 3GPP System services. Example: a person using a 3GPP System mobile station as a portable telephone.*

There is no further definition of a user within 3GPP. The following use case represents a class of use cases, where one person is assigned more than one IMSI from the same operator, which can, at the moment not be reflected in a data model according to [2].

Use Case 1: End user possesses a business cellular and a private cellular from the same provider

The business phone is provided to the end user by the company he/she works for. As it is used frequently and many supplementary services are subscribed to, the SIM card (i.e. the IMSI) and indirectly thus also the user is assigned a very high rating for customer service.

The private cellular is subscribed to by the end user himself, using as little additive services as possible, selecting the cheapest possible tariff. In this case the SIM card (i.e. the IMSI) and indirectly thus also the user is assigned a very low rating for customer service.

This situation is not satisfying for the end user, who receives different treatment from the same provider depending on the SIM card he uses. It is also not very satisfying for the provider, who would like to avoid this situation, if he only could link the two subscribers to the same end user.

Motivating statement 2

A user may have several devices (User Equipment, UE) each equipped with a UICC, UICC can even be exchanged between devices. On each UICC a USIM and several ISIM may be present. The information of co-located USIM and ISIM is not present in any current 3GPP register.

Use case 2

A network operator wants to provide users of his network combined services spanning CS, PS and IMS. For this knowledge about the user's UEs and his identities in the mentioned domains is needed, i.e. IMSIs (CS/PS) and Private Identities (IMS).

Motivating statement 3

A user using services under different subscriptions with multiple devices can not be handled as one end-user as no correlations exist between his MSISDNs and his Public Identities. Public user identities may be shared across multiple Private User Identities within the same IMS subscription. Hence, a particular Public User Identity may be simultaneously registered from multiple UEs that use different Private User Identities and different contact addresses.

Use case 3

A network operator wants to provide users of his network combined services spanning CS, PS and IMS. For this knowledge about the user's UEs and his identities in the mentioned domains is needed, i.e. MSISDNs (CS/PS) and Public Identities (IMS).

Motivating Statement 4: Avoiding inconsistent subscriber/end-user databases

Looking at a fraction of 3GPP's network architecture [13] in figure 4.1.4.

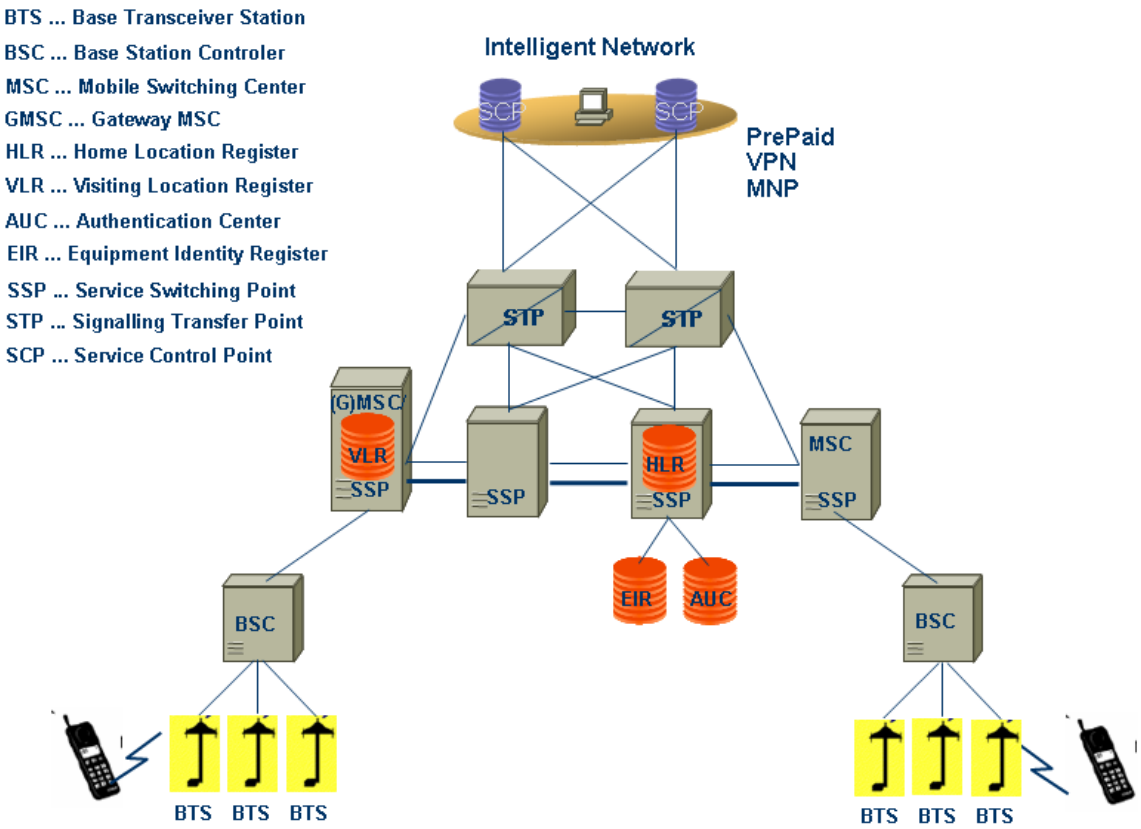


Figure 4.1.4: Part of the architecture of a 3GPP network according to [13]

it should be noted that data about one and the same end user are stored in the HLR, AuC, EIR, VLR and the SCP. Some of them (e.g. in the HLR, VLR and SCP) are necessary for a correct call processing and thus need to be kept consistent all the time.

Use Case 4: End user makes use of an IN service, which allows setting call forwarding numbers

An end user is member of an IN based VPN and uses the property "follow me", which allows him/her to be reached within the VPN at different locations. The MSISDNs configured in the SCP as "follow me" numbers could at the same time be blocked in the HLR by ODB, which would lead to the situation that the IN service "follow me" could never be used. So considerable effort has to be spent, in order to keep the two data bases synchronized.

Motivating Statement 5: High complexity in end user life cycle management

Identifying an end user has several implications:

- It provides the possibility of extending the existence of the user within the database after his/her card has been deleted. Information like preferences could thus be kept and in case of renewing the end-user's subscription, these preferences could automatically be used again.
- It may facilitate end user self management as it is easier for a vendor/provider to implement single sign on solutions
- It also leads to some obligations:
  - Openness:
    - Means for establishing the existence and nature of personal data.
    - Main purpose of the use of the data.
  - Collection Limitation:
    - Limits to collection of personal data.
    - Acquisition by lawful and fair means (evtl. with knowledge and/or consent of data subject).
  - Purpose specification:
    - Purpose, for which the data are collected, must be known latest at the moment of the beginning of the data collection.
    - Use of the data shall be limited to the fulfilment of those purposes.
  - Limitation of data usage:
    - Non-disclosure of personal data.
    - Use limited to purpose negotiated (subject to mutually agreed change requests).

Use Case 5

According to [46], technical identities simply are numbers, which can represent any object; they may identify directly or indirectly an individual, an organization, or a machine.

From the privacy perspective one should note [46] that even if those identifiers do not directly represent an individual, but only a specific device, frequently there is a relation to a person so that many of these identities have to be regarded as at least potentially personal data. But as the existence and the disclosure of those IDs often goes unnoticed by the users, managing them is quite difficult: In many cases technology does not provide the functionality to influence assignment, storage and disclosure of those IDs.

Motivating Statement 6: High data redundancy

Many of the end user data, which are necessary for call setup, can be found duplicated in the involved network elements. Using the network scenario in figure 4.1.4 and 3GGP's [5] as a reference, the following use case shows the existing data redundancy concerning the HLR, VLR and SGSN.

Use Case 6: End user data common to HLR and VLR (SGSN)

The VLR and SGSN store only a subset of the subscriber data available in the HLR. Updating of subscriber information shall be done in a way to make available and to keep consistency of data shared between the HLR and the VLR, and between the HLR and the SGSN as appropriate.

Two different cases for the updating of subscriber data can be identified:

- framed operation: during location update or restoration a complete set of the shared subscriber data needs to be inserted in the VLR or the SGSN;

- stand-alone operation: whenever subscriber data are added, deleted or changed in the HLR, this may need partial insertion, deletion or change of shared subscriber data in the VLR or the SGSN.

According to [5] the following groups of non-GPRS subscriber information are defined:

- Subscriber information (Group A):
  - International Mobile Subscriber Identity (IMSI);
  - basic Mobile Station International ISDN Number (MSISDN);
  - category;
  - subscriber status;
  - LMU identifier (GSM only).
- Basic service information (Group B):
  - Bearer Service list;
  - Teleservice list.
- Supplementary Service (SS) information (Group C):
  - forwarding information including deflection information;
  - call barring information;
  - Closed User Group (CUG) information;
  - eMLPP data;
  - MC data;
  - SS Data.
- Operator Determined Barring (ODB) information (Group D):
  - ODB Data for non-GPRS services;
- Roaming restriction information (Group E):
  - roaming restriction due to unsupported feature.
- Regional subscription information (Group F):
  - regional subscription data.
- VBS/VGCS subscription information (Group G):
  - VBS subscription data;
  - VGCS subscription data.
- CAMEL subscription information (Group H):
  - Originating CAMEL Subscription Information (O-CSI);
  - Dialled Service CAMEL Subscription Information (D-CSI);
  - VMSC Terminating CAMEL Subscription Information (VT-CSI);
  - Supplementary Service Invocation Notification CAMEL Subscription Information (SS-CSI);
  - Translation Information Flag CAMEL Subscription Information (TIF-CSI);
  - Mobile Originating Short Message Service CAMEL Subscription Information (MO-SMS-CSI);

  - Mobile Terminating Short Message Service CAMEL Subscription Information (MT-SMS-CSI);
  - Mobility Management Event Notification CAMEL Subscription Information (M-CSI).
- LSA Information (Group I):
  - LSA data.
- Super-Charger (SC) Information (Group K):
  - Age Indicator.
- Location Services (LCS) information (Group X):
  - GMLC List;
  - LCS Privacy Exception List;
  - MO-LR List;
  - LCS Service Types.
- IST Information (Group J):
  - IST data.
- Bearer Service Priority Information (Group L):
  - Bearer Service Priority Data.
- Administrative Restriction Information (Group M):
  - Access Restriction Data.

The following groups of GPRS subscriber information are defined:

- Subscriber information (Group P1):
  - International Mobile Subscriber Identity (IMSI);
  - basic Mobile Station International ISDN Number (MSISDN);
  - subscriber status.
- Basic service information (Group P2):
  - Teleservice list.
- Operator Determined Barring (ODB) information (Group P3):
  - ODB Data for GPRS services.
- Roaming restriction information (Group P4):
  - roaming restriction in SGSN due to unsupported feature.
- Regional subscription information (Group P5):
  - regional subscription data.
- GPRS subscription information (Group P6):
  - GPRS subscription data.

- SGSN CAMEL subscription information (Group P7):
  - GPRS CAMEL subscription information;
  - Mobile Originating Short Message Service CAMEL Subscription Information (MO-SMS-CSI);
  - Mobile Terminating Short Message Service CAMEL Subscription Information (MT-SMS-CSI);
  - Mobility Management Event for GPRS Notification CAMEL Subscription Information (MG-CSI).
- LSA Information (Group P8):
  - LSA data.
- Super-Charger (SC) Information (Group P9):
  - Age Indicator.
- Charging Information (Group P10):
  - Subscribed Charging Characteristics.
- Location Services (LCS) information (Group P11):
  - GMLC List;
  - LCS Privacy Exception List;
  - MO-LR List;
  - LCS Service Types.
- Administrative Restriction Information (Group P12):
  - Access Restriction Data.

These data are located both in the HLR and in the VLR or SGSN. They are transferred from the HLR according to the following rules defined in [5]:

The following rules shall apply for non-GPRS subscriber data for the order of information within an HLR-VLR dialogue:

- Group A information (subscriber status) shall be sent first;
- Group B information shall be sent after Group A information and before any Group C, E, F, G, H, J, L, M or X information;
- Group D information shall be sent after Group A information and in any order with respect to Group B, C, E, F, G, H, J, K, L, M and X information.

The following rules shall apply for GPRS subscriber data for the order of information within a dialogue:

- Group P1 information (subscriber status) shall be sent first;
- Group P2 information shall be sent after P1 information and before P4 and P5 information;
- Group P3 information shall be sent after Group P1 information and in any order with respect to Group P2, P4, P5, P6, P7, P8, P11 and P12 information.

Motivating Statement 7: NEs providing end user oriented services (e.g. HLR) need to be highly available

Each of the network elements of a 3GPP conformant network containing a subscriber database needs to be highly available. Otherwise the functionality provided by this network element is not available for the end users stored in its database.

Use Case 7: End user data stored within the HLR

At the moment the IMSI, which is the key identity of a subscriber, is bound to a specific HLR. Procedures like a location update or a mobile terminating call for one specific subscriber can only function, if the HLR in question is known and functioning.

Motivating Statement 8: Alternative possibilities of retrieving end-user data in comparison to using today's SS7 protocol stacks, allowing for a simpler handling of data queries within an operator's domain.

Some of the end user data can be queried via the SS7 protocol stack. Typical examples are the Anytime Interrogation (ATI) and the Anytime Modification (ATM) provided by MAP. This interface is highly complicated and requests like ATM and ATI create a certain load on the call processing part of the network. The following two use cases just show what may be possible, there would be others (e.g. an MMSC has to send multiple requests to get the necessary end-user data).

Use Case 8: MAP and SCP

Today the SCP of IN systems uses the MAP interface for Any Time Interrogation and Any Time Modification for the reading and/or modification of e.g. Call Forwarding Information.

Use Case 9: MAP and MNP

Today Mobile Number Portability (MNP) needs more than one step towards the acquisition of the final routing information. A central subscriber profile store would allow the same result with one read access only.

Motivating Statement 9: Not all information stored within an end-user store can be retrieved.

Some of the end user data are stored for purposes of the respective network element of a 3GPP network, which would be very welcome for other network functions, but cannot be retrieved from there.

Use Case 10: Location Information stored in the VLR

Within the VLR, amongst other information LAC information is stored. This information would be very welcome to e.g. presence services and/or management applications, but at the moment it cannot be retrieved without implementing - e.g. in the GSM case - a MAP interface.

4.2 Resulting required steps of investigation

Required step of investigation 1:

Following motivating statement 1 and motivating statement 7 the end user, as described in [7], has to be introduced formally into the data model [2] and its relations to a subscriber have to be formalized.

Required step of investigation 2:

Following motivating statement 1 all services provided by a 3GPP based network, which can be assigned to an end user should also be capable of being retrieved by identifying this end user within the database

Required step of investigation 3:

Following motivating statement 4 and motivating statement 6, it should be investigated if it is possible to identify data with identical semantic context and store these in one database only (an example would be call forwarding number, which are stored in the HLR as well as in the SCP)..

Required step of investigation 4:

Following problem statement 5, the identity defined by the characteristics of an end user has to be managed according to legal obligations. The following list highlights some of them:

The following legal acts just represent examples:

- Europe: The main legal sources of the protection of individual identity are
  - Constitutions;
  - International Treaties:
    - Treaties of the European Union;
    - European Convention for the Protection of Human Rights and Fundamental Freedoms;
    - European Directives;
    - National Law;
    - Other national Regulations.
- The aspects of human personality that are protected by the above mentioned legal sources are:
  - One's name and the identity;
  - Freedom from physical constriction (habeas corpus);
  - Inviolability of the domicile and right of privacy;
  - Freedom of speech and self expression, in particular:
    - The right to choose one's image;
    - The right to protect one's honour;
  - Freedom of movement and to settle (granted only to fully aged people).
- One of the important European Directives is:
  - The European Directive 95/46/CE: deals with data protection, is aimed at giving to the data subject (owner of data) the most control possible on its own identity and personal data, posing a series of requirements on recipients, controllers, processors and even third parties. Art. 2, letter a), giving a definition of "personal data", says: "identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".
  - The main principles behind the Data Protection Directive are:
    - Personal data must always be processed fairly and lawfully;
    - Personal data must be collected for explicit and legitimate purposes and used accordingly;
    - Personal data must be relevant and not excessive in relation to the purpose for which they are processed;
    - Data that identify individuals must not be kept longer than necessary;
    - Data must be accurate and, where necessary, kept up to date;
    - Data controllers are required to provide reasonable measures for data subjects to rectify, erase or block incorrect data about them;
    - Appropriate technical and organizational measures should be taken against unauthorized or unlawful processing of personal data;

- Personal data must not be transferred to a country or territory outside the European Economic Area unless that country ensures an "adequate level of protection" for data subjects.

- USA:

  - Privacy Act of 1974: all government agencies - federal, state and local - which request social security numbers are required to provide a disclosure statement on the form;

  - Family Educational Rights and Privacy Act (FERPA, also known as the "Buckley Amendment," enacted in 1974, 20 USC 1232g): social security numbers fall within the scope of personally identifiable information that is restricted from disclosure by schools that receive federal funding under the Family Educational Rights and Privacy Act;

  - Children's Online Privacy Protection Act (COPPA) - 15 U.S. Code 6501 et seq.: The act's goal is to place parents in control over what information is collected from their children online;

  - Financial Services Modernization Act, Gramm-Leach-Bliley (GLB), Privacy Rule - 15 USC 6801-6827: The 1999 federal law permits the consolidation of financial services companies and requires financial institutions to issue privacy notices to their customers, giving them the opportunity to opt-out of some sharing of personally identifiable financial information with outside companies;

  - Telephone Consumer Protection Act (TCPA) - 47 U.S. Code 227: This law puts restrictions on telemarketing calls and on the use of autodialers, pre-recorded messages, and fax machines to send unsolicited advertisements.

Required step of investigation 5:

Following motivating statement 7, motivating statement 8 and motivating statement 9, the possibility of NEs being made end-user dataless and putting these end user data into a common end user storage facility should be investigated.

Use case 10 leads to the question, whether it makes sense to perhaps only store the VLR data within a CPSF, if it turns out that the VLR is not one of the NEs, which lends itself to user dataless operation.

Required step of investigation 6:

Following use case 8, possibilities to migrate to a less complex signalling network topology should be investigated.

Required step of investigation 7:

According to use cases 2 and 3 a correlation of the UEs used by an end-user and his identities in the CS, PS and IMS domains has to be established.

NOTE: All required steps of investigation have to lead to findings, which are backwards compatible to today's 3GPP network scenarios.

5 Considerations on a Common User Model

This clause has multiple intentions concerning considerations on a common user model.

At the beginning, in clause 5.1, a classification of subscriber/end-user data is given. This clause mainly serves the purpose of showing, what roles the services related to subscriber/end-user data might play and for which kind of services to expect subscriber/end-user data. In addition the realization of these services within a network and the location of the respective end user data within the network are shown. The specific structure of this clause is only of limited importance for the subsequent analysis of the properties of a common user model.

Clause 5.2 lists all relevant standards pertaining to subscriber/end-user data for the network functions treated in clause 5.2 within and outside of 3GPP.

Clause 5.3 highlights some of the current difficulties when handling subscriber/end-user data in more detail.

Finally clause 5.4 deals with the important points to consider, when putting together a common end-user data model.

5.1 Network Functions and Management Applications Using Subscriber/User Data

In this clause the network functions/services as well as enterprise applications, which make up a 3GPP conformant network, or which could be put onto a 3GPP conformant network and which use or house end-user/subscriber data are listed and classified.

Two types of functions/services using end-user/subscriber data can be distinguished:

- Network functions: These network functions can be found within the 3GPP's, OMA's, IETF's, etc., network architectures.
- Enterprise applications: These can be found within the OSS/BSS environment of a network/service provider.

Clause 5.1 groups the network functions according to the type of service, they provide or at least support.

The rest of this clause is devoted to an overview of the standardized network scenarios including those network elements, which use or store subscriber data.

5.1.1 Network Supporting Services

5.1.1.1 UMTS, CS and PS Network Supporting Services

5.1.1.1.1 Location Register

[13] describes, how communication to a mobile station is supported by the network. The information where this mobile station is located is stored in a function named "location register".

According to [13] the location register is handled by four different entities.

- The Home Location Register (HLR): register to which a mobile subscriber is assigned for record purposes such as subscriber information.
- The Visitor Location Register (VLR): register for Circuit Switched (CS) services, other than the HLR, used by an MSC to retrieve information for, e.g. handling of calls to or from a roaming mobile station currently located in its area.
- The Serving GPRS Support Node (SGSN): register function in the SGSN storing subscription information and location information for Packet Switched (PS) services for each subscriber registered in the SGSN (needed only in a PLMN which supports GPRS).
- The Gateway GPRS Support Node (GGSN): register function in the GGSN storing subscription information and routeing information (needed to tunnel packet data traffic destined for a GPRS MS to the SGSN where the MS is registered) for each subscriber for which the GGSN has at least one PDP context active (needed only in a PLMN which supports GPRS).

A basic configuration of a PLMN for UMTS is given in [13]. The following figures show the configurations of the mobile network in the GSM, GPRS and UMTS case.

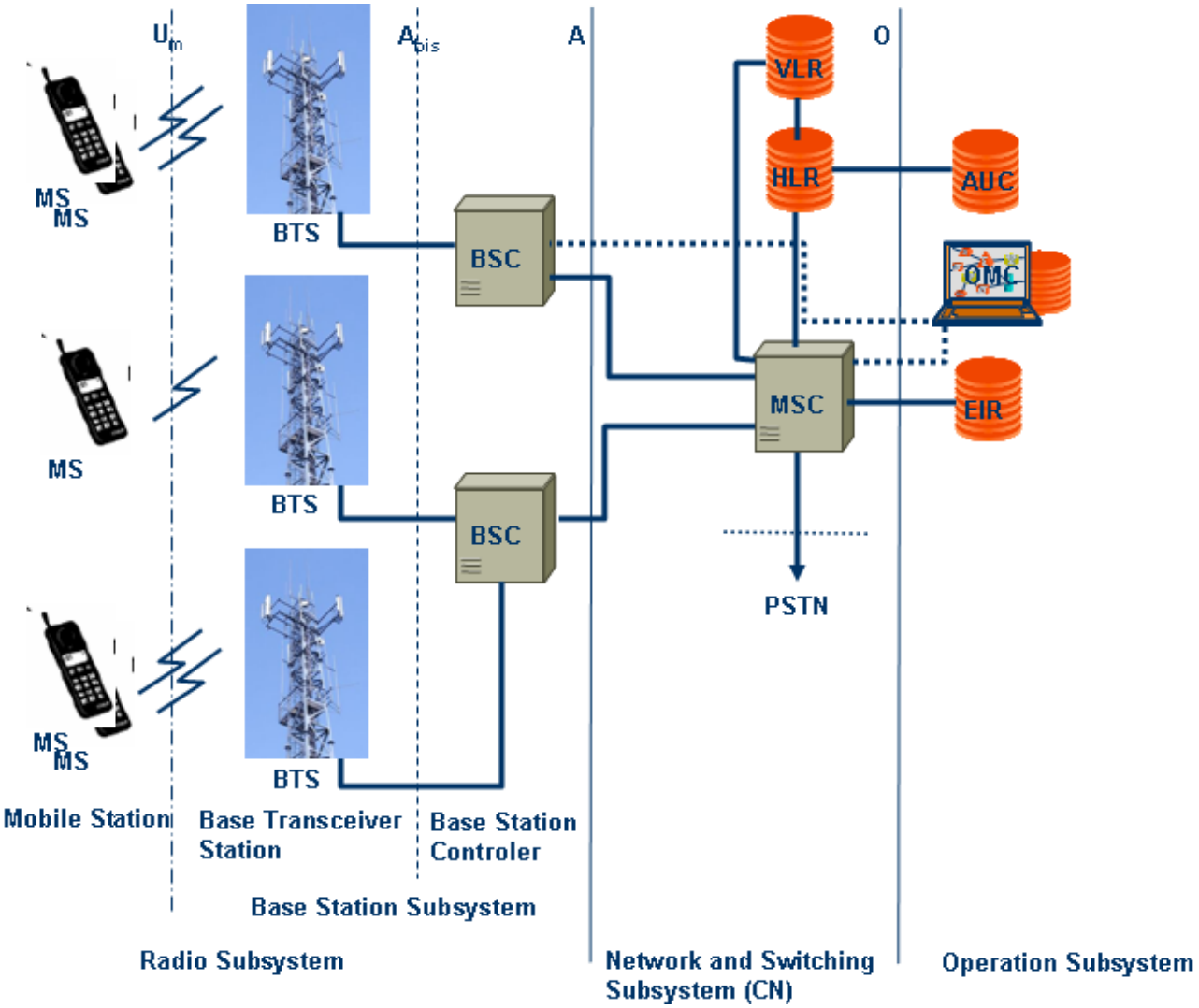


Figure 5.1.1.1.1: Basic Configuration of a GSM PLMN supporting CS services and interfaces

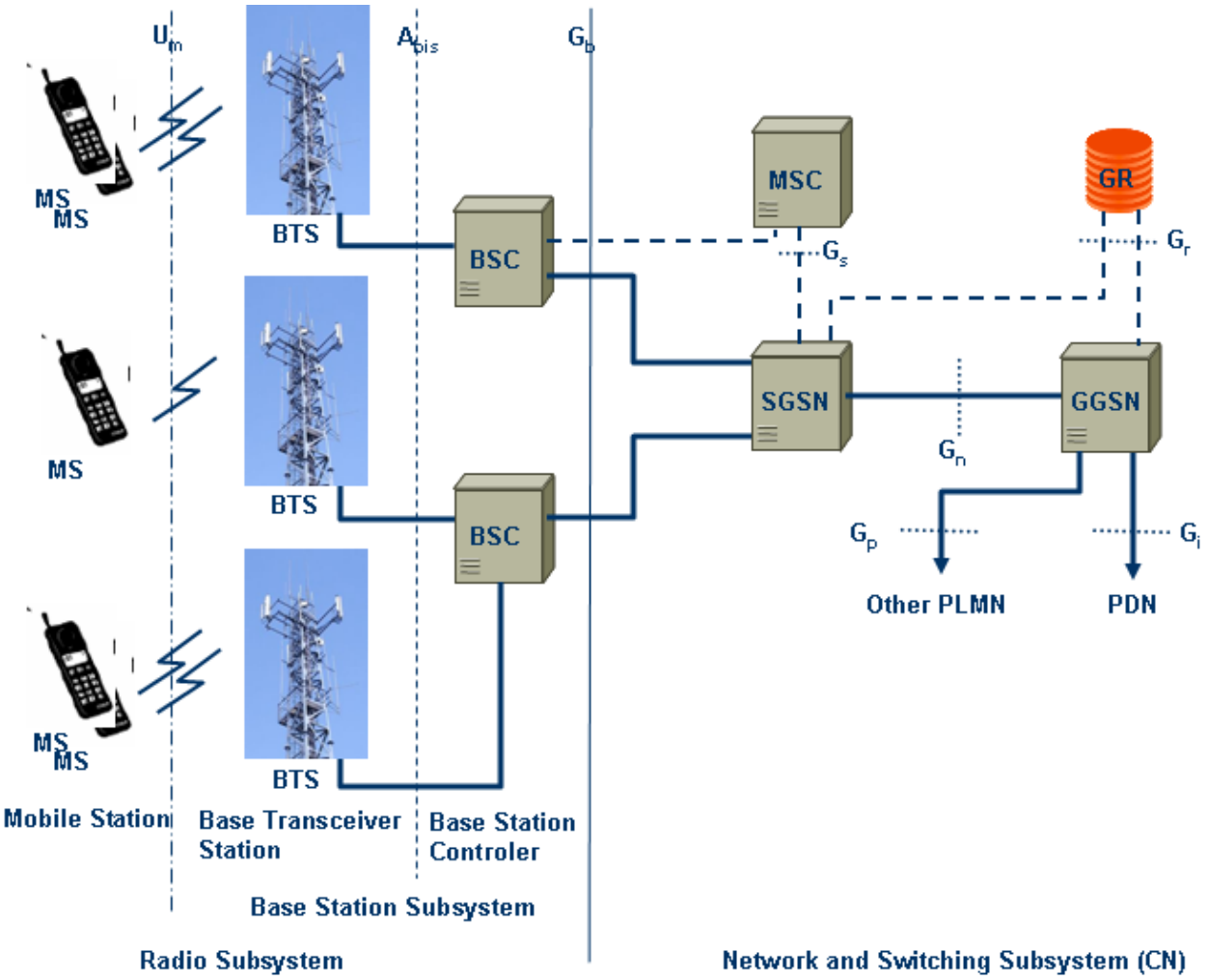


Figure 5.1.1.1.2: Basic Configuration of a GPRS PLMN supporting PS services and interfaces

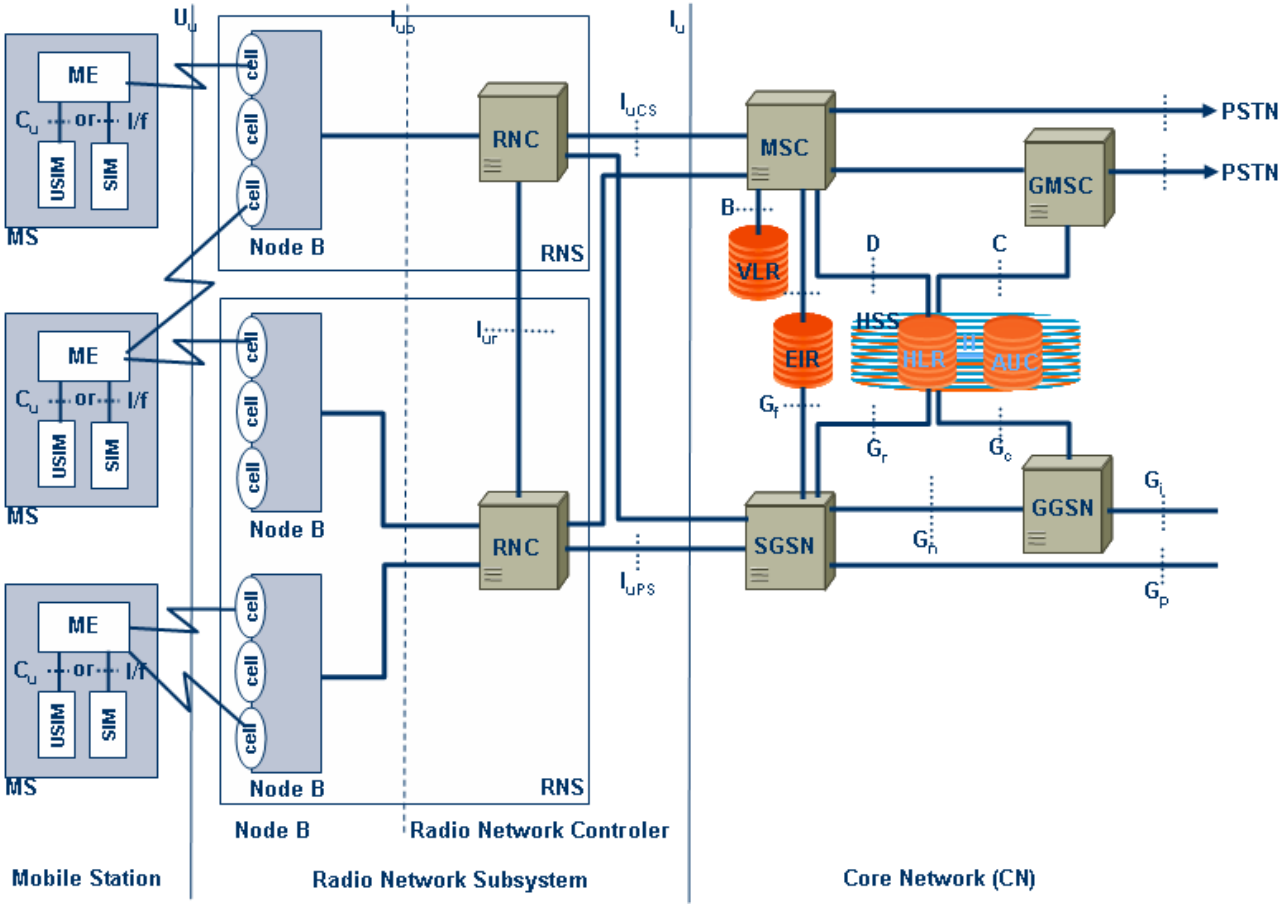


Figure 5.1.1.1.3: Basic Configuration of a UMTS PLMN supporting CS and PS services and interfaces [13]

The HSS (see figure 5.1.1.1.3) is the master database for a given user. It is the entity containing the subscription-related information to support the network entities actually handling calls/sessions.

The HSS houses the following user related information:

- User Identification, Numbering and addressing information.
- User Security information: Network access control information for authentication and authorization.
- User Location information at inter-system level: the HSS supports the user registration, and stores inter-system location information, etc.
- User profile information.

According to [13] the HSS has the following functions:

- IP multimedia functionality to provide support to control functions of the IM subsystem. It enables subscriber usage of the IM CN subsystem services.
- The subset of the HLR/AUC functionality required by the PS Domain.
- The subset of the HLR/AUC functionality required by the CS Domain, if it is desired to enable subscriber access to the CS Domain or to support roaming to legacy GSM/UMTS CS Domain networks.

Thus the HSS is a realization of parts of the location register functionality mentioned above.

The VLR contains the information needed to handle the calls set-up or received by the MSs registered in its data base including the following elements:

- the International Mobile Subscriber Identity (IMSI);
- the Mobile Station International ISDN number (MSISDN);
- the Mobile Station Roaming Number (MSRN),
- the Temporary Mobile Station Identity (TMSI), if applicable;
- the Local Mobile Station Identity (LMSI), if used;
- the location area where the mobile station has been registered;
- the identity of the SGSN where the MS has been registered. (applicable to PLMNs supporting GPRS and a Gs interface between MSC/VLR and SGSN);
- the last known location and the initial location of the MS.

The VLR also contains supplementary service parameters attached to the mobile subscriber and received from the HLR. The organization of the subscriber data is outlined in 3GPP TS 23.008 [2].

The location register function in the SGSN contains:

- subscription information:
  - the IMSI;
  - one or more temporary identities;
  - zero or more PDP addresses.
- location information:
  - depending on the operating mode of the MS, the cell or the routeing area where the MS is registered;
  - the VLR number of the associated VLR (if the Gs interface is implemented);
  - the GGSN address of each GGSN for which an active PDP context exists.

The organization of the subscriber data in the SGSN is defined in [2] and [17].

The location register function in the GGS stores subscriber data received from the HLR and the SGSN in order to be able to handle originating and terminating packet data transfer:

- subscription information:
  - the IMSI;
  - zero or more PDP addresses.
- location information:
  - the SGSN address for the SGSN where the MS is registered.

The organization of the subscriber data in the GGSN is defined in [2] and [17].

5.1.1.1.2 The Equipment Identity Register (EIR)

The EIR is part of the GSM system, responsible for storing in the network the International Mobile Equipment Identities (IMEIs), which may be classified as "white listed", "grey listed" and "black listed" and therefore may be stored in three separate lists.

5.1.1.1.3 The Mobile-services Switching Centre (MSC) Server (Media Control)

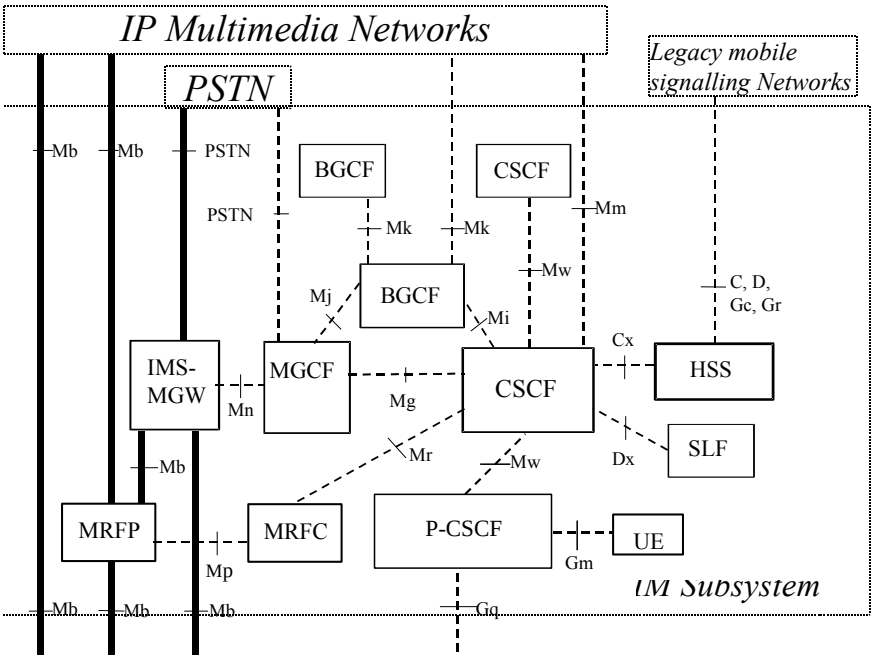
The MSC is the interface between the radio system and the fixed networks handling the circuit switched services to and from the mobile stations. The MSC Server mainly comprises the Call Control (CC) and mobility control parts of a MSC. To this end it also contains a VLR to hold the mobile subscriber's service data and CAMEL related data.

The MSC Server controls the parts of the call state that pertain to connection control for media channels in a CS-MGW (thus the name Media Control).

5.1.1.2 IP Multimedia Subsystem (IMS) Network Supporting Services

The configuration of IP Multimedia Subsystem Core Network Subsystem entities is presented in figure 5.1.1.2.1. In the figure, all the functions are considered implemented in different logical nodes. If two logical nodes are implemented in the same physical equipment, the relevant interfaces may become internal to that equipment. More information on the functions can be found from 3GPP TS 32.002 [13].

Only the interfaces specifically linked to the IM subsystem are shown.



Legend:
Bold lines: interfaces supporting user traffic;
Dashed lines: interfaces supporting only signalling.

Figure 5.1.1.2.1: Configuration of IM Subsystem entities

Figure 5.1.1.2.2 depicts an overall view of the functional architecture for services.

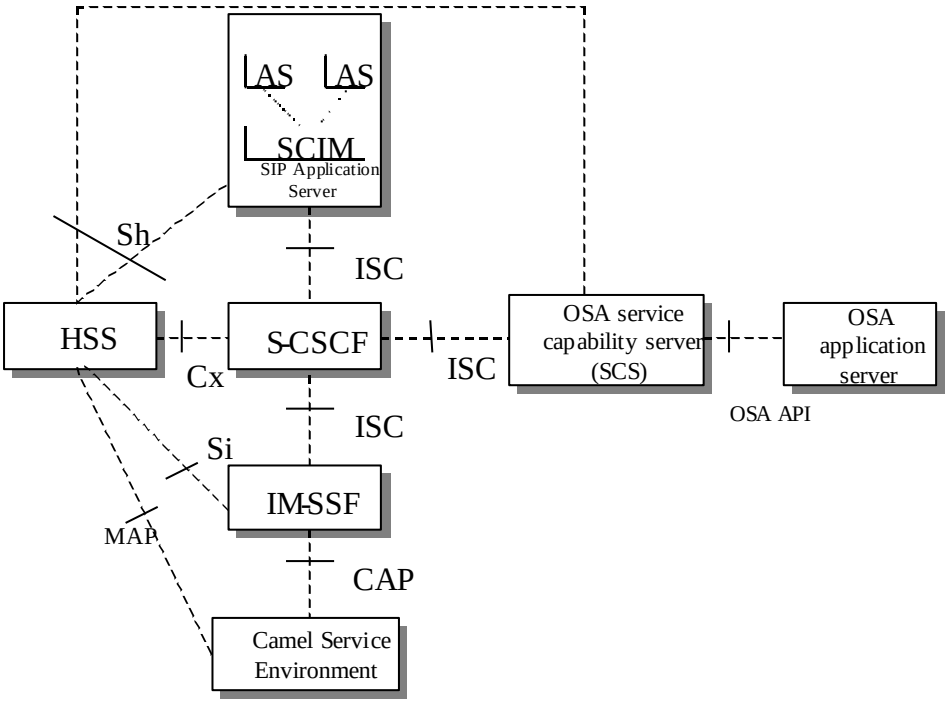


Figure 5.1.1.2.2: Functional architecture for the provision of service in the IMS

The Subscription Locator Function (SLF), the Serving Call Session Control Function (S-CSCF), the Application Server (AS) and the IM-SSF are relevant when considering where user data in existing networks is stored. More information on IMS subscriber data and where it is stored can be found in 3GPP TS 23.008 [2].

5.1.1.3 I-WLAN

3GPP/WLAN Interworking entities as defined in [13] and depicted in figure 5.1.1.3.1 (also taken from [13]):

- WLAN UE: A WLAN UE is the User Equipment using a UICC card utilized by a 3GPP subscriber to access the WLAN network for 3GPP interworking purpose.
- 3GPP AAA Proxy: The 3GPP AAA Proxy represents a AAA proxying and filtering function and resides in the visited 3GPP network. It is involved in access and service authentication and authorization procedures of a WLAN UE.
- 3GPP AAA Server: The 3GPP AAA server resides in the 3GPP network and is responsible for access and service authentication and authorization of a WLAN UE.
- WLAN Access Gateway (WAG): The WLAN access gateway is a gateway between WLAN and 3GPP network. In the roaming case it resides in the visited 3GPP network, otherwise in the home 3GPP network. It provides filtering, policing and charging functionality for the traffic between WLAN UE and 3GPP network.
- Packet Data Gateway (PDG): The Packet Data Gateway provides access to PS based services for a WLAN UE. It resides either in the home (for access to home services) or in the visited 3GPP network (for access to local services).

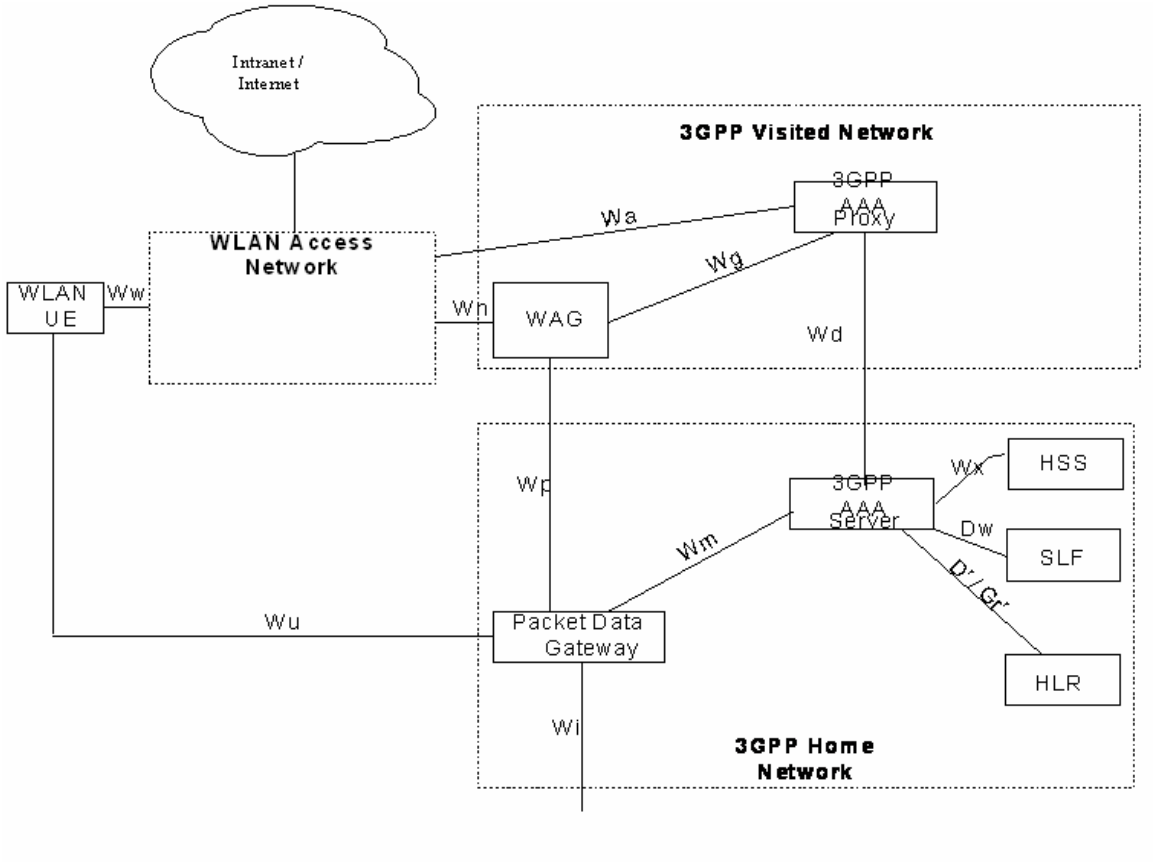


Figure 5.1.1.3.1

According to [2], the following subscription related data are defined for I-WLAN:

- Data related to subscription, identification and numbering:
  - IMSI: The International Mobile Subscriber Identity (IMSI) serves as the root of the subscriber data pseudo-tree.
  - Mobile Subscriber ISDN Number (MSISDN): One MSISDN is used for WLAN-IW subscription. If the multinumbering option applies, the MSISDN used is the Basic MSISDN.
  - W-APN: The WLAN Access Point Name (W-APN) identifies a data network and a point of interconnection to that network (Packet Data Gateway). The APN is composed of two parts as follows:
    - The APN Network Identifier: this defines to which external network the GGSN is connected and optionally a requested service by the MS. This part of the APN is mandatory.
    - The APN Operator Identifier; this defines in which PLMN GPRS backbone the GGSN is located. This part of the APN is optional.
    - The APN Operator Identifier is placed after the APN Network Identifier. An APN consisting of both the Network Identifier and Operator Identifier corresponds to a DNS name of a GGSN; the APN has, after encoding as defined in the paragraph below, a maximum length of 100 octets.
  - List of authorized visited network identifiers: The list of authorized visited network identifiers field indicates which 3GPP visited network identifiers are allowed for roaming.
  - 3GPP AAA Proxy Name: The 3GPP AAA Proxy Name defines the Diameter or RADIUS Identity of the 3GPP AAA Proxy node.
  - 3GPP AAA Server Name: The 3GPP AAA Server Name defines the Diameter or RADIUS Identity of the 3GPP AAA Server node.

- Serving PDG List: The Serving PDG List field contains the addresses of the PDGs to which the WLAN UE is connected.
- Serving WAG: The Serving WAG field contains the WAG address information obtained through the successful user authentication procedure.
- WLAN UE Local IP Address: The WLAN UE Local IP Address field represents the IPv4/IPv6 address of the WLAN UE in the WLAN AN. It is an address used to deliver the packet to a WLAN UE in a WLAN AN.
- WLAN UE Remote IP Address: The WLAN UE Remote IP Address field represents the IPv4/IPv6 address of the WLAN UE in the network which the WLAN UE is accessing. It is an address used in the data packet encapsulated by the WLAN UE-initiated tunnel and is the source address used by applications in the WLAN UE. The WLAN UE Remote IP address is per W-APN.

- Data related to registration:
  - User Status: The User Status field identifies the registration status of the I-WLAN User. The User Status shall be either REGISTERED, in which case there is an associated Serving 3GPP AAA Server Name stored at the HSS, or UNREGISTERED, in which case no 3GPP AAA Server Name stored.
- Data related to authentication and ciphering:
  - Random Number (RAND), Signed Response (SRES) and Ciphering Key (Kc):
    - Random Number (RAND), Signed Response (SRES) and Ciphering Key (Kc) fields form a triplet vector used for authentication and encryption.
    - In I-WLAN for SIM based users, triplet vectors are calculated in the 2G AuC and provided to the 2G HLR/HSS. For USIM based users, triplet vectors are derived from quintuplet vectors in the 3G HLR/HSS if needed.
    - A set of up to 5 triplet values are sent from the 2G HLR/HSS to the 3GPP AAA Server upon request. These data are temporary subscriber data stored in the 3GPP AAA Server.
  - Random Challenge (RAND), Expected Response (XRES), Cipher Key (CK), Integrity Key (IK) and Authentication Token (AUTN):
    - Random Challenge (RAND), Expected Response (XRES), Cipher Key (CK), Integrity Key (IK) and Authentication Token (AUTN) fields form a quintuplet vector used for user authentication, data confidentiality and data integrity.
    - In I-WLAN, a set of quintuplet vectors are calculated in the AuC, and up to 5 quintuplets are sent from the HLR/HSS to the 3GPP AAA Server upon request.
    - These data are temporary subscriber data stored in the HSS and 3GPP AAA Server.
  - Master Key (MK) : The Master Key (MK) field enables keys to be derived.
  - Transient EAP Keys (TEKs): The Transient EAP Keys (TEKs) field is used to protect the EAP packets.
  - Master Session Key (MSK): The Master Session Key (MSK) field is used to obtain the key material required for the link layer confidentiality mechanism and IPsec confidentiality mechanism.
- Data related to session:
  - Session Identifier: The Session Identifier field indicates a unique Diameter signalling session specific to the user.
  - Session-Timeout: The Session-Timeout field indicates the maximum period for a session measured in seconds. It is used for re-authentication purposes. If this field does not appear, the WLAN AN shall apply default time intervals.
- Operator Determined Barring general data:

- W-APN Authorized List: The W-APN contains authorization information for each W-APN. This parameter indicates the list of allowed W-APNs, the environment where the access is allowed and optionally the charging data specific for that W-APN and the Static IP address.
  - W-APN Identifier List
  - W-APN Barring Type List: The W-APN Barring Type field indicates the subscriber access type to the home and visited network's services. The parameter takes either of the following values:
    - Allow access to this W-APN regardless of whether the subscriber is located in a VPLMN or in the HPLMN;
    - Prohibit access to this W-APN within the HPLMN when the subscriber is located in a VPLMN;
    - Prohibit access to this W-APN within the VPLMN when the subscriber is located in a VPLMN;
    - Prohibit access to this W-APN within the HPLMN when the subscriber is located in the HPLMN.
  - W-APN Charging Data List: When this parameter is present, it supersedes the general charging information to be applied for the subscriber.
  - Static WLAN UE Remote IP Address List: WLAN UE IP Address field identifies the IPv4/IPv6 address that the operator has statically assigned to the WLAN UE.
  - Maximum Number of Accesses List: The Maximum Number of Accesses enables operators to specify the maximum number of concurrent accesses per W-APN.
  - Access Number List: Access Number is an integer counter kept at the 3GPP AAA Server per W-APN.
- Access Dependence Flag: The Access Dependence Flag enables operators to authenticate a subscriber accessing the I-WLAN by WLAN 3GPP IP Access independently of a previous WLAN 3GPP Direct WLAN Access. The parameter takes either of the following values:
  - Allow access to WLAN 3GPP IP Access independently of a previous WLAN 3GPP Direct Access.
  - Prohibit access to WLAN 3GPP IP Access independently of a previous WLAN 3GPP Direct Access.
- I-WLAN Access Type: The I-WLAN Access Type field indicates the types of access the subscriber has used to access to the IWLAN. The parameter takes either of the following values:
  - WLAN 3GPP IP Access;
  - WLAN 3GPP Direct Access.

- QoS general data
  - Max Subscribed Bandwidth: The Max Subscribed Bandwidth field indicates the Max subscribed bandwidth.
  - Routing Policy: The Routing Policy field defines a packet filter for an IP flow.
- Data related to Charging
  - Charging Data: The Charging Data field identifies the Charging Characteristics plus the Charging Nodes to be applied per user for all W-APNs or per user for individual W-APNs.
  - Charging Characteristics: The Charging Characteristics field indicates the charging type to be applied to the user tunnel.
  - Primary OCS Charging Function Name: The Primary OCS Charging Function Name field identifies the Primary OCS Function node that performs on-line based charging.
  - Secondary OCS Charging Function Name: The Secondary OCS Charging Function Name field identifies the Secondary OCS Charging Function node that performs on-line based charging.

- Primary Charging Collection Function Name: The Primary Charging Collection Function Name field identifies the primary Charging Collection Function node that provides off-line charging support for the IMS subscribers.
- Secondary Charging Collection Function Name: The Secondary Charging Collection Function Name field identifies the secondary Charging Collection Function node that provides off-line charging support for the IMS subscribers.

5.1.2 Enabling Services

5.1.2.1 Presence Service

5.1.2.1.1 IETF

In [39] IETF describes the Presence Service facilities as accepting information, storing it, and distributing it. Architecturally it has two distinct sets of "clients":

- Presentities: provide presence information to be stored and distributed.
- Watchers: receive presence information from the service.

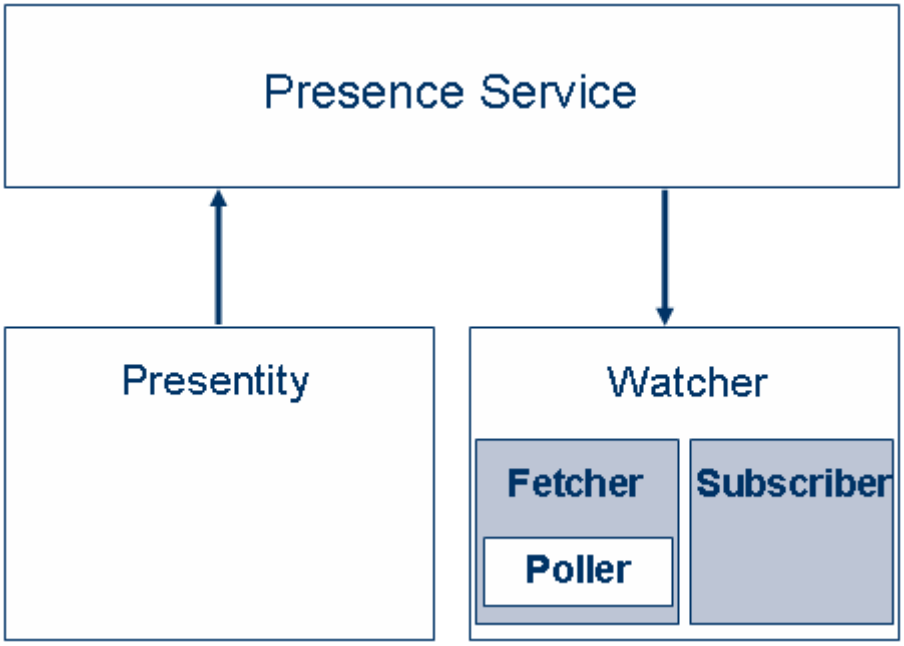


Figure 5.1.2.1.1.1: Overview over presence service support defined by IETF [39]

There are two kinds of Watchers:

- Fetchers: requests the current value of some Presentity's presence information from the Presence Service. A special kind of Fetcher (the Poller) is one that fetches information on a regular basis.
- Subscribers: requests notifications from the Presence Service of changes in some Presentity's presence information.

IETF's model for Presence Information consists of an arbitrary number of elements, called "presence tuples". Each such element consists of:

- a status marker: (e.g. online/offline/busy/away/do not disturb);
- a communication address: optional (containing communication means and communication address);
- other presence mark-up: optional.

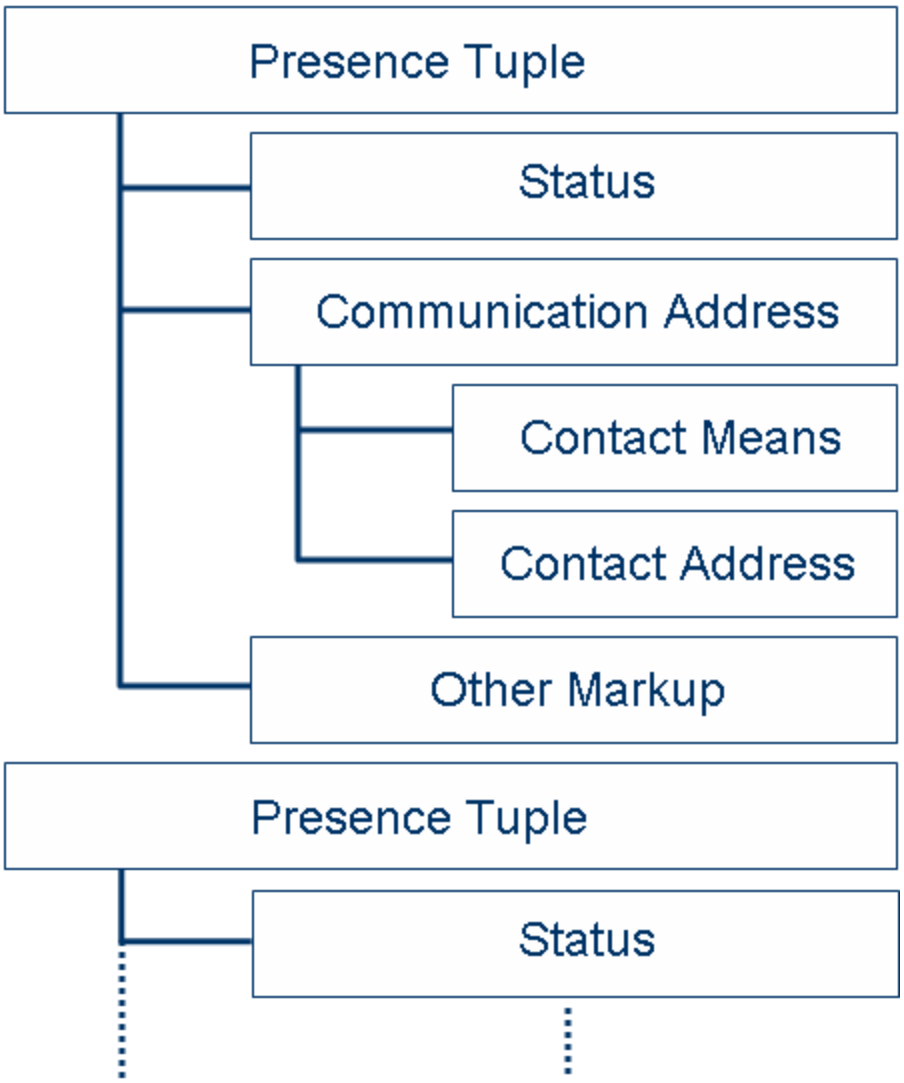


Figure 5.1.2.1.1.2: Overview over presence information defined by IETF [39]

The IETF model includes additional elements that are useful in characterizing how the protocol and mark-up work:

- Principals: people, groups, and/or software in the "real world" outside the system using the system as a means of coordination and communication.

A Principal interacts with the system via one of several user agents:

- INBOX USER AGENT.
- SENDER USER AGENT.
- PRESENCE USER AGENT.
- WATCHER USER AGENT.

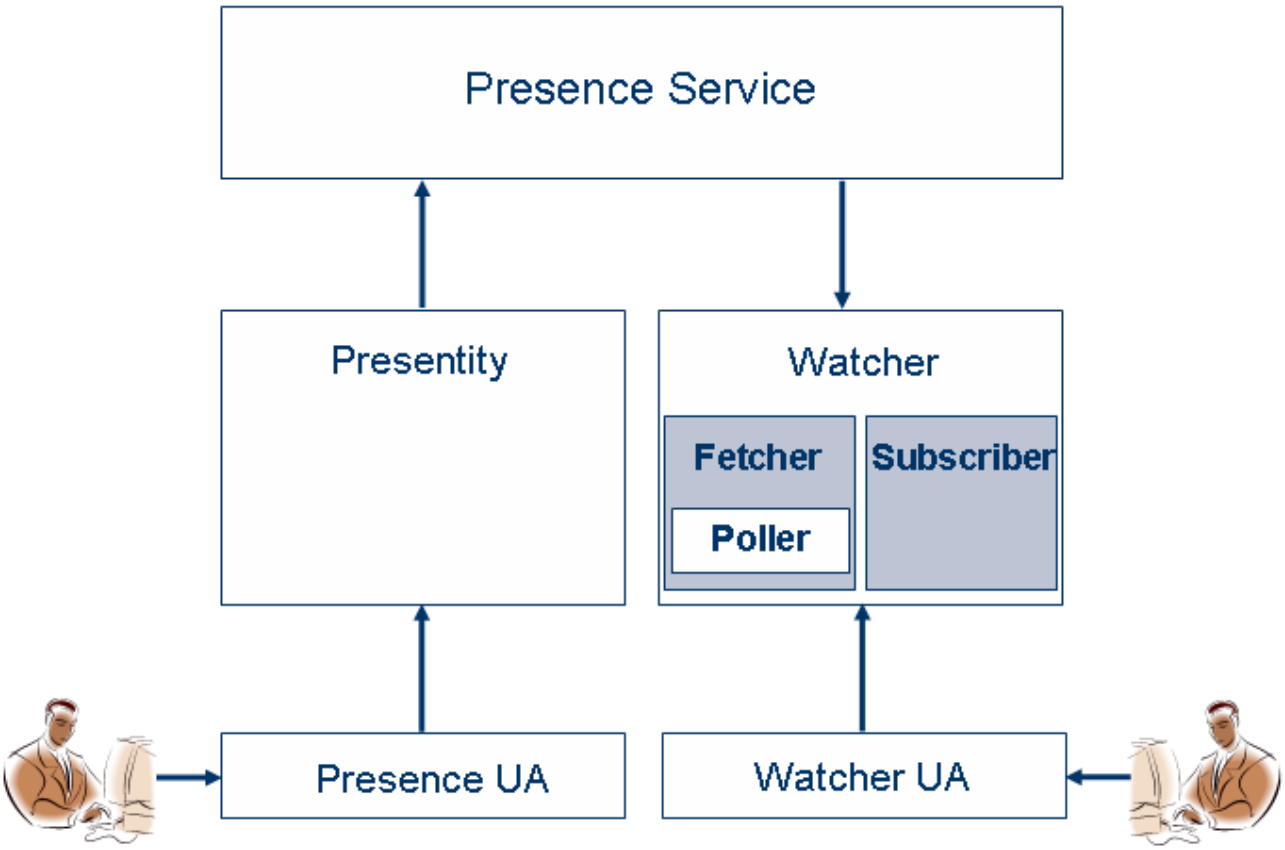


Figure 5.1.2.1.1.3: Overview over presence system defined by IETF [39]

Information Model of [39]:

- Access Rules: constraints on how a presence service makes presence information available to Watchers. For each presentity's presence information, the applicable Access Rules are manipulated by the Presence User Agent of a Principal that controls the Presentity.
- Communication Address: consists of
  - Communication Means: indicates a method whereby communication can take place (e.g. instant message service).
  - Contact Address: a specific point of contact via some Communication Means (e.g. for an instant message service it is the instant inbox address).
- Fetcher: a form of Watcher that has asked the Presence Service to for the Presence Information of one or more Presentities, but no Subscription to be created.
- Notification: a message sent from the Presence Service to a Subscriber when there is a change in the Presence Information of some Presentity of interest, as recorded in one or more Subscriptions.
- Other Presence Markup: any additional information included in the Presence Information of a Presentity [39] does not define this further.
- Poller: a Fetcher that requests Presence Information on a regular basis.
- Presence Information: consists of one or more Presence Tuples.
- Presence Service: accepts, stores, and distributes Presence Information:
  - May require authentication of Presentities, and/or Watchers.
  - May have different authentication requirements for different Presentities.

- May have different authentication requirements for different Watchers, and may also have different authentication requirements for different Presentities being watched by a single Watcher.
- May have an internal structure involving multiple servers and/or proxies. There may be complex patterns of redirection and/or proxying while retaining logical connectivity to a single Presence Service.
- The service may be implemented as direct communication among Presentity and Watchers.
- May have an internal structure involving other Presence Services, which may be independently accessible in their own right as well as being reachable through the initial Presence Service.

- Presence Tuple: consists of a Status, an optional Communication Address, and optional Other Presence Markup.
- Presence User Agent: means for a Principal to manipulate zero or more Presentities.
- Presentity (presence entity): provides Presence Information to a Presence Service.
- Note that the presentity is not (usually) located in the presence service: the presence service only has a recent version of the presentity's presence information. The presentity initiates changes in the presence information to be distributed by the presence service.
- Principal: human, program, or collection of humans and/or programs that chooses to appear to the Presence Service as a single actor, distinct from all other Principals.
- Proxy: a server that communicates Presence Information, subscriptions and/or notifications to another server. Sometimes a Proxy acts on behalf of a Presentity or a Watcher.
- Server: an indivisible unit of a Presence Service.
- Status: a distinguished part of the Presence Information of a Presentity. Status has at least the mutually-exclusive values OPEN and CLOSED. There may be other values of Status that may be combined with OPEN and CLOSED or they may be mutually-exclusive with those values.
- Subscriber: a form of Watcher that has asked the Presence Service to notify it immediately of changes in the Presence Information of one or more Presentities.
- Subscription: the information kept by the Presence Service about a Subscriber 's request to be notified of changes in the Presence Information of one or more Presentities.
- Visibility Rules: constraints on how a Presence Service makes Watcher Information available to Watchers. For each Watcher 's Watcher Information, the applicable Visibility Rules are manipulated by the Watcher User Agent of a Principal that controls the Watcher.
- Watcher: requests Presence Information about a Presentity, or Watcher Information about a Watcher, from the Presence Service. Special types of Watcher are Fetcher, Poller, and Subscriber.
- Watcher Information: information about Watchers that have received Presence Information about a particular Presentity within a particular recent span of time. Watcher Information is maintained by the Presence Service, which may choose to present it in the same form as Presence Information.
- Watcher User Agent: means for a Principal to manipulate zero or more Watchers controlled by that Principal.

5.1.2.1.2 3GPP

The Presence Service for GSM and GPRS [21] provides the ability for the home network to manage presence information of a user's device, service or service media even whilst roaming. A user's presence information may be obtained through input from the user, information supplied by network entities or information supplied by elements external to the home network. Consumers of presence information, watchers, may be internal or external to the home network.

The principal architecture of the 3GPP presence service is summarized in figure 5.1.2.1.2.1.

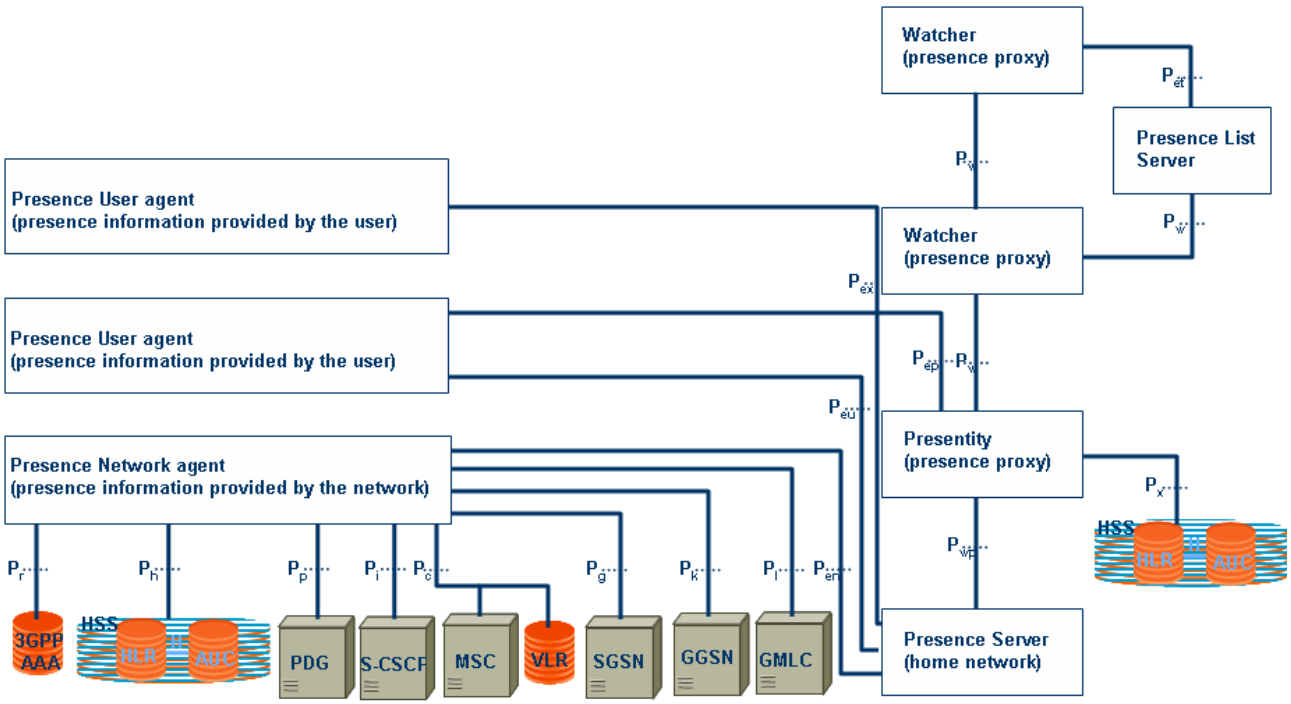


Figure 5.1.2.1.2.1: Reference Architecture for Presence service support defined by 3GPP [21]

[21] describes a 3GPP subscriber by the following attributes: *subscriber's status, communication means status, one or more communication address(es)* (containing *communication means* and *contact address*), *location (subscriber provided location and/or network provided location), priority, text.*

The attributes can be categorized as:

- communication means and contact address specific information: *communication means* status, communication means, contact address, priority and text; or
- generic information: subscriber's status, location and text.

In [21] these attributes are assigned the following values:

- Generic information attributes:
  - Subscriber's status (willing, willing with limitations, not willing, not disclosed).
  - The subscriber's status attribute is not intended to be used when interworking with IM clients. Subscribers are able to provide more detailed willingness information as well as other information through the generic Text attribute, and the communication means and contact address specific Text attribute.
  - Location (Last known CGI/SAI and/or geographic co-ordinates and/or free format text and timestamp).
  - Text (free format text).
- Communication means and contact address specific information attributes, if these attributes are used as part of any tuple they shall use following values (values in parenthesis) to enable interoperability:
  - communication means status (online, offline);
  - communication means (Service type (e.g. telephony, SMS, email, multimedia messaging service, instant messaging service));
  - contact address (E.164 (e.g. MSISDN), SIP URL, Email, Instant message address e.g. IM:name@domain name);

- priority (Priority order for each of the defined communication means and contact address);
- text (free format text).

5.1.2.1.3 *3GPP2*

The principal architecture of the 3GPP2 presence service is summarized in figure 5.1.2.1.3.1.

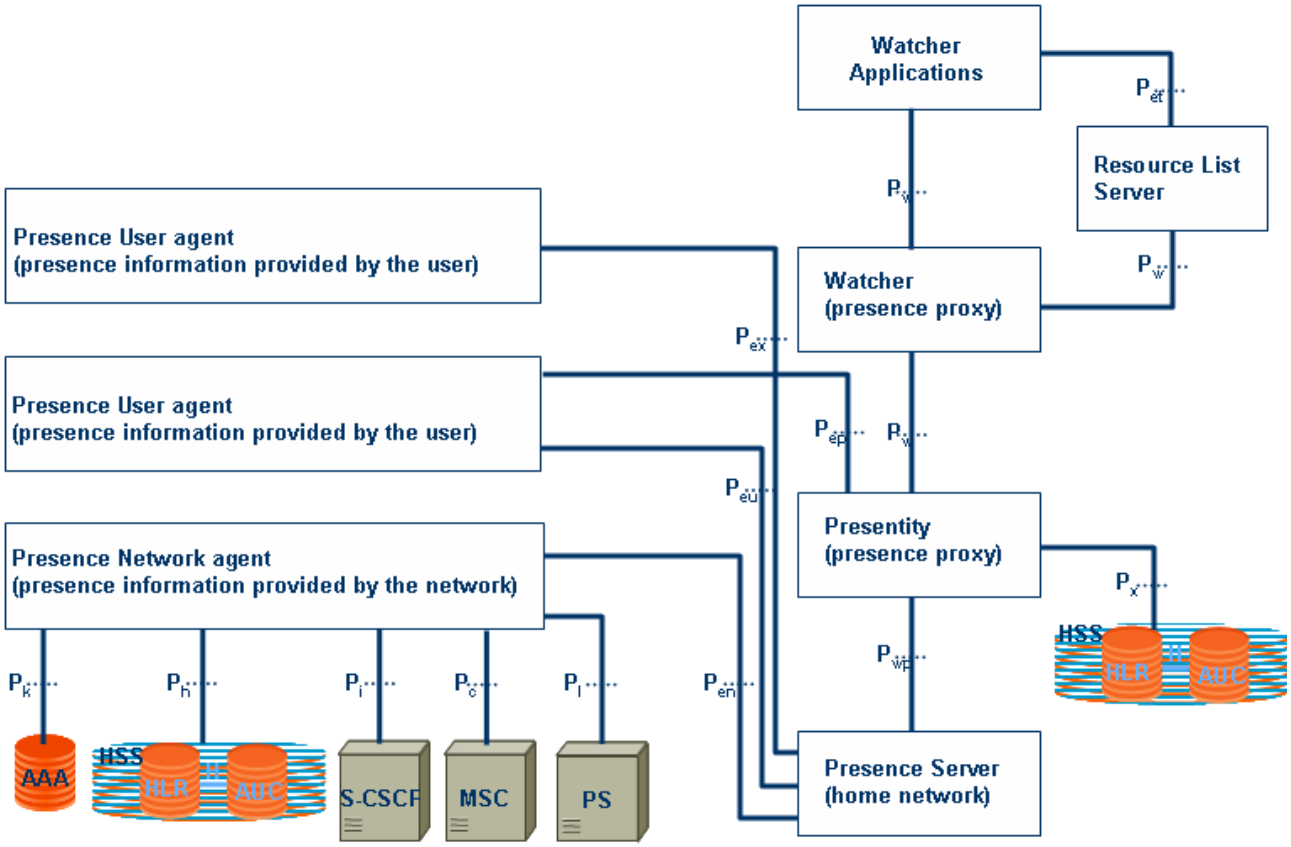


Figure 5.1.2.1.3.1: Reference Architecture for Presence service support defined by 3GPP2 [29]

[29] describes a 3GPP2 subscriber by the following attributes:

- subscriber's status;
- communication means status;
- one or more communication address(es) (containing communication means and contact address);
- location (subscriber provided location and/or network provided location);
- priority;
- text.

The only information element, which differs from 3GPP in the name is the element "contact information", from "communication means" , which replaces "contact address".

5.1.2.1.4 OMA

OMA's Presence Framework leverages IETF's protocols and formats for presence in its SIMPLE (SIP Instant Messaging and Presence Leveraging Extensions) activity (see RFC 3856 [101]).

3GPP [21] and 3GPP2 [29] have defined an aligned Presence Service framework both in the:

- "network layer": communication that is required between the Presence Service functional elements (e.g. Presence Server) and various network elements as they are defined in the network architectures of 3GPP and 3GPP2 (e.g. MSC, HLR); and

- "application layer": communication that is required between the various Presence Service elements (e.g. Presence Server and Presence Source), which includes the "application layer" functional entities;

defining end-to-end presence information flows.

In addition OMA's Presence Architecture supports presence services that do not leverage core network infrastructure as defined by 3GPP and 3GPP2, but which are still relevant to the mobile domain. The following picture shows the SIMPLE reference architecture on which it is based.

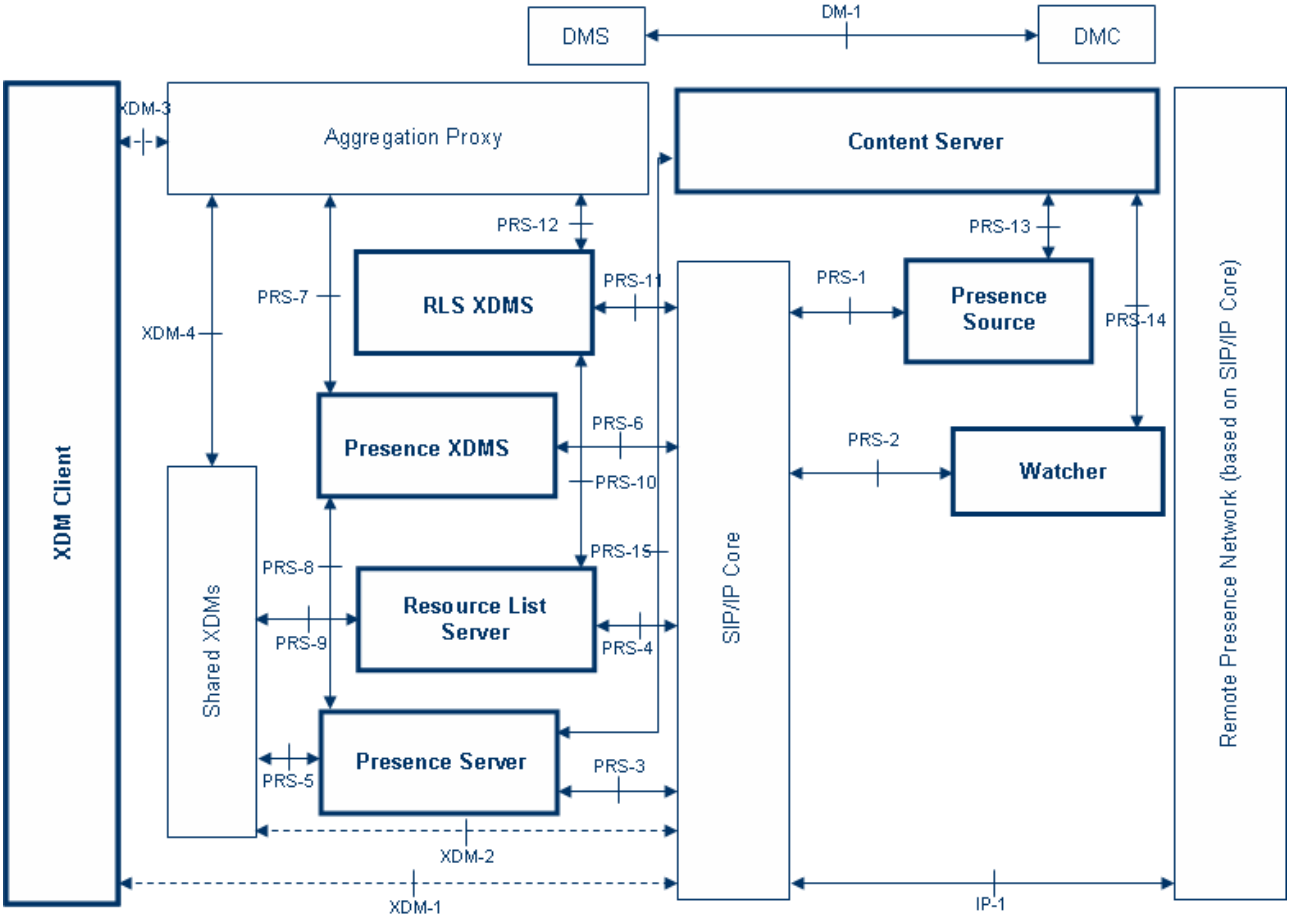


Figure 5.1.2.1.4.1: SIMPLE Reference Architecture for Presence service support based on IETF [31]

Presence Source

The Presence Source is an entity that provides presence information to a Presence Service [31]. It can be located in the user's terminal or within a network entity.

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, the Presence Source can be implemented in a UE or an AS as defined in 3GPP and 3GPP2 respectively.

The following figure shows an architecture for the PNA in the case that no 3GPP/3GPP2 network represents the core.

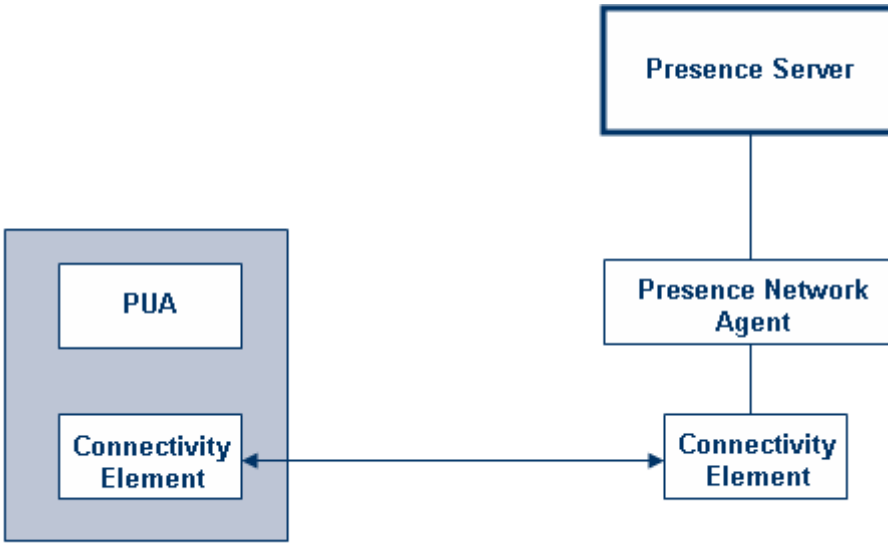


Figure 5.1.2.1.4.2: OMA Reference Architecture for Presence service support in a non-3GPP/3GPP2 case [30]

Watcher

The watcher is an entity that subscribes to presence information about a presentity or list of presentities (i.e. presence list) [30].

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, the watcher can be implemented in a UE or an AS as defined in 3GPP and 3GPP2.

Presence Server

The Presence Server (PS) is an entity that accepts, stores and distributes presence information. The PS performs the following functions:

- Handles publications from one or multiple Presence Source(s) of a certain presentity. This includes:
  - refreshing presence information;
  - replacing existing presence information with newly published information; or
  - removing presence information, for a given Presence Source.
- Composes the presence information received from one or multiple Presence Source(s) into a single presence document.
- Handles subscriptions from watchers to presence information and generates notifications about the presence information state changes.
- Handles subscriptions from watcher information subscribers to watcher information and generates notifications about the watcher information state changes.
- Authorizes the watcher's subscription to the presentity's presence information and applies policies.
- Applies the watcher's event notification filtering preferences, as appropriate.
- Applies rate control mechanisms to the notifications, as appropriate.

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, the PS is implemented in an AS as defined in 3GPP and 3GPP2 respectively.

Resource List Server

The Resource List Server (RLS) performs the following functions:

- Accepts subscriptions to presence lists.
- Authorizes the watcher's usage of the presence list.
- Creates and manages back-end subscriptions to all presentities in the presence list, on behalf of the watcher.
- Sends notifications to the watcher, based on information received from the back-end subscriptions.
- Applies aggregation and rate control mechanisms to the notifications, as appropriate.

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, the RLS has to be implemented in an AS as defined in 3GPP and 3GPP2 respectively.

XDM Client

The XDM Client has to support the XDM Client procedures and the XCAP application usages.

Presence XDMS

The Presence XDMS has to support the XDM Server procedures and the XCAP application usages.

RLS XDMS

The RLS XDMS has to support the XDM Server procedures and the XCAP application usages.

Content Server

The Content Server has to support IETF's HTTP GET and PUT methods [30], and the procedures defined in [30].

The Content Server has to store a MIME object when receiving it in an HTTP PUT request behind the HTTP URI therein.

The Content Server has to return a MIME object in a 200 OK response to an HTTP GET request. The Content Server has to fetch the MIME object from the Request URI of the HTTP GET request.

The Content Server can be used by Presence Sources, Watchers and the Presence Server as described in figure 5.1.2.1.4.

The Presence data model

The Presence Data Model defined by IETF (see above) is categorized in four key components: the Presentity URI, the Person, the Service and the Device:

- The Presentity's URI component indicating the Presentity's identifier (e.g. SIP URI, tel. URI)
- The Person components model the information about the Presentity: The "person" component models information about the Presentity whom the presence data is trying to describe. It has the following components:
  - Overriding Willingness.
  - Activity.
  - Location.
  - Time Zone.
  - Mood.
  - Icon.
  - Class.
  - Geographical Location (location info, usage rules).
  - Note.

- Timestamp.

  The model supports only one "person" component per presentity, or a group, which appears to the watcher as a single Presentity.

NOTE: According to [30] more than one "person" component instance may exist in the Presence document in cases where composition policy in the PS cannot clearly semantically differentiate between the multiple instances of the same component.

- The Service components model the forms of communication used by the Presentity and has potentially access to:
  - Application-specific Availability (registration state, barring state).
  - Application-specific willingness.
  - Icon.
  - Session Participation.
  - Service Description.
  - Class.
  - Per service device identifier (device-id).
  - Communication address (contact).
  - Timestamp.

    One important characteristic of each "service" might be the devices on which that service executes. Each device is uniquely identified by the device identifier <deviceID>. A service may contain zero or more <deviceID> elements to indicate which devices that service is available on. The Presence document may contain information on each device, but this is a separate part of the document modelled by the "device" component.

    The "service" component has to be mapped to the <tuple> element specified in [31].

- The Device components model the physical pieces of equipment used by the Presentity:
  - Network Availability.
  - Geographical Location (location-info, location-rules).
  - Device identifier (device-id).
  - Timestamp.

    Examples of Presence information that can be represented by "device" elements include mobile phones, PCs and PDAs.

    The mapping of services to devices is many to many. Devices are uniquely identified with a device identifier. The model supports only one "device" component per device identifier, however the Presence Sources publish their own "device" component instances. The PS composes the multiple instances into one component and resolves conflicts among the Presence Sources according to [30].

    The "device" component has to be mapped to the <device> element, which is specified in [31].

    For a given presentity, the value of the <deviceID> element of the <device> element have to be unique for each device used by the presentity.

    A version 4 UUID as defined in [30] has to be used for <deviceID> to uniquely identify the device. This is a purely random identifier, providing uniqueness. It is not allowed to change over the lifetime of the device and has to be stored in a non-volatile memory. It has to be used in all the Presence publications requiring the use of <deviceID>.

The relationship between the data elements is shown in figure 5.1.2.1.4.3.

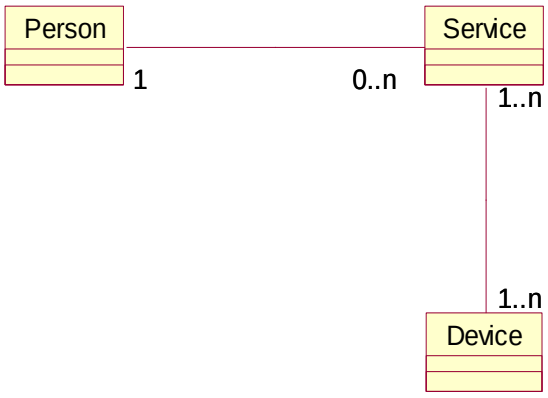


Figure 5.1.2.1.4.3: Presence Object Model defined by OMA [31]

5.1.2.2 Location Service

5.1.2.2.1 3GPP

The functional model defined in [18] and presented in figure 5.1.2.2.1.1 includes functional entities for both CS and PS related LCS. In addition, it consists of all the entities needed for different positioning methods:

- i.e. network based;
- mobile based;
- mobile assisted; and
- network assisted positioning, exploiting:
  - either uplink; or
  - downlink measurements.

NOTE: The UE may use e.g. the GPS positioning mechanism, but still demand e.g. auxiliary measurements from the serving network. RAN specific functional entities are specified in 3GPP TS 25.305 [19] for UTRAN and in 3GPP TS 43.059 [20] for GERAN.

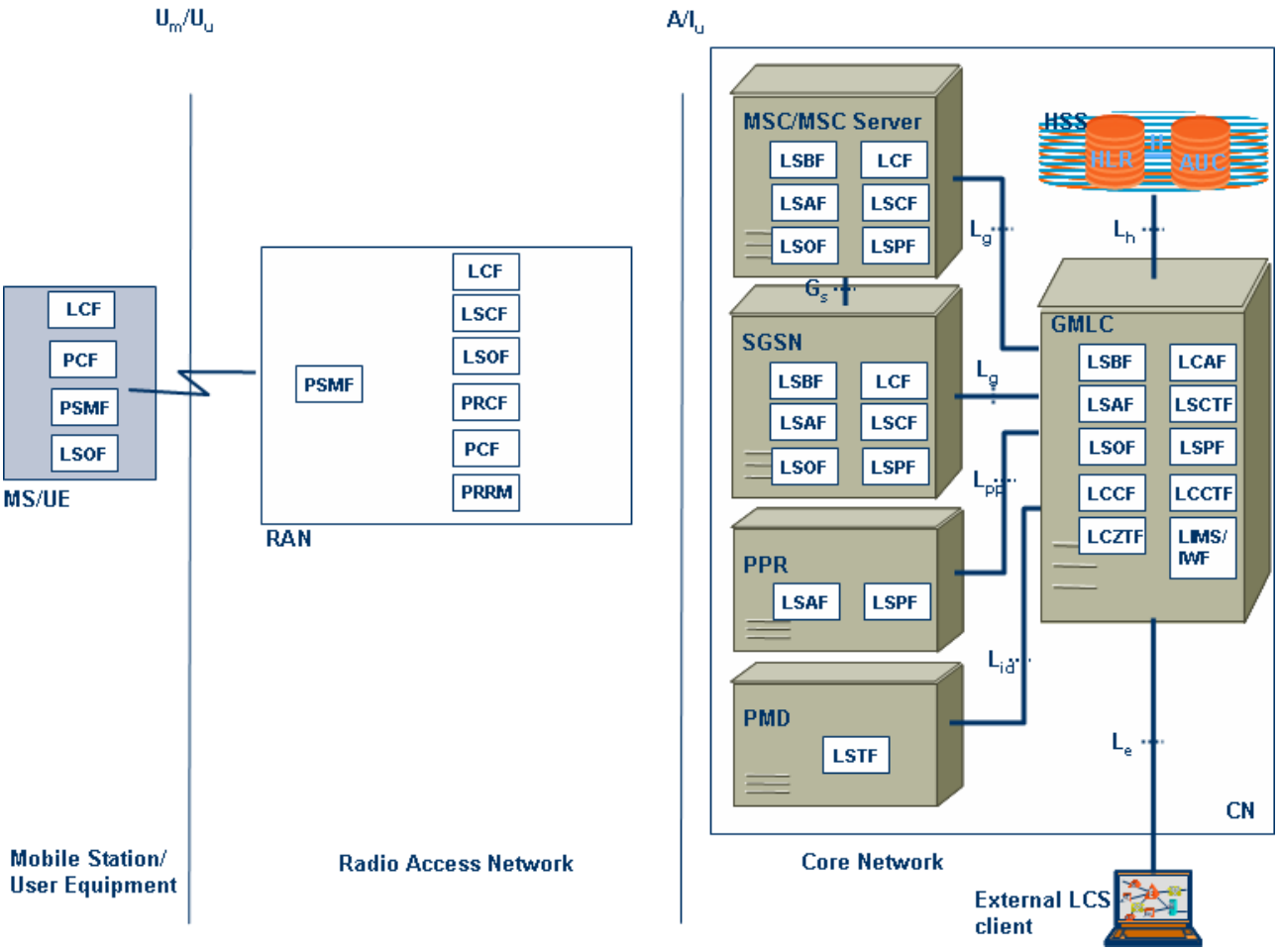


Figure 5.1.2.2.1.1: Generic Logical LCS Architecture defined by 3GPP [18]

The LCS client Subscription profile shall contain a minimum set of parameters assigned on per LCS client basis for an agreed contractual period. The LCS client profile shall contain the following set of access parameters:

- LCS client identity;
- allowed LCS request types (i.e. LIR, LDR or both) (see note);
- maximum number of subscribers allowed in a single LCS request;
- priority;
- position override indicator;
- state(s);
- event(s) (applicable to LDR requests only);
- local coordinate system;
- LCS client access barring list (optional);
- PLMN access barring list applicability.

5.1.2.2.2 OMA

For certain authorized LCS clients internal to the PLMN, a subscription profile is unnecessary. These clients are empowered to access any defined service that is not barred for an UE subscriber. This permits positioning of emergency calls without the need for pre-subscription.

The OMA Mobile Location Service V1.0 (MLS V1.0 [34]) consists of a set of location specifications complying with 3GPP Release 6 LCS Specification [18].

The Architecture of MLS V1.0 as described in [34] defines four reference points Le, Lr, Lpp and Lid. It also describes the components in the architecture as shown in figure 5.1.2.2.2.1:

- Location Privacy Checking Entity that is described in [18], clauses 6.3.11 and 6.3.12.
- MLS Client that is described in [18], clause 6.3.2.
- Requesting Location Server, Home Location Server and Visited Location Server that are described in [18], clause 6.3.3.

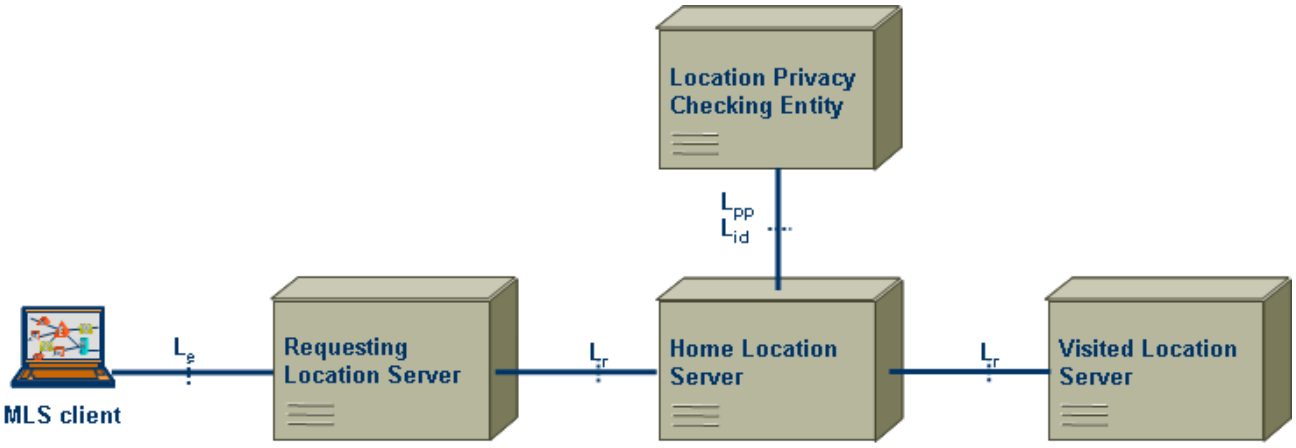


Figure 5.1.2.2.2.1: Logical LCS Architecture defined by OMA [34]

5.1.2.3 XDM

5.1.2.3.1 OMA

Various network functions such as, Presence, Push to Talk Over Cellular (PoC), Instant Messaging (IM), etc. need to access and manipulate certain information (e.g. the list of PoC participants who can take part in a PoC session as well as additional PoC-specific properties, the lists of PoC callers who are allowed/not allowed to call a given user, a list of users who are potential presentities, so that this list can be used to collectively subscribe to the presence status of each member in that list, an access control policy for Presence, which specifies whether a particular watcher is authorized to subscribe to a certain set of events).

NOTE: Such information is not always composed of pure lists (of principals), but can be a combination of lists together with other properties that define an end-user's personalization of the service behaviour.

The XDM enabler [35] specifies documents that can be shared by multiple enablers. One such case is a particular type of list, the URI List, which is a convenient way for a principal to group together a number of end users (e.g. "Friends" or "Family) or other resources, where such a list is expected to be reused for a number of different enablers. Such a list can be re-used wherever a principal has a need to collectively refer to a group of other end users or resources.

URI lists: The end-user can store URI information about other end-users to later initiate URI with them or to subscribe for their presence. A URI list is an essential basis for other OMA enabler (such as, PoC or messaging) as the addresses on the URI list are used to set up a session.

Group lists: Groups described in [35] are used for communication sessions (e.g. PoC sessions) or immediate messaging sessions for chat rooms. The group has properties (e.g. "open" or "restricted") that sets the rules for the communication.

Access Control list: According to [35] it shall be possible for Access Control lists to be created, modified and deleted by the subscriber or another authorized end-user.

XDM Client

- has to support the XDM Client procedures (document management, subscription to changes in XML documents); and
- the XCAP application usages (XCAP-Server Capabilities, XML Documents Directory).

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, the XDM Client can be implemented in a UE or an AS as defined in [22].

Aggregation Proxy

The Aggregation Proxy is the contact point for the XDM Client implemented in an UE to access XML documents stored in any XDMS. When realized with 3GPP IMS or 3GPP2 MMD networks, the Aggregation Proxy shall act as an Authentication Proxy defined in [23].

Example: Obtaining a PoC Group Document [67]

Figure 5.1.2.3.1.1 shows the call flow for obtaining a PoC group document.

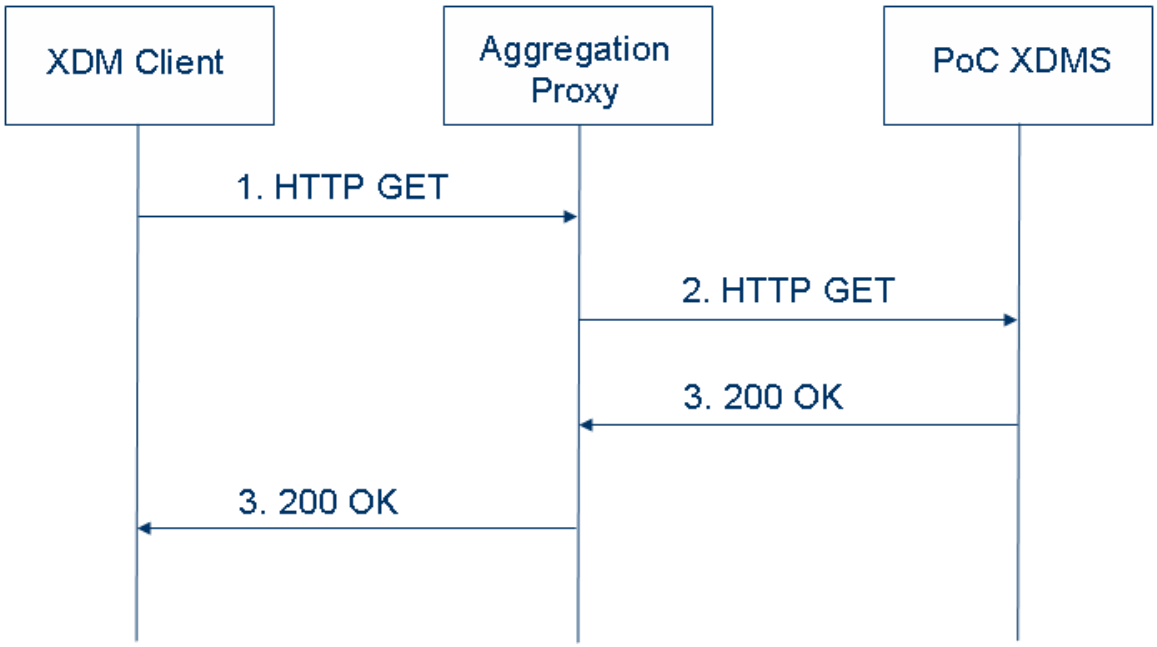


Figure 5.1.2.3.1.1: Obtaining a PoC group document as defined by OMA [67]

- The user "sip:ronald.underwood@example.com" wants to obtain the document describing his PoC User Access Policy rules. For this purpose the XDMC sends an HTTP GET request to the Aggregation Proxy.
- Based on the AUID the Aggregation Proxy forwards the request to PoC XDMS.
- After the PoC XDMS has performed the necessary authorization checks on the request originator, the PoC XDMS sends an HTTP "200 OK" response including the requested document in the body.
- The Aggregation Proxy routes the response to the XDM Client.

Step 1 and 3 have the following XML representation.

```
GET http://xcap.example.com/services
/org.openmobilealliance.poc-groups/users/sip:ronald.underwood@example.com/gossips.xml HTTP/1.1
...
Content-Length: 0
```

```
HTTP/1.1 200 OK
Etag: "et53"
...
Content-Type: application/vnd.oma.poc.groups+xml
<?xml version="1.0" encoding="UTF-8"?>
<group xmlns="urn:oma:xml:poc:list-service"
xmlns:rl="urn:ietf:params:xml:ns:resource-lists"
xmlns:cr="urn:ietf:params:xml:ns:common-policy"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <list-service uri="sip:myconference@example.com">
  <display-name xml:lang="en-us">Friends</display-name>
  <list>
   <entry uri="tel:+43012345678"/>
   <entry uri="sip:hermione.blossom@example.com"/>
  </list>
  <max-participant-count>10</max-participant-count>
  <cr:ruleset>
   <cr:rule id="a7c">
    <cr:conditions>
     <is-list-member/>
    </cr:conditions>
    <cr:actions>
     <join-handling>true</join-handling>
     <allow-anonymity>true</allow-anonymity>
    </cr:actions>
   </cr:rule>
  </cr:ruleset>
 </list-service>
</group>
```

Figure 5.1.2.3.1.2: XML representation of steps 1 and 3 for obtaining a PoC group document as defined by OMA [67]

5.1.2.4 Device Management

5.1.2.4.1 OMA

Architecture

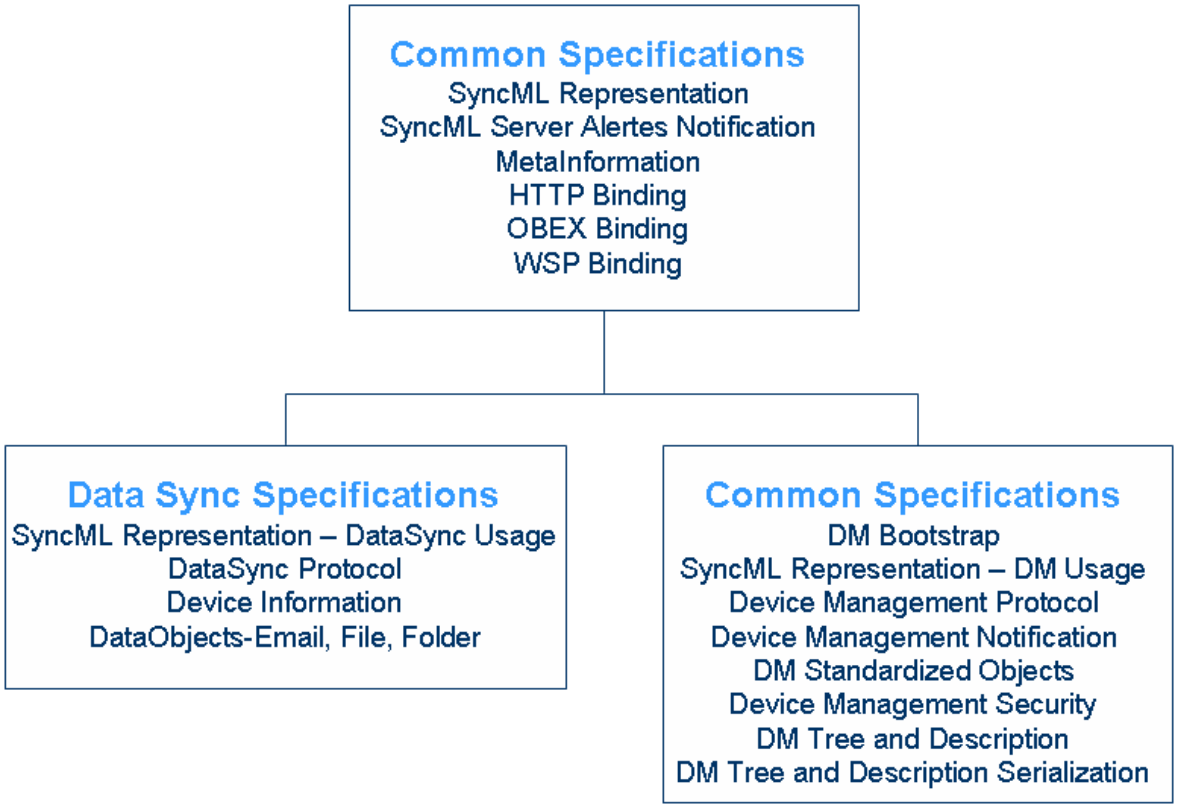


Figure 5.1.2.4.1.1: Document Structure for Device Management defined by OMA [35]

The OMA DM v1.2 specifications are based on the OMA Device Management (DM) v1.1.2 specifications and make use of the OMA SyncML Common v1.2 specifications as specified in the OMA SyncML common specification as can be seen in figure 5.1.2.4.1.1.

The SyncML Initiative, Ltd. was a not-for-profit corporation formed by a group of companies who co-operated to produce an open specification for data synchronization and device management.

The SyncML Initiative merged with the Open Mobile Alliance in November 2002. The SyncML legacy specifications were converted to the OMA format with the 1.1.2 versions of OMA SyncML Common, OMA Data Synchronization and OMA Device Management in May 2002.

The SyncML specification contains the following main components:

- An XML-based representation protocol.
- A synchronization protocol and a device management protocol.
- Transport bindings for the protocol.

A device description framework for device management OMA DM management objects are defined using the OMA DM Device Description Framework [DMTND], or DDF.

The following figure gives an example of OMA's definition of device information.

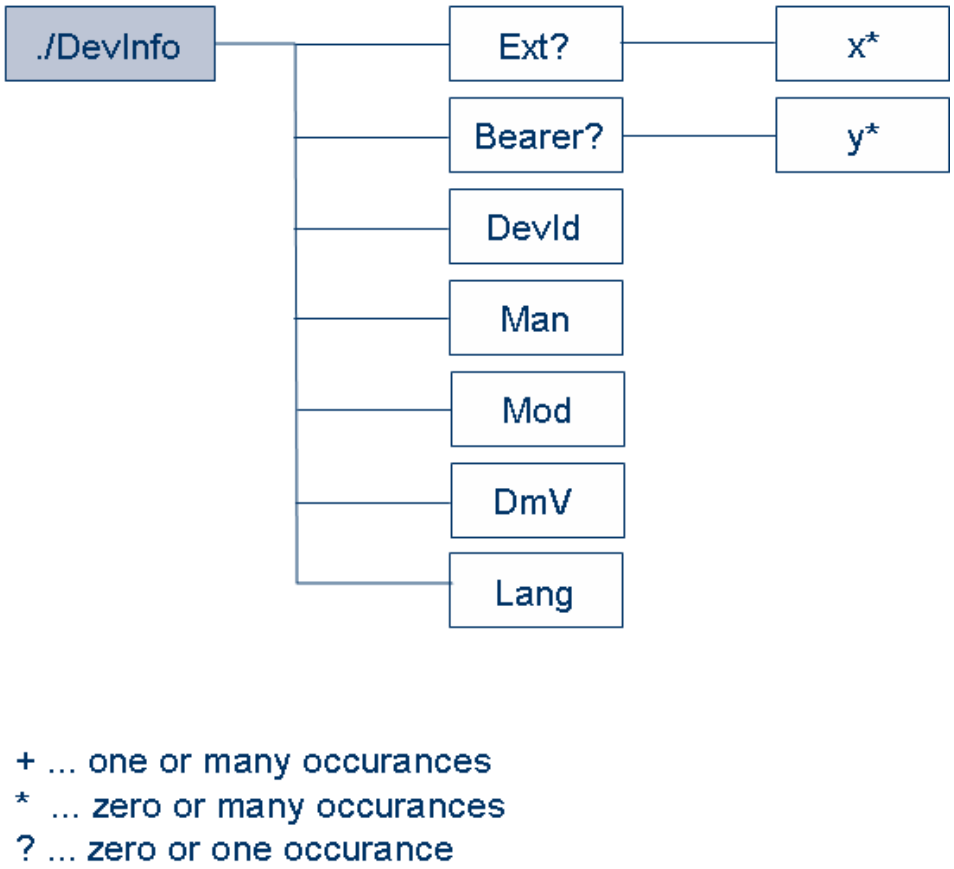


Figure 5.1.2.4.1.2: Example of a management object for Device Management defined by OMA [36]

Figure 5.1.2.4.1.2 provides some points to note:

- All the blocks with names in place occur exactly once, except Ext and Bearer that are optional and may not be present at all.
- The named node DevInfo has child nodes and is an interior node. With the exception of Ext and Bearer, which can have children, the other named nodes are leaf nodes.
- The un-named leaf nodes marked with * can be represented by any number of instantiated nodes at run-time, including none. The only limit is that the node names must be unique and memory must be available to store the nodes.

As part of the common definitions OMA [36] provides the following management objects:

DMAcc: the management object is used to manage settings for the OMA DM protocol.

DevInfo:

- Ext: An optional, interior node, designating the only branch of the DevInfo sub tree into which extensions can be added, permanently or dynamically.
- Bearer: An optional, interior node of the DevInfo sub tree in which items related to the bearer (CDMA, etc.) are stored. Use of this sub tree can be mandated by other standards.
- DevId: A unique identifier for the device, which should be globally unique and must be formatted as a URN as defined in RFC 2141 [102].
- Man: The manufacturer identifier.
- Mod: A model identifier (manufacturer specified string).
- DmV: OMA device management client version identifier (manufacturer specified string).

- Lang: The current language setting of the device. The syntax of the language tags and their use are defined in RFC 1766 [103]. Language codes are defined by ISO in the standard ISO 639 [104].

DevDetail:

- Ext: An optional, interior node, designating the only branch of the DevDetail sub tree into which extensions can be added, permanently or dynamically.
- Bearer: An optional, interior node, designating a branch of the DevDetail sub tree into which items related to the bearer (CDMA, etc.) are stored. Use of this sub tree can be mandated by other standards.
- URI/MaxDepth: Specifies the maximum depth of the management tree supported by the device. The maximum depth of the tree is defined as the maximum number of URI segments that the device supports. The value is a 16 bit, unsigned integer encoded as a numerical string. The value "'"' means that the device supports a tree of "unlimited" depth.
- URI/MaxTotLen: Specifies the maximum total length of any URI used to address a node or node property. The maximum total length of a URI is defined as the largest total number of characters making up the URI which the device can support. Note that depending on the character set this might not be the same as the number of bytes. The value is a 16 bit, unsigned integer encoded as a numerical string. The value "'0"' means that the device supports URI of "'unlimited"' length.
- URI/MaxSegLen: Specifies the maximum total length of any URI segment in a URI used to address a node or node property. The maximum total length of a URI segment is defined as the largest number of characters which the device can support in a single URI segment. Note that depending on the used character set this might not be the same as the number of bytes. The value is a 16 bit, unsigned integer encoded as a numerical string. The value "'0"' means that the device supports URI segments of "'unlimited"' length.
- DevTyp: Device type, e.g. PDA, pager, or phone.
- OEM: Original Equipment Manufacturer of the device.
- FwV: Firmware version of the device.
- SwV: Software version of the device.
- HwV: Hardware version of the device.
- LrgObj: Indicates whether the device supports the OMA DM Large Object Handling specification, as defined in [DMPRO].

Inbox:

In some circumstances a Management Object's URI is not the preferred addressing method and the management object identifier is enough information for the device to resolve a suitable location for that Management Object. In that case the URI: "./Inbox" is a reserved location for this purpose.

As part of the SyncML definitions OMA [37] provides the following management objects.

SyncML DM:

The SyncML DM management object consists of two parts.

- The first part is the DMAcc node which is where the SyncML DM specific settings are stored. These settings are collectively referred to as a SyncML DM account.
- The second part is Con, which is used for connectivity settings needed to communicate with a SyncML DM server. The sub tree of the Con node is similar to what a generic connectivity management object might look like and there is also substantial overlap with WAP Provisioning parameters here.

DevInfo: see above

DevDetail: see above

Example: Client Provisioning

According to [68] Client Provisioning is the process by which a device is initially configured with connectivity and application access parameters. This covers

- OTA provisioning; and
- provisioning by means of, e.g. Smart cards.

The actors involved in Client Provisioning include (see [68]):

- Management Authorities (including Network Operators, Enterprise Managers, Service Providers);
- Device Management Systems;
- Subscribers; and
- Users.

According to [68] a Device (e.g. a handset or PDA) has to be provisioned with correct Wireless Local Area Network (WLAN) parameters so that the user is able to access the WLAN service:

- network identifier;
- operation mode;
- security and authentication related parameters;
- etc.

The Device provisioning can be done via a local or public transport mechanisms, e.g. IR, Bluetooth, local, or non-local, wired, or wireless network.

5.1.2.5 Authorization and Authentication

5.1.2.5.1 ITU-T

ITU-T Recommendation X.509 [44] defines a framework for public-key certificates, which includes the specification of:

- data objects used to represent the certificates themselves; as well as
- revocation notices for issued certificates that should no longer be trusted.

In addition ITU-T Recommendation X.509 [44] defines a framework for attribute certificates, which includes specification of:

- data objects used to represent the certificates themselves; as well as
- revocation notices for issued certificates that should no longer be trusted.

In order for a user to be able to trust a public-key for another user, for instance to authenticate the identity of that user, ITU-T Recommendation X.509 [44] defines how the public-key is to be obtained from a trusted source. Such a source, called a Certification Authority (CA), certifies a public key by issuing a public-key certificate which binds the public-key to the entity which holds the corresponding private-key.

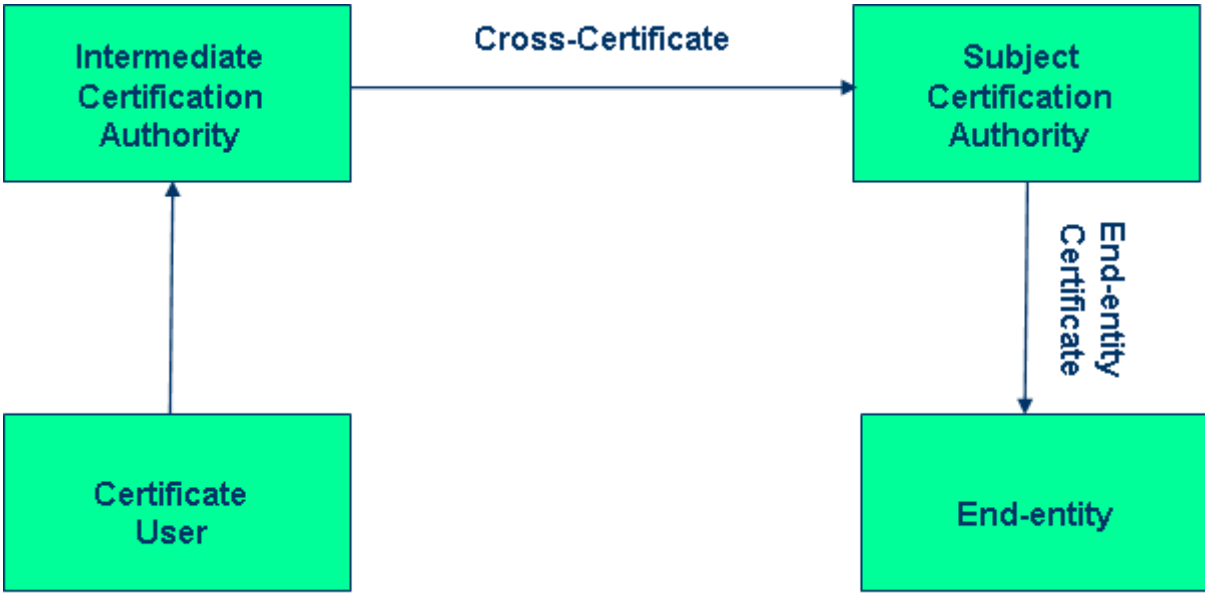


Figure 5.1.2.5.1.1: Example of a cross authentication architecture from ITU-T Recommendation X.509 [44]

The following ASN.1 data type has been defined by ITU-T Recommendation X.509 [44] to represent certificates:

```
Certificate                         ::=     SIGNED { SEQUENCE {
   version                  [0] Version DEFAULT v1,
   serialNumber                 CertificateSerialNumber,
   signature                    AlgorithmIdentifier,
   issuer                       Name,
   validity                         Validity,
   subject                      Name,
   subjectPublicKeyInfo         SubjectPublicKeyInfo,
   issuerUniqueIdentifier [1]   IMPLICIT UniqueIdentifier OPTIONAL,
                                    -- if present, version shall be v2 or v3
   subjectUniqueIdentifier[2]   IMPLICIT UniqueIdentifier OPTIONAL,
                                    -- if present, version shall be v2 or v3
   extensions               [3] Extensions OPTIONAL
                                    -- If present, version shall be v3 -- } }


   Version                      ::=     INTEGER { v1(0), v2(1), v3(2) }

   CertificateSerialNumber      ::=     INTEGER

AlgorithmIdentifier             ::=     SEQUENCE {
algorithm       ALGORITHM.&id ({SupportedAlgorithms}),
parameters          ALGORITHM.&Type ({SupportedAlgorithms}{ @algorithm}) OPTIONAL }
-- Definition of the following information object set is deferred, perhaps to standardized
-- profiles or to protocol implementation conformance statements. The set is required to
-- specify a table constraint on the parameters component of AlgorithmIdentifier.
-- SupportedAlgorithms          ALGORITHM           ::= { ... }

Validity                    ::=     SEQUENCE {
   notBefore        Time,
   notAfter         Time }

SubjectPublicKeyInfo                ::=     SEQUENCE {
   algorithm                AlgorithmIdentifier,
   subjectPublicKey         BIT STRING }

Time  ::=  CHOICE {
   utcTime              UTCTime,
   generalizedTime          GeneralizedTime }

Extensions ::= SEQUENCE OF Extension

Extension ::= SEQUENCE {
   extnId      EXTENSION.&id ({ExtensionSet}),
   critical        BOOLEAN DEFAULT FALSE,
   extnValue  OCTET STRING
```

```
            -- contains a DER encoding of a value of type &ExtnType
            -- for the extension object identified by extnId -- }

ExtensionSet EXTENSION      ::=     { ... }
```

- version: the version of the encoded certificate. If the extensions component is present in the certificate, version shall be v3. If the issuerUniqueIdentifier or subjectUniqueIdentifier component is present version shall be v2 or v3.
- serialNumber: is an integer assigned by the CA to each certificate. The value of serialNumber shall be unique for each certificate issued by a given CA (i.e. the issuer name and serial number identify a unique certificate).
- signature: contains the algorithm identifier for the algorithm and hash function used by the CA in signing the certificate.
- issuer: identifies the entity that has signed and issued the certificate.
- validity: time interval during which the CA warrants that it will maintain information about the status of the certificate.
- Subject: identifies the entity associated with the public-key found in the subject public key field.
- subjectPublicKeyInfo: carries the public key being certified and identifies the algorithm which this public key is an instance of .
- issuerUniqueIdentifier: uniquely identifies an issuer in case of name re-use.
- subjectUniqueIdentifier: uniquely identifies a subject in case of name re-use.
- Extensions: field, which allows addition of new fields to the structure without modification to the ASN.1 definition. An extension field consists of an extension identifier, a criticality flag, and an encoding of a data value of an ASN.1 type associated with the identified extension.

If revocation lists are published, they the following information:

- Certificate revocation list.
- Authority revocation list.
- Delta revocation list.
- Attribute certificate revocation list.
- Attribute authority revocation list.

The following ASN.1 data type has been defined by ITU-T Recommendation X.509 [44] to represent revocation lists:

```
CertificateList          ::=     SIGNED { SEQUENCE {
    version                          Version OPTIONAL,
                                     -- if present, version shall be v2
    signature                        AlgorithmIdentifier,
    issuer                           Name,
    thisUpdate                       Time,
    nextUpdate                       Time OPTIONAL,
    revokedCertificates              SEQUENCE OF SEQUENCE {
        serialNumber                         CertificateSerialNumber,
        revocationDate                       Time,
        crlEntryExtensions           Extensions OPTIONAL } OPTIONAL,
    crlExtensions        [0]             Extensions OPTIONAL }}
```

- version: version of the encoded revocation list. If the extensions component flagged as critical is present in the revocation list, version shall be v2. If no extensions component flagged as critical is present in the revocation list, version may either be absent or present as v2.
- Signature: contains the algorithm identifier for the algorithm used by the authority to sign the revocation list.
- Issuer: identifies the entity that has signed and issued the revocation list.
- thisUpdate: date/time at which this revocation list was issued.

- nextUpdate: if present, indicates the date/time by which the next revocation list in this series will be issued.
- revokedCertificates: identifies certificates that have been revoked. The revoked certificates are identified by their serial numbers.
- crlExtensions: if present, contains one or more CRL extensions.

The attribute certificate framework defined in ITU-T Recommendation X.509 [44] provides a foundation upon which Privilege Management Infrastructures (PMI) can be built. These infrastructures can support applications such as access control.

The binding of a privilege to an entity is provided by an authority through a digitally signed data structure called an attribute certificate or through a public-key certificate containing an extension defined explicitly for this purpose.

An attribute certificate using system needs to validate a certificate prior to using that certificate for an application. Procedures for performing that validation are also defined here, including verifying the integrity of the certificate itself, its revocation status, and its validity with respect to the intended use.

An attribute certificate is a separate structure from a subject's public key certificate. A subject may have multiple attribute certificates associated with each of its public key certificates. There is no requirement that the same authority create both the public key certificate and attribute certificate(s) for a user; in fact separation of duties will frequently dictate otherwise.

The attribute certificate is defined as follows ITU-T Recommendation X.509 [44].

```
AttributeCertificate ::= SIGNED {AttributeCertificateInfo}

AttributeCertificateInfo ::= SEQUENCE
   {
   version                    AttCertVersion, --version is v2
   holder                         Holder,
   issuer                     AttCertIssuer,
   signature                  AlgorithmIdentifier,
   serialNumber               CertificateSerialNumber,
   attrCertValidityPeriod     AttCertValidityPeriod,
   attributes                 SEQUENCE OF Attribute,
   issuerUniqueID             UniqueIdentifier OPTIONAL,
   extensions                 Extensions  OPTIONAL
   }

AttCertVersion    ::= INTEGER { v2(1) }

Holder    ::= SEQUENCE
          {
          baseCertificateID        [0] IssuerSerial    OPTIONAL,
               -- the issuer and serial number of the holder's Public Key Certificate
          entityName               [1] GeneralNames    OPTIONAL,
               -- the name of the entity or role
          objectDigestInfo         [2] ObjectDigestInfo OPTIONAL
               -- used to directly authenticate the holder, e.g. an executable
-- at least one of baseCertificateID, entityName or objectDigestInfo shall be present --}

ObjectDigestInfo    ::= SEQUENCE {
   digestedObjectType  ENUMERATED {
     publicKey            (0),
     publicKeyCert        (1),
     otherObjectTypes     (2) },
   otherObjectTypeID      OBJECT IDENTIFIER  OPTIONAL,
   digestAlgorithm            AlgorithmIdentifier,
   objectDigest           BIT STRING }

AttCertIssuer ::= [0] SEQUENCE {
issuerName                GeneralNames OPTIONAL,
baseCertificateID     [0] IssuerSerial OPTIONAL,
objectDigestInfo      [1] ObjectDigestInfo OPTIONAL }
-- At least one component shall be present
   ( WITH COMPONENTS { ..., issuerName PRESENT } |
   WITH COMPONENTS { ..., baseCertificateID PRESENT } |
   WITH COMPONENTS { ..., objectDigestInfo PRESENT } )

IssuerSerial  ::=  SEQUENCE {
   issuer     GeneralNames,
   serial     CertificateSerialNumber,
   issuerUID  UniqueIdentifier OPTIONAL }
```

```
AttCertValidityPeriod  ::= SEQUENCE {
   notBeforeTime      GeneralizedTime,
   notAfterTime       GeneralizedTime }
```

- version: differentiates between different versions of the attribute certificate. For attribute certificates issued in accordance with the syntax in the present document, version shall be v2.
- Holder: field which conveys the identity of the attribute certificate's holder.
  - baseCertificateID: if present, identifies a particular public-key certificate that is to be used to authenticate the identity of this holder when asserting privileges with this attribute certificate;
  - entityName: if present, identifies one or more names for the holder;
  - objectDigestInfo: if present, is used directly to authenticate the identity of a holder, including an executable holder (e.g. an applet).
- issuer field: conveys the identity of the AA that issued the certificate.
  - issuerName: if present, identifies one or more names for the issuer.
  - baseCertificateID: if present, identifies the issuer by reference to a specific public-key certificate for which this issuer is the subject.
  - objectDigestInfo: if present, identifies the issuer by providing a hash of identifying information for the issuer.
- Signature: identifies the cryptographic algorithm used to digitally sign the attribute certificate.
- serialNumber: uniquely identifies the attribute certificate within the scope of its issuer.
- attrCertValidityPeriod: conveys the time period during which the attribute certificate is considered valid, expressed in GeneralizedTime format.
- attributes: contains the attributes associated with the holder that are being certified (e.g. the privileges).
- issuerUniqueID: may be used to identify the issuer of the attribute certificate in instances where the issuer component is not sufficient.
- extensions: allows addition of new fields to the attribute certificate.

5.1.2.5.2 IETF

The Diameter base protocol [41] provides an Authentication, Authorization and Accounting (AAA) framework for network functions such as network access or IP mobility. Diameter is applicable in both local Authentication, Authorization and Accounting and roaming situations.

Diameter can provide two different types of services to network functions:

- Authentication and authorization, optionally making use of accounting.
- Accounting only.

[41] defines the following AVPs for Authentication and Authorization.

- Origin-State-Id AVP: Origin-State-Id is used to allow rapid detection of terminated sessions.
- Auth-Request-Type AVP: The Auth-Request-Type AVP is included in network function-specific auth requests to inform the peers whether a user is to be authenticated only, authorized only or both.
- Session-Id AVP: The Session-Id AVP is used to identify a specific session.
- Authorization-Lifetime AVP: The Authorization-Lifetime AVP contains the maximum number of seconds of service to be provided to the user before the user is to be re-authenticated and/or re-authorized.
- Auth-Grace-Period AVP: The Auth-Grace-Period AVP contains the number of seconds the Diameter server will wait following the expiration of the Authorization-Lifetime AVP before cleaning up resources for the session.

- Auth-Session-State AVP: The Auth-Session-State AVP specifies whether state is maintained for a particular session.
- Re-Auth-Request-Type AVP: The Re-Auth-Request-Type AVP is included in network function-specific auth answers to inform the client of the action expected upon expiration of the Authorization-Lifetime.
- Session-Timeout AVP: The Session-Timeout AVP contains the maximum number of seconds of service to be provided to the user before termination of the session.
- User-Name AVP: The User-Name AVP (AVP Code 1) [RADIUS] is of type UTF8String, which contains the User-Name, in a format consistent with the NAI specification.
- Termination-Cause AVP: The Termination-Cause AVP is used to indicate the reason why a session was terminated on the access device.
- Origin-State-Id AVP: The Origin-State-Id AVP is a monotonically increasing value that is advanced whenever a Diameter entity restarts with loss of previous state, for example upon reboot.
- Session-Binding AVP: The Session-Binding AVP may be present in network function-specific authorization answer messages.
- Session-Server-Failover AVP: The Session-Server-Failover AVP may be present in network function-specific authorization answer messages that either do not include the Session-Binding AVP or include the Session-Binding AVP with any of the bits set to a zero value.
- Multi-Round-Time-Out AVP: The Multi-Round-Time-Out AVP should be present in network function-specific authorization answer messages whose Result-Code AVP is set to DIAMETER_MULTI_ROUND_AUTH. This AVP contains the maximum number of seconds that the access device must provide the user in responding to an authentication request.
- Class AVP: The Class AVP is used to by Diameter servers to return state information to the access device.
- Event-Timestamp AVP: The Event-Timestamp may be included in an Accounting-Request and Accounting-Answer messages to record the time that the reported event occurred, in seconds since January 1, 1900 00:00 UTC.

RFC 3280 [42] profiles the format and semantics of certificates and Certificate Revocation Lists (CRLs) for the Internet PKI.

The users of certificates will operate in a wide range of environments with respect to their communication topology, especially users of secure electronic mail. This profile supports users without high bandwidth, real-time IP connectivity, or high connection availability.

The following figure gives an overview over the basic building blocks of IETF's PKI infrastructure.

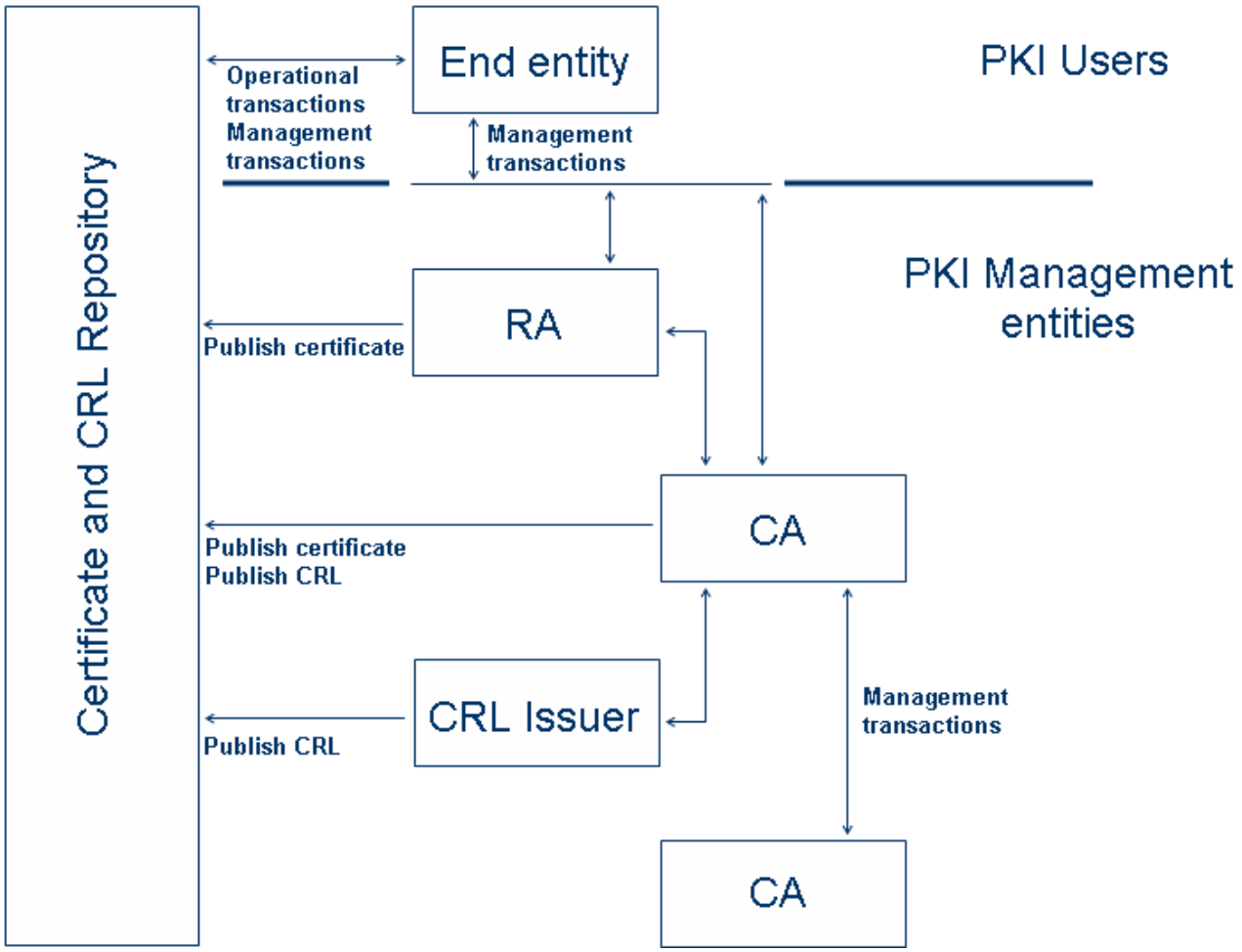


Figure 5.1.2.5.2.1: PKI Entities defined by IETF [42]

The following paragraphs present the profile for public key certificates according to RFC 3280 [42] that will foster interoperability and a reusable PKI. This clause is based upon the X.509 v3 certificate format and the standard certificate extensions defined in ITU-T Recommendation X.509 [44].

- Certificate: The Certificate is a SEQUENCE of three required fields.
  - tbsCertificate: The field contains the names of the subject and issuer, a public key associated with the subject, a validity period, and other associated information.
  - SignatureAlgorithm: The signatureAlgorithm field contains the identifier for the cryptographic algorithm used by the CA to sign this certificate.
  - SignatureValue: The signatureValue field contains a digital signature computed upon the ASN.1 DER encoded tbsCertificate. The ASN.1 DER encoded tbsCertificate is used as the input to the signature function.

- TBSCertificate: The sequence TBSCertificate contains information associated with the subject of the certificate and the CA who issued it. Every TBSCertificate contains the names of the subject and issuer, a public key associated with the subject, a validity period, a version number, and a serial number; some MAY contain optional unique identifier fields.
  - Version: This field describes the version of the encoded certificate.
  - Serial number: The serial number must be a positive integer assigned by the CA to each certificate. It must be unique for each certificate issued by a given CA (i.e. the issuer name and serial number identify a unique certificate).
  - Signature: This field contains the algorithm identifier for the algorithm used by the CA to sign the certificate.
  - Issuer: The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). The issuer field is defined as the X.501 type Name.
  - Validity: The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. The field is represented as a SEQUENCE of two dates: the date on which the certificate validity period begins (notBefore) and the date on which the certificate validity period ends (notAfter).
  - Subject: The subject field identifies the entity associated with the public key stored in the subject public key field.
  - Subject Public Key Info: This field is used to carry the public key and identify the algorithm with which the key is used (e.g. RSA, DSA, or Diffie-Hellman).
  - Unique Identifiers: These fields MUST only appear if the version is 2 or 3.
  - Extensions: This field must only appear if the version is 3.

In addition IETF uses the extensions defined for X.509 v3 certificates, which provide methods for associating additional attributes with users or public keys and for managing a certification hierarchy.

As discussed in [42], one goal of this X.509 v2 CRL profile is to provide the basis for the creation of an interoperable and reusable Internet PKI. The profile defines:

- a set of information that can be expected in every CRL; and
- common locations within the CRL for frequently used attributes as well as common representations for these attributes.

The following items describe the use of the X.509 v2 CRL in the Internet PKI.

- CertificateList: The CertificateList is a sequence of three required fields.
  - tbsCertList: This field is itself a sequence containing the name of the issuer, issue date, issue date of the next list, the optional list of revoked certificates, and optional CRL extensions.
  - signatureAlgorithm: The signatureAlgorithm field contains the algorithm identifier for the algorithm used by the CRL issuer to sign the CertificateList.
  - signatureValue: The signatureValue field contains a digital signature computed upon the ASN.1 DER encoded tbsCertList.
- Certificate List "To Be Signed": The or TBSCertList is a sequence of required and optional fields. The required fields identify the CRL issuer, the algorithm used to sign the CRL, the date and time the CRL was issued, and the date and time by which the CRL issuer will issue the next CRL.
  - Version: This optional field describes the version of the encoded CRL.
  - Signature: This field contains the algorithm identifier for the algorithm used to sign the CRL.
  - Issuer Name: The issuer name identifies the entity that has signed and issued the CRL.
  - This Update: This field indicates the issue date of this CRL.

- Next Update: This field indicates the date by which the next CRL will be issued.
- Revoked Certificates: When there are revoked certificates, they are listed by their serial numbers.
- Extensions: This field may only appear if the version is 2. If present, this field is a sequence of one or more CRL extensions.

5.1.2.5.3 3GPP

For 3G networks the following security features related to entity authentication are provided [24]:

- user authentication: the property that the serving network corroborates the user identity of the user;
- network authentication: the property that the user corroborates that he is connected to a serving network that is authorized by the user's HE to provide him services; this includes the guarantee that this authorization is recent.

To achieve these objectives, 3GPP assumes that entity authentication occurs at each connection set-up between the user and the network. To this end two mechanisms have been defined:

- an authentication mechanism using an authentication vector delivered by the user's HE to the serving network; and
- a local authentication mechanism using the integrity key established between the user and serving network during the previous execution of the authentication and key establishment procedure.

The SN may request the MS to send it the IMEI or IMEISV of the terminal. The IMEI should be securely stored in the terminal.

User to USIM authentication restricts access to the USIM until the USIM has authenticated the user. Thereby, it is ensured that access to the USIM can be restricted to an authorized user or to a number of authorized users.

To accomplish this feature, user and USIM must share a secret (e.g. a PIN) that is stored securely in the USIM. The user gets access to the USIM only if he/she proves knowledge of the secret.

USIM to terminal authentication ensures that access to a terminal or other user equipment can be restricted to an authorized USIM.

To this end, the USIM and the terminal must share a secret that is stored securely in the USIM and the terminal.

Assignment of temporary identities allows the identification of a user on the radio access link.

These are:

- a temporary mobile subscriber identity (TMSI/P-TMSI), which has local significance only in the location area or routing area in which the user is registered; and which
- outside that area should be a accompanied by an appropriate:
  - Location Area Identification (LAI); or
  - Routing Area Identification (RAI) in order to avoid ambiguities.

The association between the permanent and temporary user identities is kept by the Visited Location Register (VLR/SGSN) in which the user is registered.

Authentication by key agreement achieves mutual authentication by the user and the network.

Both parties show knowledge of:

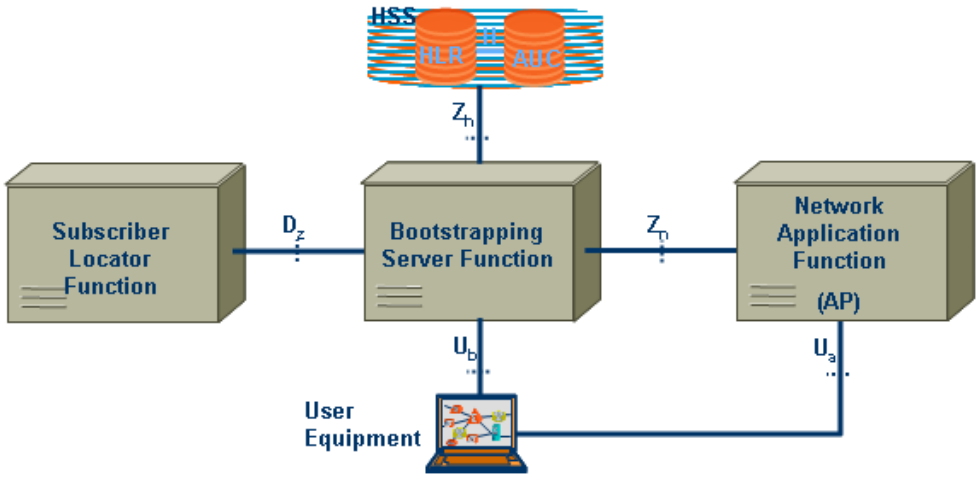
- A secret key K which is shared between and available only to the USIM and the AuC in the user's HE.
- In addition the USIM and the HE keep track of counters:
  - SQN_{MS}; and
  - SQN_{HE} respectively to support network authentication.

The sequence number SQN_{HE} is an individual counter for each user and the sequence number SQN_{MS} denotes the highest sequence number the USIM has accepted.

Upon receipt of a request from the VLR/SGSN, the HE/AuC sends an ordered array of *n* authentication vectors (the equivalent of a GSM "triplet") to the VLR/SGSN. The authentication vectors are ordered based on sequence number. Each authentication vector consists of the following components:

- a random number RAND;
- an expected response XRES;
- a cipher key CK;
- an integrity key IK and an authentication token AUTN.

Authorization of IMS-SIP based services has the following basic architecture if the NAF is based in the home network.



BSF Bootstrapping Server Functionality
HSS Home Subscriber System
NAF Operator-controlled network application function functionality
UE User Equipment

Figure 5.1.2.5.3.1: Simple network architecture for bootstrap in the home network defined by 3GPP [23]

Authorization of IMS-SIP based services has the following basic architecture if the NAF is based in the visited network.

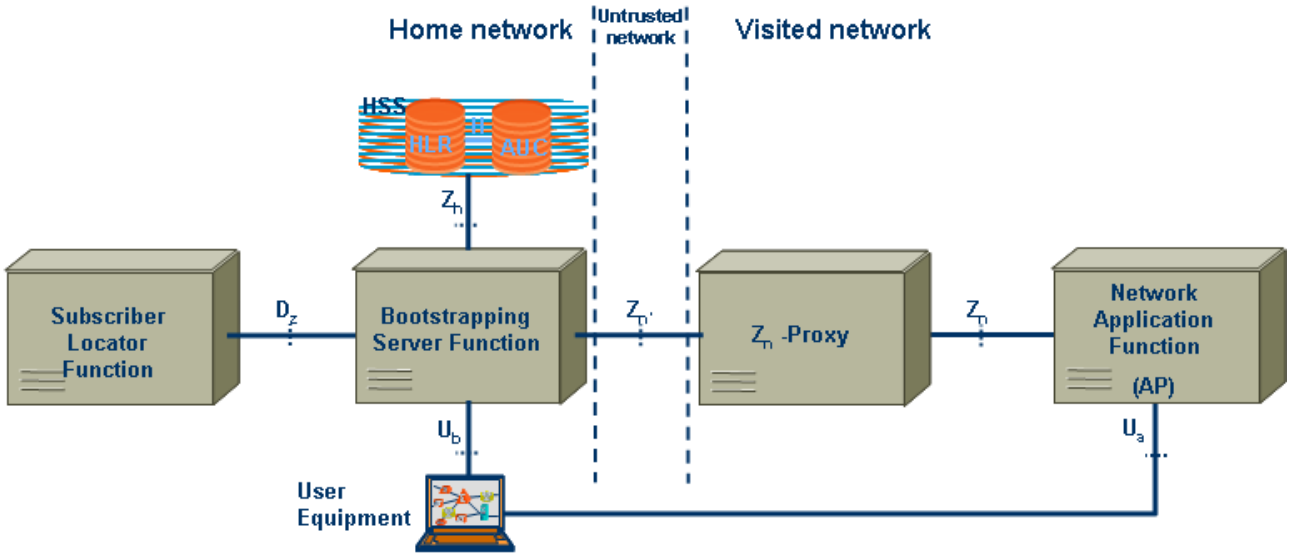


Figure 5.1.2.5.3.2: Simple network architecture for bootstrap in the visited network defined by 3GPP [23]

As described in [23], the generic Bootstrapping Server Function (BSF) and the UE shall mutually authenticate using the AKA protocol, and agree on session keys that are afterwards applied between UE and a Network Application Function (NAF).

After the bootstrapping has been completed, the UE and a NAF can run some application specific protocol where the authentication of messages will be based on those session keys generated during the mutual authentication between UE and BSF.

In the case where UE has contacted a NAF that is operated in another network than home network, this visited NAF shall use a Zn-Proxy of the NAFs network to communicate with subscriber's BSF (i.e. home BSF).

The set of all user security settings (USSs), i.e. GUSS, is stored in the HSS. In the case where the subscriber has multiple subscriptions, i.e. multiple ISIM or USIM applications on the UICC, the HSS shall contain one or more GUSSs that can be mapped to one or more private identities, i.e. IMPIs and IMSIs.

The required functionalities from the UE are:

- the support of HTTP Digest AKA protocol;
- the capability to use both a USIM and an ISIM in bootstrapping;
- the capability to select either a USIM or an ISIM to be used in bootstrapping, when both of them are present;
- the capability for a Ua application on the ME to indicate to the GBA Function on the ME the type or the name of UICC application to use in bootstrapping;
- the capability to derive new key material to be used with the protocol over Ua interface from CK and IK;
- support of NAF-specific application protocol.

The SLF:

- is queried by the BSF in conjunction with the Zh interface operation to get the name of the HSS containing the required subscriber specific data;
- is accessed via the Dz interface by the BSF.

5.1.2.5.4 OMA

Internet Certificate Profile

In [38] OMA defines WAP certificate profiles. The profiles are mainly based on the Internet Certificate Profile defined in RFC 3280 [42], which in turn is based on the format defined in ITU-T Recommendation X.509 [44]. Specification [38] provides, for each certificate type discussed, additional details regarding the contents of some individual fields in the certificate.

Network functions must recognize all the following required distinguished name attributes:

- countryName;
- organizationName;
- organizationalUnitName;
- stateOrProvinceName;
- commonName;
- domainComponent;
- serialNumber.

CAs are not required to issue certificates with the:

- serialNumber attribute;

but they should be able to do so.

All network functions must recognize all required distinguished name attributes listed above. Further, they must recognize the serialNumber attribute.

According to [38] certificate-processing network functions must recognize the following standard extensions:

- keyUsage;
- extKeyUsage;
- certificatePolicies;
- subjectAltName; and
- basicConstraints.

If the keyUsage extension is included, it shall have the:

- digitalSignature bit;

set if the public key is an RSA key.

Global Permissions Management (GPM)

In OMA's current service environment framework, user permissions may be distributed across multiple sources to address the service-specific solutions required by each enabler (e.g. location services). In this case user permissions involve dynamic data about an end-user:

- location information that is to be shared only under certain conditions; and
- how specific actions are to be executed in doing so.

Functionality to perform location privacy checking is being specified in OMA for mobile location services using an optional privacy checking protocol (PCP) defined over an interface between the location server and a separate privacy checking entity. However mechanisms to allow the end-user to manage the permissions rules governing the release of his/her own location are not clearly specified nor mandated for mobile location services in OMA.

In Global Permissions Management, (GPM) [69], OMA aims to specify an enabler that is capable of generically managing permissions rules across OMA service enablers providing end-users with a global view of their permissions. These determine if, when, how and to what extent information about a permissions target can be released.

The [69] specifically identifies use cases and requirements from end-user and service provider perspective. These show for example how:

- Authorized principals express and manage their permissions rules through user-friendly provisioning tools (not to be specified), and manage related events such as being notified of changes to permissions rules, or when /if consent is required and by whom.
- Permissions rules are evaluated to determine what data can be shared with whom and in what situations.

According to [69] authorized principals can manage their permissions over time in a logically centralized manner, e.g. by adding new services and having these services re-use existing permission rules.

The following figure gives an idea of the actors involved in GPM.

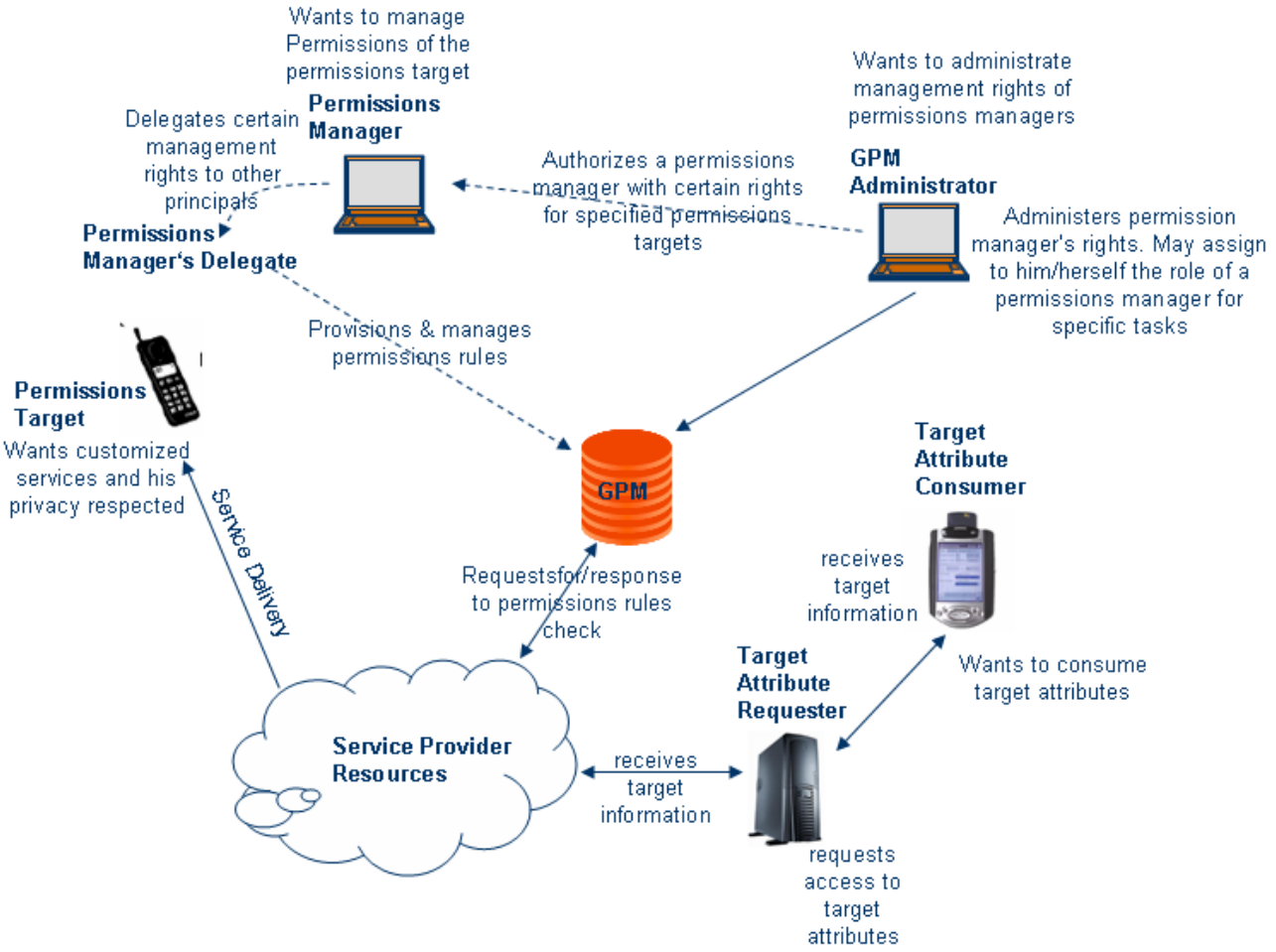


Figure 5.1.2.5.4.1: Actors for GPM defined by [69]

The Permissions Target is the principal who is the subject of permissions rules that govern the way other principals access information about him and ultimately how his services are executed. The Permissions Target is usually a human end-user (or a group of human end-users) of services.

Permissions Manager: is an authorized principal who manages, (creates, modifies, deletes, etc.) permissions rules.

Permissions Manager's Delegate: is a principal authorized by a Permissions Manager to perform certain responsibilities on his/her behalf.

GPM Administrator: is responsible for determining who the authorized permissions managers are, what their GPM management rights are, and to which permissions targets those rights apply. The GPM Administrator is typically employed by an operator or service provider.

Target Attribute Consumer: any principal who wishes to consume information (target attributes) about the Permissions Target either directly or through the invocation of a service.

Target Attribute Requester: is the actor who requests access to the attributes of the Permissions Target (e.g. on behalf of the Target Attribute Consumer).

Service provider: will want to use GPM to check permissions set for the Permissions Target before any data about him is disclosed to the Requester as part of its service delivery.

In [70] the following interfaces for the architecture shown in the figure 5.1.2.5.4.2 are defined:

GPM-1 (PEM-1): This interface is derived from PEM-1 [71], using the PEEM defined process of using templates.

GPM-2 (PEM-2): This interface is derived from PEM-2 [71]. It allows Authorized Principals to manage Permissions Rules.

Interface to other resources: Like in the [x5, Clause 5.3.5], the Interface to other external resources is not specified by GPM.

The architecture [71] for PEEM is defined as follows:

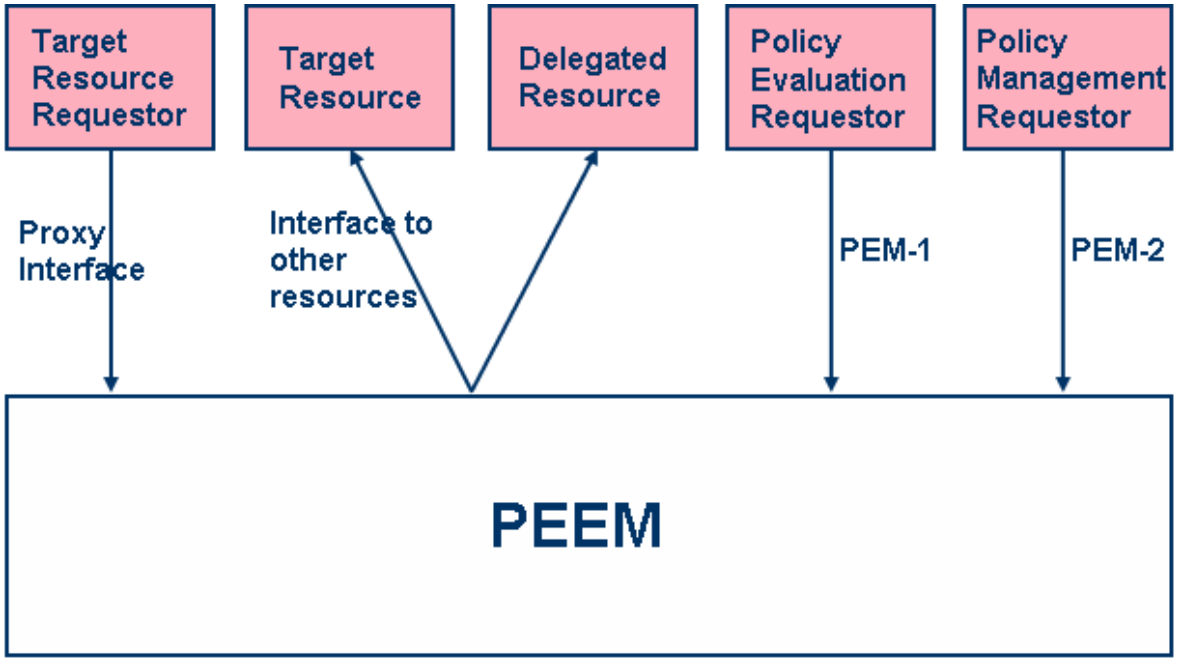


Figure 5.1.2.5.4.2: Architecture for PEEM defined in [71]

The PEEM [71] enabler exposes the following interfaces:

- PEM-1 (PEEM specified callable interface);
- PEM-2 (PEEM specified management interface);
- Proxy interface (used for intercepting requests to target resources).

In addition to PEEM components and interfaces, there are other elements represented in figure 5.1.2.5.4.2 for a better understanding of the architectural diagram. The following is a list of other elements identified in figure 5.1.2.5.4.2 that interact with PEEM [71]:

- Target Resource Requestor:
  - Target Resource Requestor represents a resource (e.g. application, enabler) that issues a request to a target resource.
- Target Resource:
  - Target Resource represents the destination resource for a request made by another resource.
- Delegated Resource:
  - Delegated Resource represents the resource to which PEEM may delegate certain policy actions during the policy processing process.
- Evaluation Requestor:
  - Evaluation Requestor represents a resource (e.g. application, enabler) that issues a request for policy processing to PEEM.

- Management Requestor:
  - Management Requestor represents a resource (e.g. application, enabler) that issues a request for policy management to PEEM.
- Interface to other resources:
  - The interface to other resources is not specified by PEEM, but is used to exchange messages compliant to the interface of the target or delegated enablers or more generally messages compliant to the target or delegated resource interfaces.

By definition (see [71]), policies are combinations of policy rules, each of which is defined as a policy condition and actions (i.e. IF condition THEN action).

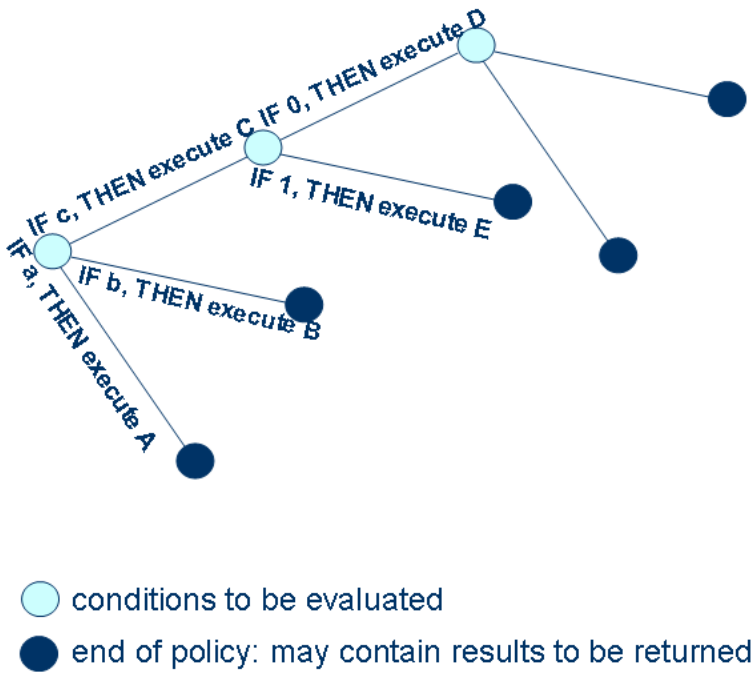


Figure 5.1.2.5.4.3: PEEM Information Model defined in [71]

Evaluation may involve arbitrary computations. The conditions and actions in policy rules may require the execution of arbitrary functions that include delegation to OMA enabler implementations.

The topology of a policy is defined as a graph where each node represents a condition to be evaluated and each outbound branch has actions to be executed if the corresponding condition is true. This is illustrated in figure 5.1.2.5.4.3.

There are 2 execution models described by the IETF policy model defined in RFC 3060 [87]:

- single condition at each node;
- permits case statements on the nodes where each includes a priority that determines the order of evaluation of these simple conditions.

5.1.2.6 Accounting

5.1.2.6.1 ITU-T

ITU-T Recommendation Q.825 [45] specifies how CDRs (Call Detail Records) are produced and managed in Network Elements for POTS, ISDN and IN (Intelligent Networks).

The information model for Call Detail Recording is formally described in terms of an Entity-Relationship model, and an object model specified in terms of GDMO templates (Guidelines for the Definition of Managed Objects).

[40] defines the following attributes with very brief only, see [45] for the complete text.

1	accessDelivery:	Indicates that the call was delivered to the called subscriber.
2	accountCodeInput:	Account code (for billing), supplied by subscriber.
78	additionalParticipantInfo:	(No details given).
5	b-PartyCategory:	Subscriber category for called subscriber.
4	bearerService:	Bearer capability information (only for ISDN calls).
13	cDRPurpose:	Reason for triggering this Call Data Record.
70	callDetailDataId:	Unique identifier for the CallDetailData object.
79	callDuration:	Duration of call.
6	callIdentificationNumber:	Identification number for call; all records produced for this call have the same callIdenfificationNumber.
73	callStatus:	Identifies whether the call was answered or not.
9	calledPartyNumber:	Telephone number of the called subscriber (may be a "diverted-to" or "translated" number).
7	callingPartyCategory:	Calling subscriber category.
8	callingPartyNumber:	Telephone number of the calling party.
10	callingPartyNumberNotScreened:	An additional, user-provided (not screened) number to the calling party.
11	callingPartyType:	Calling subscriber type.
74	carrierId:	Carrier ID to which the call is sent.
12	cause:	Cause and location value for the termination of the call.
14	chargedDirectoryNumber:	Charged directory number (where the charged participant element can't indicate the number).
16	chargedParticipant:	Participant to be charged for the usage.
15	chargingInformation:	Charging information generated by a Network Element which is capable of charging.
17	configurationMask:	Time consumption, e.g. from B-answer to termination time, between partial call records, etc.
18	conversationTime:	Time consumption from B-answer to end of call.
19	creationTriggerList:	List of trigger values which will create Call Detail data objects.
75	dPC:	Destination point code (for analysis purposes).
20	dataValidity:	Indicates that the NE is having problems, contents of the generated Call Detail record is not reliable.
23	durationTimeACM:	Time consumption from seizure until received ACM.
21	durationTimeB-Answer:	Time consumption from seizure until B-answer.
22	durationTimeNoB-Answer:	Time from seizure to termination when no B-answer was received.
25	exchangeInfo:	Identity of exchange where Call Detail record was generated.
26	fallbackBearerService:	Fallback bearer capability information for a call.
27	glare:	Indicates if a glare condition was encountered.
31	iNServiceInformationList:	Contains information about the use of IN (Intelligent Network) services.
32	iNSpecificInformation:	Contains information about the use of one IN service.
33	iSUPPreferred:	Indicate whether an ISUP preference was requested.
28	immediateNotificationForUsageMetering:	Indicates that the Call Detail records requires immediate data transfer to the Operations System.
34	maxBlockSize:	Maximum number of Call Detail records in a block.
35	maxTimeInterval:	Maximum latency allowable for near-real-time Call Detail data delivery.
36	networkManagementControls:	Indicates which Traffic Management Control has affected the call.
37	networkProviderId:	Indicates the Network Provider for whom the CDR is generated.
76	oPC:	Originating point code for a failed call (for analysis purposes).
38	operatorSpecific1AdditionalNumber	
40	operatorSpecific2AdditionalNumber	

42 operatorSpecific3AdditionalNumber: Operator-defined additional participant information.
39 operatorSpecific1Number
41 operatorSpecific2Number
43 operatorSpecific3Number: Operator-defined participant information.
44 originalCalledNumber: Telephone number of the original called party.
45 partialGeneration: Included if the CDR (Call Detail record) output is partial. Such CDRs have a field indicating their partial record number.
77 participantInfo: (No details given).
46 percentageToBeBilled: Percentage to be billed when normal billing rules are not to be followed.
47 periodicTrigger: Defines the intervals at which the CDR file should be created.
48 personalUserId: Internationally unique personal User Identity (for UPT calls).
49 physicalLineCode: Identifies the call subscriber's physical line.
50 progress: Describes an event which occurred during the life of a call.
51 queueInfo: Used to record usage of queuing resources with IN calls.
52 receivedDigits: The digits dialled by the subscriber. (Normally only included for customer care purposes).
53 recordExtensions: Information elements added by network operators and/or manufacturers in addition to the standard ones above.

5.1.2.6.2 IETF

Figure 5.1.2.6.2.1 shows the main architectural components of IETF's way to collect data [40]. Based on this architecture IETF defines the following accounting attributes:

RADIUS

Each RADIUS attribute is identified by an 8-bit number, the RADIUS Type field. Up-to-date values of this field can be found in the most recent Assigned Numbers RFC [ASG-NBR], at the time of writing the Technical Report is as follows:

1 User-Name
2 User-Password
3 CHAP-Password
4 NAS-IP-Address
5 NAS-Port
6 Service-Type
7 Framed-Protocol
8 Framed-IP-Address
9 Framed-IP-Netmask
10 Framed-Routing
11 Filter-Id
12 Framed-MTU
13 Framed-Compression
14 Login-IP-Host
15 Login-Service
16 Login-TCP-Port
17 (unassigned)
18 Reply-Message
19 Callback-Number
20 Callback-Id
21 (unassigned)
22 Framed-Route
23 Framed-IPX-Network
24 State
25 Class
26 Vendor-Specific
27 Session-Timeout
28 Idle-Timeout
29 Termination-Action
30 Called-Station-Id
31 Calling-Station-Id
32 NAS-Identifier
33 Proxy-State

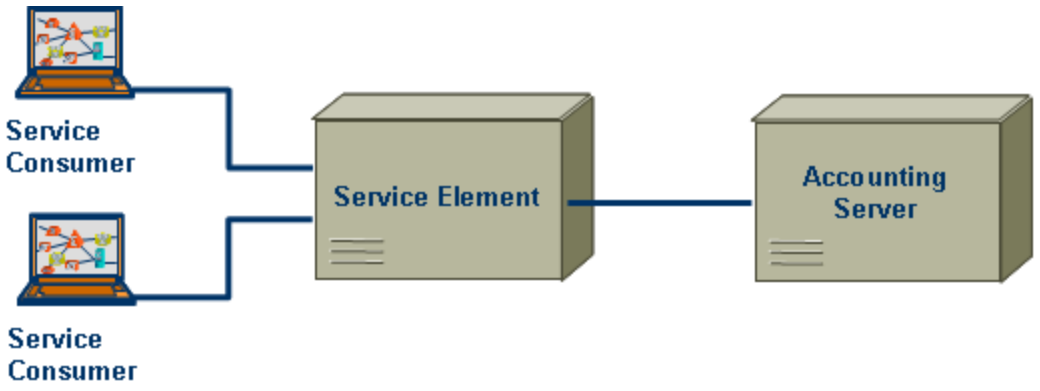
34 Login-LAT-Service
35 Login-LAT-Node
36 Login-LAT-Group
37 Framed-AppleTalk-Link
38 Framed-AppleTalk-Network
39 Framed-AppleTalk-Zone
40 Acct-Status-Type
41 Acct-Delay-Time
42 Acct-Input-Octets
43 Acct-Output-Octets
44 Acct-Session-Id
45 Acct-Authentic
46 Acct-Session-Time
47 Acct-Input-Packets
48 Acct-Output-Packets
49 Acct-Terminate-Cause
50 Acct-Multi-Session-Id
51 Acct-Link-Count
52 Acct-Input-Gigawords
53 Acct-Output-Gigawords
54 Unused
55 Event-Timestamp
60 CHAP-Challenge
61 NAS-Port-Type
62 Port-Limit
63 Login-LAT-Port
64 Tunnel-Type
65 Tunnel-Medium-Type
66 Tunnel-Client-Endpoint
67 Tunnel-Server-Endpoint
68 Acct-Tunnel-Connection
69 Tunnel-Password
70 ARAP-Password
71 ARAP-Features
72 ARAP-Zone-Access
73 ARAP-Security
74 ARAP-Security-Data
75 Password-Retry
76 Prompt
77 Connect-Info
78 Configuration-Token
79 EAP-Message
80 Message-Authenticator
81 Tunnel-Private-Group-ID
82 Tunnel-Assignment-ID
83 Tunnel-Preference
84 ARAP-Challenge-Response
85 Acct-Interim-Interval
87 NAS-Port-Id
88 Framed-Pool
90 Tunnel-Client-Auth-ID
91 Tunnel-Server-Auth-ID

DIAMETER [40]

The DIAMETER framework [41] defines a policy protocol used by clients to perform Policy, AAA and Resource Control allowing a single server to handle policies for many services. DIAMETER defines a base protocol that specifies the header formats, security extensions and requirements as well as a small number of mandatory commands and AVPs.

In the list below attribute numbers which are used for RADIUS attributes but not for DIAMETER are indicated with a star (*). RADIUS attributes used by DIAMETER are not listed again here.

4	(unassigned, *)
17	(unassigned)
21	(unassigned)
24	(unassigned, *)
25	(unassigned, *)
27	(unassigned, *)
32	(unassigned, *)
33	(unassigned, *)
280	Filter-Rule
281	Framed-Password-Policy
480	Accounting-Record-Type
481	ADIF-Record
482	Accounting-Interim-Interval
483	Accounting-Delivery-Max-Batch
484	Accounting-Delivery-Max-Delay
485	Accounting-Record-Number
600	SIP-Sequence
601	SIP-Call-ID
602	SIP-To
603	SIP-From



Accounting Server

A network element that accepts Usage Events from Service Elements. It acts as an interface to back-end rating, billing, and operations support systems.

Service

A type of task that is performed by a Service Element for a Service Consumer.

Service Consumer

Client of a Service Element. End-user of a network service.

Service Element

A network element that provides a service to Service Consumers. Examples include RAS devices, voice and fax gateways, conference bridges.

Figure 5.1.2.6.2.1: Accounting architecture defined by IETF [40]

5.1.2.6.3 3GPP

According to [47] GSM/UMTS networks provide functions that implement offline and/or online charging mechanisms on the:

- bearer (e.g. GPRS);
- subsystem (e.g. IMS); and
- service (e.g. MMS) levels.

In support the network performs real-time monitoring of resource usage on the above three levels in order to detect the relevant chargeable events. The charging levels are further described in clause 5.3.

Offline charging: the resource usage is reported from the network to the Billing Domain after the resource usage has occurred.

Online charging: a subscriber account, located in an online charging system, is queried prior to granting permission to use the requested network resource(s).

[48] enumerates the requirements for charging according to 3GPP.

The following figure shows 3GPP's charging entity relationships for IMS according to [48].

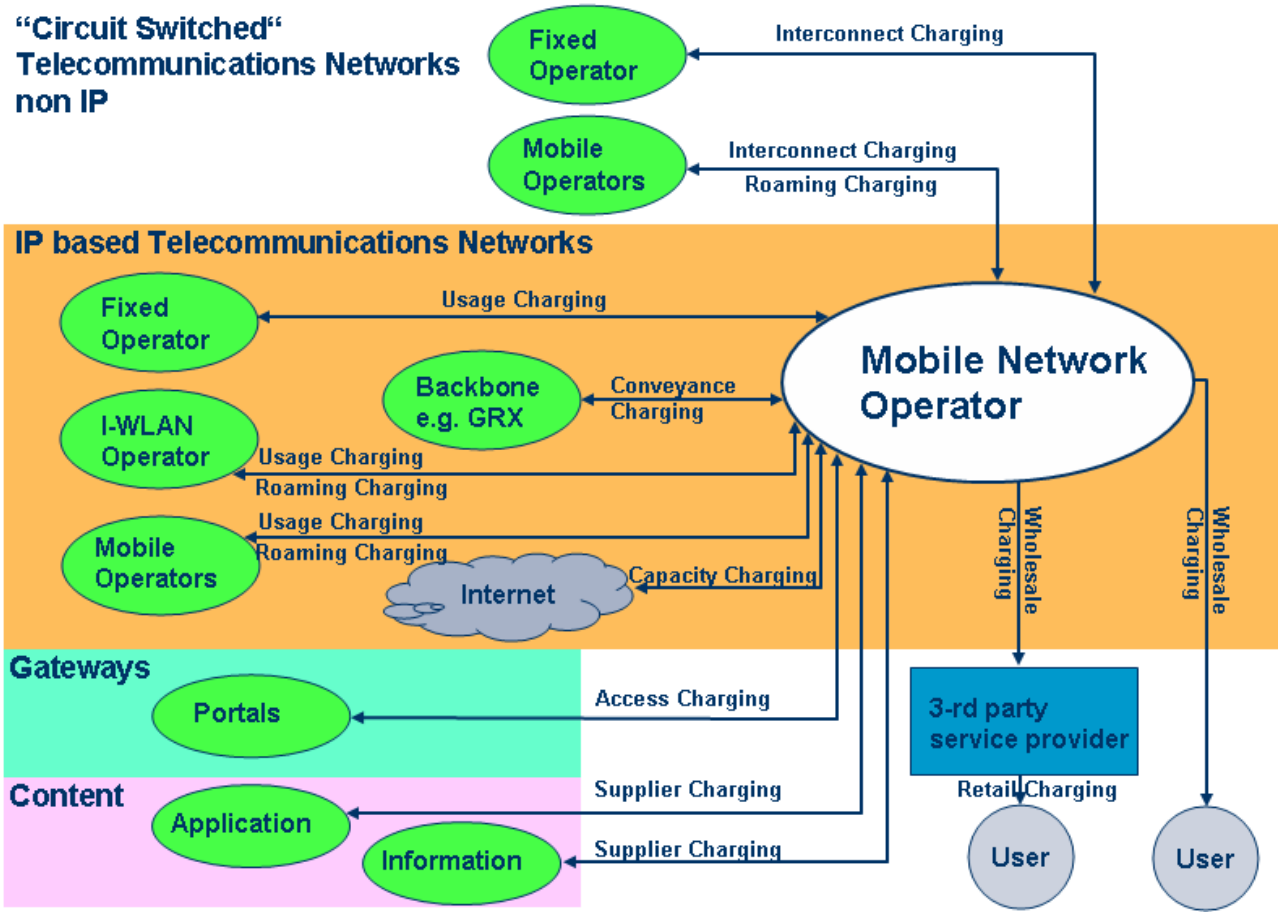


Figure 5.1.2.6.3.1: Charging entity relationship defined by 3GPP [48]

The types of entities and the relevant type of charging as shown in figure 5.1.2.6.3.1 and described in [48] are as follows:

- **Users:** retail charged by Mobile Network Operator or 3rd Party Service Provider.
- **3rd Party Service Providers:** wholesale charged by Mobile Network Operator.

- **Other telecommunications operators:** interconnect charging between Mobile Network Operator and non-IP "circuit-switched" Network Operators for call traffic carried; usage charging between Mobile Network Operator and IP-based Network Operators for session traffic carried.
- **Other mobile operators:** roaming charging between these entities, this may require different mechanisms for IP-based types from the traditional "circuit-switched" types. Also, where mobile operators need to pass traffic to one another, there will be interconnect charging for non-IP "circuit switched" types; usage charging for IP-based types.
- **I-WLAN operators:** where I-WLAN operators need to pass traffic to mobile operators or mobile operators to I-WLAN operators, there may be roaming and usage charging.
- **IP backbone carriers:** conveyance charging Mobile Network Operators for traffic carried.
- **3rd Party content & application suppliers:** supplier charging between Mobile Network Operators and Value Added Service Providers for information exchanged.
- **3rd Party Portals:** access charging between Mobile Network Operators and this entity.
- **Internet:** charge for capacity of connection between Mobile Network Operator and Internet. An Operator pays a provider for a connection based on capacity, e.g. annual charge for a 2Mbit/s "pipe".

According to [48] charging information is collected in the Serving Network to record:

- chargeable User or Mobile Station activity; and
- inter-carrier connections.

This information is partly provided by the user, partly by the network element of the serving network.

Depending on the type of charging information some of the data may not be available or might not be required.

Information provided by the user (user equipment) [48]:

- User identity used for authentication.
- Home environment identity.
- Terminal Identity and Terminal Class.
- Destination endpoint identifier for service requested (e.g. B number).
- Resource requested (e.g. bandwidth, connectionless).
- QoS parameters (e.g. maximum delay).
- IP Multimedia capability requested (e.g. media components).

Information provided by the serving network [48]:

- All of the information listed in clause above (Information provided by the user).
- Serving network identity.
- Recording network element identity.
- Universal Time (UT) at which the service request was initiated.
- Universal Time (UT) at which the resource was allocated to the user.
- Resource allocated to the user.
- Quantity of data transferred both to and from the user.
- QoS provided to the user.

- Location of the user in the standard format used for 3GPP location based services (e.g. geographical co-ordinates, Cell ID).
- whether GSM Optimal Routing was applied.
- If IN or CAMEL services were applied, the service parameters and the actually used destination number and calling party number identification.
- Time duration covered by this charging information to an accuracy of at least 1 second.
- Unique identity of the chargeable event which allows the billing system to correlate all charging information belonging to the same chargeable event.
- Unique charging information identity (unique per network element in a period of about 100 days).
- IP Multimedia capability provided to the user.
- VAS information.
- Identifier of third party accessed by the user.
- Presence Information.
- Service Identification (e.g. voice call, video call, data download, etc.).
- Supplementary Services used.
- Prepay account identifier and related information.

Charged Party [48]:

- Subscription related chargeable events:
  - the charging information shall indicate the charged party (i.e. normally the calling party);
  - alternatively it should be possible to apply reverse charging; or
  - to charge the event to a party not involved in the event itself (e.g. a company as VPN subscriber).
- Inter-network chargeable events:
  - the charging information usually does not contain the charged party, but it can be derived from network configuration information contained in the charging event data.

Information provided by the third party accessed by the user [48]:

Supply of Value Added Services with the aid of third parties typically represented by portals and content/application providers can be charged, if the following charging information is provided by the third party:

- Third party identity.
- Type of service (information, entertainment, gaming, public utility).
- Type of content (picture, video clip, mp3 file, java file).
- Universal Time (UT) at which the service request was initiated.
- Universal Time (UT) at which the service provision was completed.
- Cause for Abnormal reject of the service.
- Universal Time (UT) for abnormal reject of the service.

5.1.2.6.4 OMA

MCC (Mobile Commerce and Charging)

The OMA Charging Enabler [74] enables charging for various types of Chargeable Events to a subscriber's account, possibly maintained by an underlying Charging Infrastructure. It is not a Charging Infrastructure in its own right.

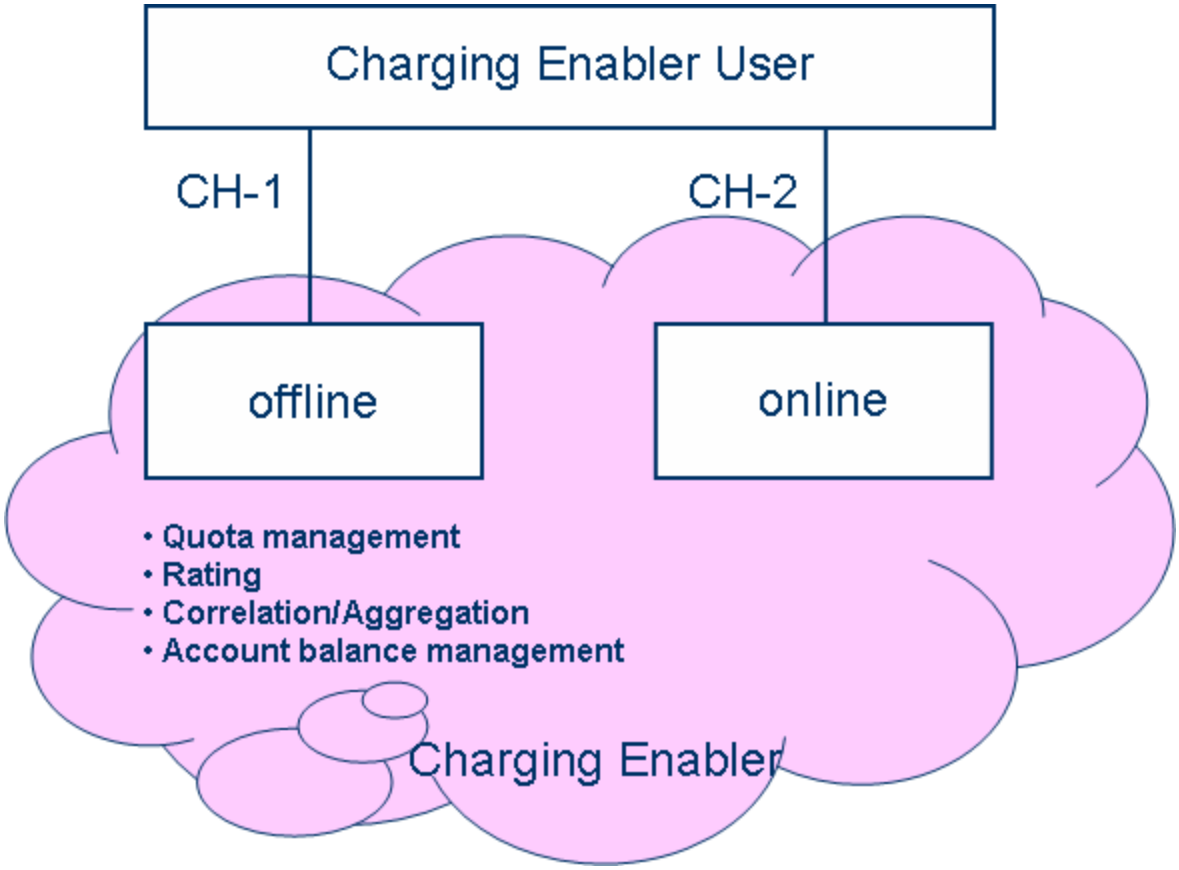


Figure 5.1.2.6.4.1: Charging Enabler Architecture [74]

The Charging Enabler Architecture - shown in the figure above - supports both online and offline charging methods. For either method, any of the charging functions listed below may be applied by the Charging Enabler.

Charging Events are generated by a Charging Enabler User as the result of a user consuming a service. Each event will then be processed and potentially modified by some combination of the following charging functions.

Quota Management

The Quota Management function is responsible for allocating and granting quotas of service usage that a particular user may engage.

A Charging Enabler User that is granted a quota from the Quota Management function is responsible for ensuring that the service usage does not exceed the quota, or in some cases, may request additional quotas.

Correlation/Aggregation

Aggregation is the association of Charging Events generated by the same entity over a period of time.

Correlation could occur between the Charging Events generated by different entities while they are collaboratively providing a single service. The correlation function provides an association of events for the user/application that will be charged.

Rating

This function computes the price or value of a Charging Event indicating a particular action performed by a service.

The rating function receives details of the event to be rated (i.e. the Chargeable Event). The determination of the price or value of the event may be based:

- on one or several attributes of the Charging Event (for example measures of volume, start and end time, or type of service accessed); or
- on other context factors (for example, information related to the account which is to be charged).

Account Balance Management

For Charging Events of a particular subscriber, the Account Balance Management function determines whether credit will be granted for service usage under the following conditions (list not mandatory, nor exhaustive):

- The service provider has enabled the Charging Enabler functionality.
- The subscriber is known to the Charging Enabler instance.
- The subscriber has sufficient credit, and has not exceeded any spending limits configured for him.
- The subscriber has not prohibited the Charging Enabler User that issued the Charging Event (e.g. service barring).
- The subscriber has given an explicit, interactive confirmation (user consent) for the particular request, or has given advance consent to be charged.

The interfaces shown in figure 5.1.2.6.4.1 support the following properties [74].

Offline Charging Interface (CH-1)

This interface is used for offline Charging Event reporting. This interface supports the following functions:

- The sending of Charging Events after service delivery.
- The sending of interim Charging Events during service delivery.
- Correlation.

Online Charging Interface (CH-2)

This interface is used for online charging. This interface supports the following functions:

- Quota requests.
- Renewed quota requests.
- Reporting of portion of unused quota.
- Rating.
- Credit checking.
- Correlation.
- Refunding facility.

According to [75] the charging enabler has to fulfil the following requirements:

When the OMA service layer is controlling the credit, according to [75] it must be able to:

- Accept an expiration time period for the credit acquired. Additional causes for credit expiration could be also provided.

- Accept credit that is shared among the several Service Providers that are involved in providing a service, so the OMA service layer provides credit control coordination for all the parties involved.
- To acquire certain units of time/volume/events as the credit unit:
  - The credit acquired may be referred to service units in this way (i.e. credit for 10 events).
  - Or the credit acquired may be monetary units with a relationship between service units and credit (i.e. 10 monetary-units, the service is 1 monetary-unit/event). The relationship between service units and credit does not imply that monetary units can be converted into money.
- It should be possible to acquire units of different measurements (i.e. volume and time, whichever ends first). This will allow a credit of the type (10 Megs or 5 minutes).

Rating of a service must consider:

- All the elements involved in the delivery of the service, including bearer charges, session charges and event/content charges.
- Specific prices for that event due to bundling, promotions, protected content, rights objects, etc.
- The difference between requested capabilities and those provided (i.e. the user asks for a premium service and he is granted a normal one).
- Account used for the charges.

The charging enabler must support charging input parameters related to the service provided, which affect user/subscriber charges.

The charging enabler must consider three levels for charging:

- Bearer.
- Session.
- Application/Content.

The charging enabler should consider that charging can be done based on:

- Volume (upload, download, a combination of those), time and event.
- Separated charges for each type of medium or service used.
- Each leg of a service independently.
- Technology used to deliver the service, including the QoS requested/used to deliver the service.
- Additional information (location, presence, push services), etc.

The charging enabler shall allow charging customers:

- for obtaining services (e.g. WLAN access time, receiving the "goal of the day as a streamed video, or using a conference bridge); or
- purchasing goods (e.g. weather forecasts or ring tones, protected content or rights objects);

no matter what the nature of the services or goods are.

It shall be possible for the end-user to set limits for:

- accumulated charges;
- volume of transferred data;
- number of events;

etc. per time interval.

It shall be possible for any party to add another media to the current service delivery in progress and any of the parties can be charged for the additional media.

During an active session, media types can change (e.g. audio changed to data) and shall be charged for appropriately.

It shall be possible to charge the end-user according to the service used irrespective of the technology used to deliver it.

It shall be possible to charge the end-user according to the technology used to deliver a service.

The charging enabler must support resolving the account type of the end-user (e.g. if the end-user has a prepaid or a post-paid agreement).

The charging enabler shall support widely used identification mechanisms to identify the customer to the ACE. In particular, the charging enabler should support the following:

- MSISDN: The merchant may automatically determine the customer's MSISDN (if the underlying communication protocol allows so, e.g. if the service being charged for is based on a voice call), or they may ask the customer explicitly to convey the MSISDN as an identity (e.g. in a WLAN scenario).
- Username/PIN[/TAN]: The customer may be requested to manually enter this information.
- IP address: Typically, the IP address is assigned by the ISP to user agent devices. When the ISP also acts as the ACE, the IP address could be used for identifying the customer.
- Account numbers.

Services must be authorized prior to the delivery:

- The service should be authorized in the Service Provider and the ACE (provisioning).
- The user should consent on the service delivery and the payment method (user preferences).
- The user must be authorized to use the service (not blacklisted).
- The authorization can be provided at the same time that the service itself (self-provisioning).

There must be a method to identify uniquely one instance of a service, characterized at least by:

- Service Provider's identifier (i.e. Network Identifier, 3rd Party identifier, etc.).
- Service Identifier.
- User identifier.
- Time and date.

The method will allow a spectator to differentiate between service instances (e.g. to differentiate the same service sent to the same users in different times -download of the same ring-tone twice).

The charging enabler must provide enough information for mechanisms based on Fraud Avoidance and Revenue Assurance to work.

The charging enabler must provide a mechanism to ensure that the service can be provided to the user for the charging perspective prior to the delivery of it:

- It must be possible to assure that the User has given its permission to be delivered the service.
- It must be possible to revocate the permission to deliver a service for charging reasons.
- It must provide Non-repudiation mechanisms to all the interfaces.

The charging enabler shall support subscription based charging.

The information used for charging should be secured by any means available. For the end-user this means

- Authentication of information and senders must be provided.

It must be possible to identify and authenticate all relevant participants involved in a service delivery in order to ensure accurate charging and prevent fraud, e.g.:

- Customer (e.g. a mobile phone user).
- Service Provider.
- Network Operator.
- Device (e.g. a mobile terminal).

It must be possible to use pseudonyms to refer to one user to maintain his privacy:

- In a way that makes it possible for the Third Party to differentiate users (i.e. a unique way hash).

It must be possible for a user to identify anonymously to a Service Provider:

- In a way that identifies an instance of a service to the ACE, allowing only the ACE to identify the user and the account.

The choice of one method of anonymity may depend on user preferences, business agreement, service necessities or other circumstances.

5.1.3 Network Hosted Business Services and Network functions

5.1.3.1 MM Messaging Services (MMS)

5.1.3.1.1 3GPP

According to [49] the MMS shall be able to support the ability to create, update, store, transfer, interrogate, manage and retrieve a user's multimedia messaging profiles.

- Multimedia messaging profiles: allows a user to configure and personalize his multimedia messaging environment with the multimedia messaging profiles:
  - media types (e.g. voice only or text only); and
  - notifications that shall be delivered to the recipient.

The multimedia messaging profiles shall form part of the user's virtual home environment.

- User profile: allows the user to create and manipulate a list of users, identified by their addresses, from which the user does not want to receive messages ("user-level blacklist"). This blacklist differs from ODB blacklist.
- If the MMS supports a network based repository of MMs, it shall be possible for the users to configure where incoming MMs will be stored.

The corresponding network architecture, as described in [50], is shown in figure 5.1.3.1.1.1.

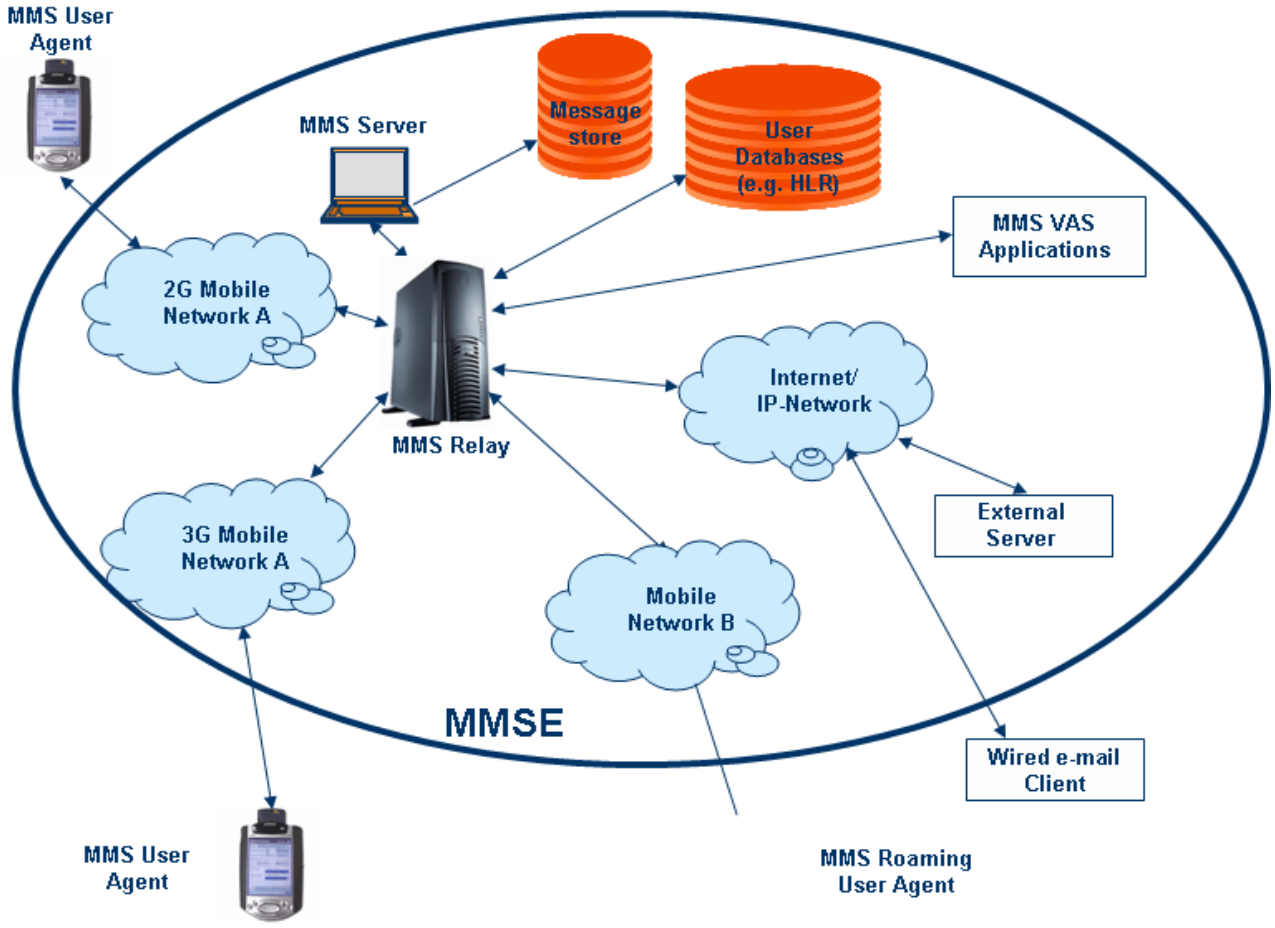


Figure 5.1.3.1.1.1: 3GPP's MMS Network Architecture [50]

MMSNA

According to [50] the Multimedia Messaging Service Network Architecture encompasses all the various elements that provide a complete MMS to a user (including interworking between service providers).

- MMSE: a collection of MMS-specific network elements under the control of a single administration.
- MMS Relay/Server: is responsible for storage and handling of incoming and outgoing messages and for the transfer of messages between different messaging systems.
- The MMS Relay/Server should be able to generate charging data (Charging Data Record - CDR) when receiving MMs from or when delivering MMs to another element of the MMSNA. The MMS Relay/Server should be able to generate charging data for VASP-related operations.
- MMS User Databases: This element may be comprised of one or more entities that contain user related information such as subscription and configuration (e.g. user profile, HLR).
- MMS User Agent: resides on a UE, an MS or on an external device connected to a UE/MS. It is an application layer function that provides the users with the ability to view, compose and handle MMs (e.g. submitting, receiving, deleting of MMs).
- MMS VAS Applications: The MMS VAS Applications offer Value Added Services to MMS users. There could be several MMS VAS Applications included in or connected to an MMSE.

Addressing [50]:

MMS shall support:

- the use of E-Mail addresses (RFC 2822 [105]); or
- MSISDN (E.164); or
- both to address the recipient of an MM.

MMS may support the use of:

- service provider specific addresses to address the recipient of an MM.
  - In the case of E-Mail addresses standard internet message routing should be used.
  - MMS may support short codes to address Value Added Services.

The usage of MSISDN for addressing a recipient in a different MMS service provider's domain shall be possible. For that the need of MSISDN translation to a routable address has been identified.

MMS connectivity across different networks (MMSEs) is provided based on Internet protocols, thus each MMSE should be assigned a unique domain name (e.g. mms.operatora.net).

MMS recipient addresses provided by an MMS User Agent may be in a:

- format of an RFC 2822 [105] routable address, e.g. E-Mail address; or
- other formats, such as:
  - E.164; or
  - service provider specific addresses.

MMS shall support address hiding, i.e. anonymous messages where the sender's address is not shown to the recipient MMS User Agent.

The MMS may have access to several User databases. These may consist of , e.g. user profile database, subscription database, HLR.

These User Databases shall provide:

- MMS user subscription information;
- information for the control of access to the MMS;
- information for the control of the extent of available service capability (e.g. server storage space);
- a set of rules how to handle incoming messages and their delivery;
- information of the current capabilities of the user's terminal.

Figure 5.1.3.1.1.2 shows the MMS reference architecture:

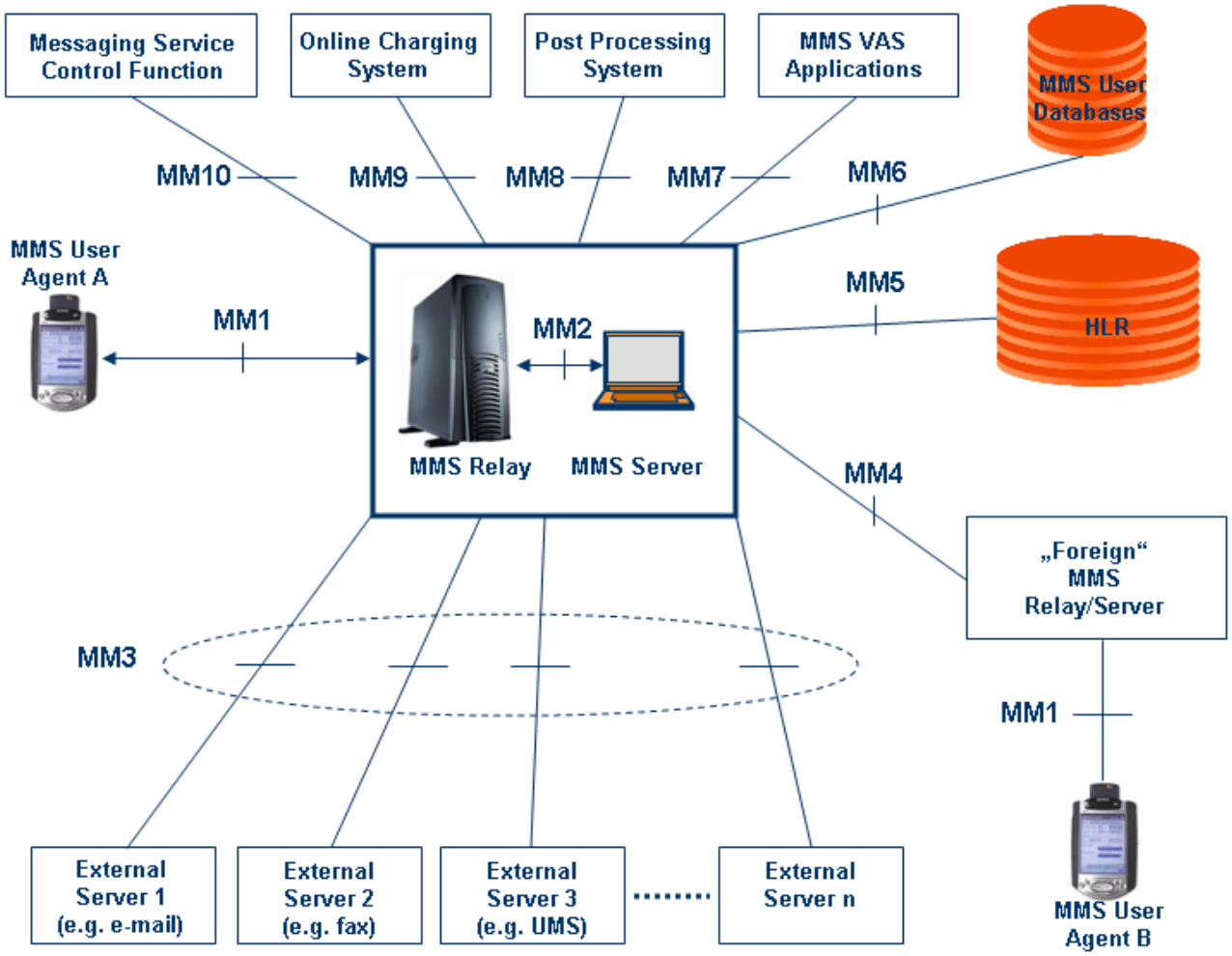


Figure 5.1.3.1.1.2: 3GPP's MMS Reference Architecture [50]

The Reference Architecture defines the following interfaces [50]:

- MM1: The reference point between the MMS User Agent and the MMS Relay/Server.
- MM2: The reference point between the MMS Relay and the MMS Server.
- MM3: The reference point between the MMS Relay/Server and external (legacy) messaging systems.
- MM4: The reference point between the MMS Relay/Server and another MMS Relay/Server that is within another MMSE.
- MM5: The reference point between the MMS Relay/Server and the Home Location Register (HLR).
- MM6: The reference point between the MMS Relay/Server and the MMS User Databases.
- MM7: The reference point between the MMS Relay/Server and MMS VAS Applications.
- MM8: The reference point between the MMS Relay/Server and the post-processing system.
- MM9: The reference point between the MMS Relay/Server and the online charging system.
- MM10: The reference point between the MMS Relay/Server and a Messaging Service Control Function (MSCF).

5.1.3.1.2 3GPP2

[66] defines the requirements for the MMS as a framework enabling non real-time transmission of different types of media content, including:

- Multiple media elements per single message.
- Individual handling of message elements.
- Different delivery methods for each message element.
- Negotiation or accommodation of different terminal and network MM capabilities.
- Notification and acknowledgement of MM related events (e.g. delivery, deletion, etc.).
- Handling of undeliverable MM.
- Personalized MMS configuration.
- Flexible charging.

[66] allows network operators to design and configure networks in different ways (see figure below). On the one hand, the MMS functionality could be implemented within the core network (e.g. Scenarios 1 and 2), on the other hand it may be placed on the periphery of the core network (e.g. Scenario 3 as a centralized network model instead of a distributed architecture). Further, some network operators may wish to support a limited set of MMS functionality, while others may require extensive and elaborate MMS support according to their business models (e.g. basic MMS instead of advanced MMS, Scenario 4). In addition, some network operators may allow a 3rd Party MMS Provider to use their networks for provisioning MMS (e.g. Scenario 5).

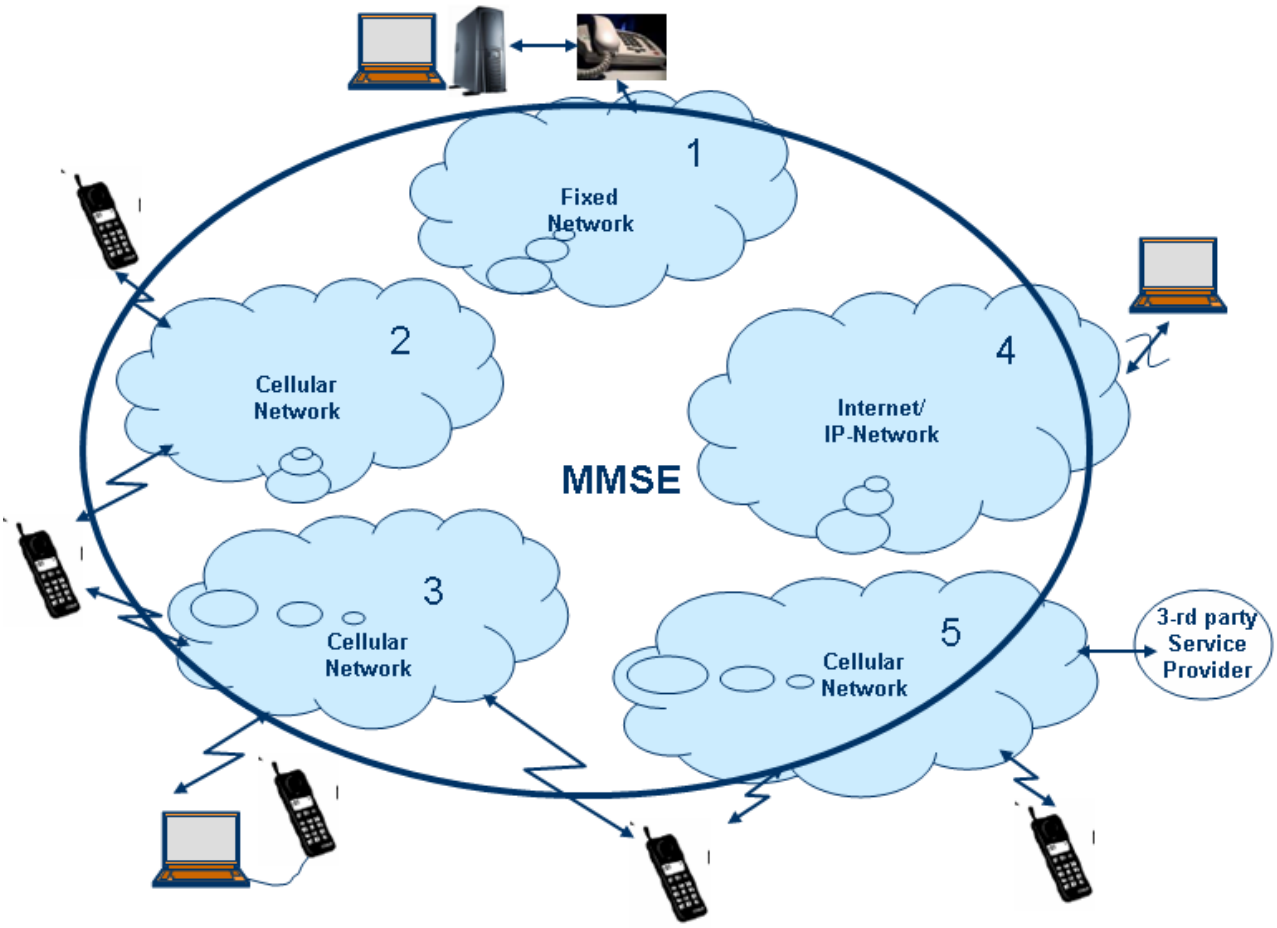


Figure 5.1.3.1.2.1: 3GPP2's MMS Reference Architecture [50]

User Profile Management

According to [15] the MMS shall support the ability to create, update, modify, store, transfer, interrogate, and retrieve a user's multimedia messaging profiles.

Multimedia messaging profiles: allow the user to configure and personalize user's multimedia messaging environment with the multimedia messaging profiles (e.g. which media types and notifications shall be delivered to the recipient, such as voice only or text only).

The MMS profile shall support the user preference for message delivery.

The data that the user is allowed to personalize shall be managed and controlled by the MMS.

Security

The user shall be able to use and access MM in a secure manner.

- It shall be possible for the contents of an MM to be read only by the intended recipient(s).
- A recipient shall be reliably informed of the identity of the sender in case the sender has authorized his identity to be transmitted.
- The MMS shall have the ability to authenticate the user regardless of access technology.
- The MMS shall support data transport in a secure manner between the user and MMS.
- The MMS authentication scheme shall use access specific information.

Addressing:

The MMS shall support different addressing formats to identify the sender and recipient. It shall be possible to submit one message to multiple recipients.

The MMS shall support the capability for both:

- Mobile Directory Number (MDN); and
- e-mail addressing schemes.

to be used, and the user may use either form of addressing to send a message.

The MMS shall be able to support the request to hide the sender's address from the recipient.

5.1.3.1.3 OMA

According to OMA's [72] the Multimedia Messaging Service (MMS) is intended to provide a set of content to subscribers in a messaging context. It supports both sending and receiving of such messages by properly enabled client devices.

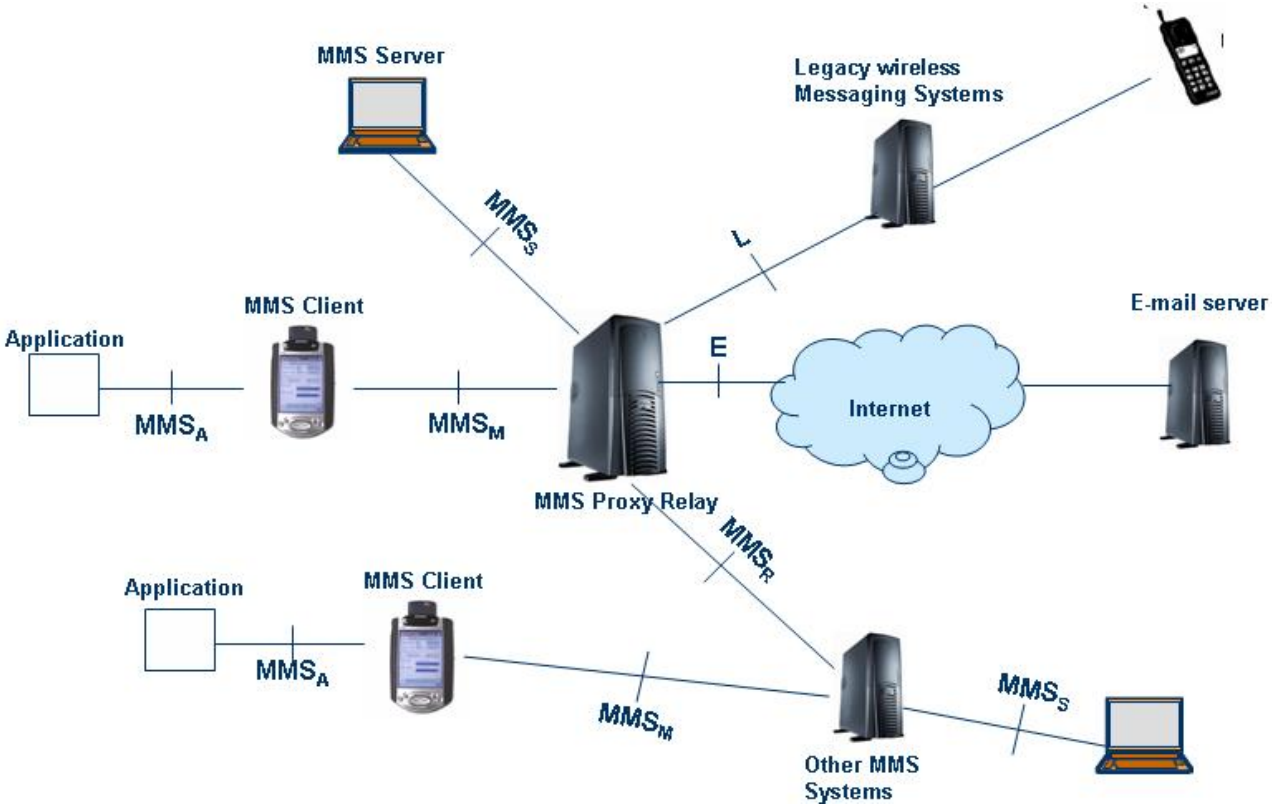


Figure 5.1.3.1.3.1: OMA's MMS Architecture [74]

The following entities are shown in figure 5.1.3.1.3.1:

- MMS Client: This is the system element that interacts with the user (could be implemented as an application on the user's wireless device).
- Application: This system element may interact with the MMS Client in order to transport application specific data via MMS.
- MMS Proxy-Relay: This is the system element, which represents the interface to the MMS Client, provides access to the components that provide message storage services, and it is responsible for messaging activities with other available messaging systems.
- MMS Server: This system element provides storage services for MM messages.
- Email Server: This system element provides traditional Internet email services. supporting the SMTP protocol to send messages as well as POP and/or IMAP protocols to retrieve messages.
- Legacy Wireless Messaging Systems: Represents various systems that currently exist in support of wireless messaging systems (includes paging and SMS systems that provide messaging to a large number of subscribers).

Figure 5.1.3.1.3.1 shows the following interfaces:

- MMS_m: the interface defined between the MMS Client and the MMS Proxy-Relay.
- MMS_S: the interface defined between the MMS Server and the MMS Proxy-Relay. This interface is not defined in the OMA specifications.

- MMS_R: the interface defined between MMS Proxy-Relays of separate MMS Systems. This interface is not defined in the OMA Specifications.
- MMS_A: the interface defined between the MMS Client and an application that may use MMS to transport application specific data, see clause 9. This interface is not defined in the OMA Specifications.
- E: the standard email interface used between the MMS Proxy-Relay and internet-based email systems utilising SMTP, POP and IMAP transport protocols, see clause. This interface is not defined in the OMA Specifications.
- L: the interfaces used between the MMS Proxy-Relay and legacy wireless messaging systems. As there are various such systems, this is viewed as being a set of interfaces. This interface is not defined in the OMA Specifications.

Messaging systems are able to address the users in a way that can be efficient for the system as well as meaningful for the senders of messages. This is described in [72] and [73] as follows:

Internet Addressing

In the Internet world addresses are normally expressed in the email address paradigm. In this scheme, addresses look like user@system where the system specification may be a domain name or a fully qualified host address. In general, this scheme provides users the ability to have a complete and unique address in an unbounded text string [72].

Wireless network addressing

In the wireless world, where bandwidth efficiency is critical, short address lengths and ease of user entry on limited keypads are the hallmarks of the various systems. The MMS addressing model, as defined in [73], makes a more direct or efficient addressing scheme available to MMS subscribers and services. This is seen as particularly important for interoperability with legacy systems such as the above mentioned, and e.g. for mobile-to-mobile operation.

The MMS addressing model contains two addresses:

- the address of the MMS Proxy-Relay: shall be the URI of MMS Proxy-Relay given by the MMS service provider;
- the address of the recipient user and terminal: The addressing model allows only single user in the terminal, thus combining the address of the terminal and the user. The MMS Proxy-Relay has to be able to parse the address formats described below, and it has to be able to determine whether it supports the specified address type or not.

The following is a copy of the description of the MMS addressing model described in [73]:

```
address = ( e-mail / device-address / alphanum-shortcode / num-shortcode)
e-mail = mailbox     ; to the definition of mailbox as described in clause 3.4 of RFC 2822, but
excluding the obsolete definitions as indicated by the "obs-" prefix.
device-address = ( global-phone-number "/TYPE=PLMN" )
/ ( ipv4 "/TYPE=IPv4" )
/ ( ipv6 "/TYPE=IPv6" )
/ ( escaped-value "/TYPE=" address-type )
address-type = 1*address-char
; A network bearer address type
address-char = ( ALPHA / DIGIT / "_" )
escaped-value = 1*( safe-char )
; the actual value escaped to use only safe characters by replacing
; any unsafe-octet with its hex-escape
safe-char = ALPHA / DIGIT / "+" / "-" / "." / "%" / "_"
unsafe-octet = %x00-2A / %x2C / %x2F / %x3A-40 / %x5B-60 / %x7B-FF
hex-escape = "%" 2HEXDIG ; value of octet as hexadecimal value
global-phone-number = ["+"] 1*( DIGIT / written-sep )
written-sep =("-"/".")
ipv4 = 1*3DIGIT 3( "." 1*3DIGIT ) ; IPv4 address value
ipv6 = 4HEXDIG 7( ":" 4HEXDIG ) ; IPv6 address per RFC 2373
num-shortcode = [ ( "+" /  "*" / "#") ] 1*DIGIT
alphanum-shortcode = 1*(ALPHA / DIGIT)
```

Each value of a user-defined-identifier is a sequence of arbitrary octets. They can be safely embedded in this address syntax only by escaping potentially offending values. The conversion to escaped-value is done by replacing each instance of unsafe-octet by a hex-escape which encodes the numeric value of the octet.

Some examples of the mechanism:

To: 0401234567/TYPE=PLMN

To: +358501234567/TYPE=PLMN

To: Joe User <joe@user.org>

To: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210/TYPE=IPv6

To: 195.153.199.30/TYPE=IPv4

The terminal has to support at least one of the addressing methods.

5.1.3.2 Content Services

5.1.3.2.1 Digital Right Management (DRM)

5.1.3.2.1.1 3GPP

3GPP states in [51] that DRM specifications are elaborated in the Open Mobile Alliance (OMA) according to an agreement between 3GPP and OMA.

5.1.3.2.1.2 OMA

According to OMA [51] Digital Rights Management (DRM) supports the distribution of content in order to enable business models whereby the consumption and use of content is controlled. As such, DRM allows managing the content lifecycle. When a user buys content, she may agree to certain constraints - for example by choosing between a free preview version or a full version at cost, or she may agree to pay a monthly fee. DRM allows this choice to be translated into permissions and constraints, which are then enforced when the user accesses the content.

In the OMA DRM architecture [51]:

- functional entities (logical and need not represent physical network nodes) are used to embody specific roles in the DRM system; and
- an actor is defined as an external entity involved in carrying out use cases. Depending on deployment scenario, different actors can play different roles in the system.

From the point of view of digital rights management, the following functional entities have been identified in the architecture (see also figure 5.1.3.2.1.2.1):

- DRM Agent.
- A DRM Agent, a trusted entity in a device, is responsible for enforcing permissions and constraints associated with DRM Content, controlling access to DRM Content, etc.
- Content Issuer.
- The content issuer is an entity that delivers DRM Content according to the format of DRM Content and the way DRM Content can be transported from a content issuer to a DRM Agent defined by OMA.
- Rights Issuer.
- The rights issuer is an entity that assigns permissions and constraints to DRM Content, and generates Rights Objects (XML document expressing permissions and constraints associated with a piece of DRM Content).
- User.
- A user is the human user of DRM Content. Users can only access DRM Content through a DRM Agent.
- Off-device Storage.

According to [51] DRM Content is inherently secure, and may be stored by users off-device - for example in a network store, a PC, on removable media or similar. This may be used for backup purposes, to free up memory in a device, and so on. Similarly, Rights Objects that only contain stateless permissions may be stored off-device.

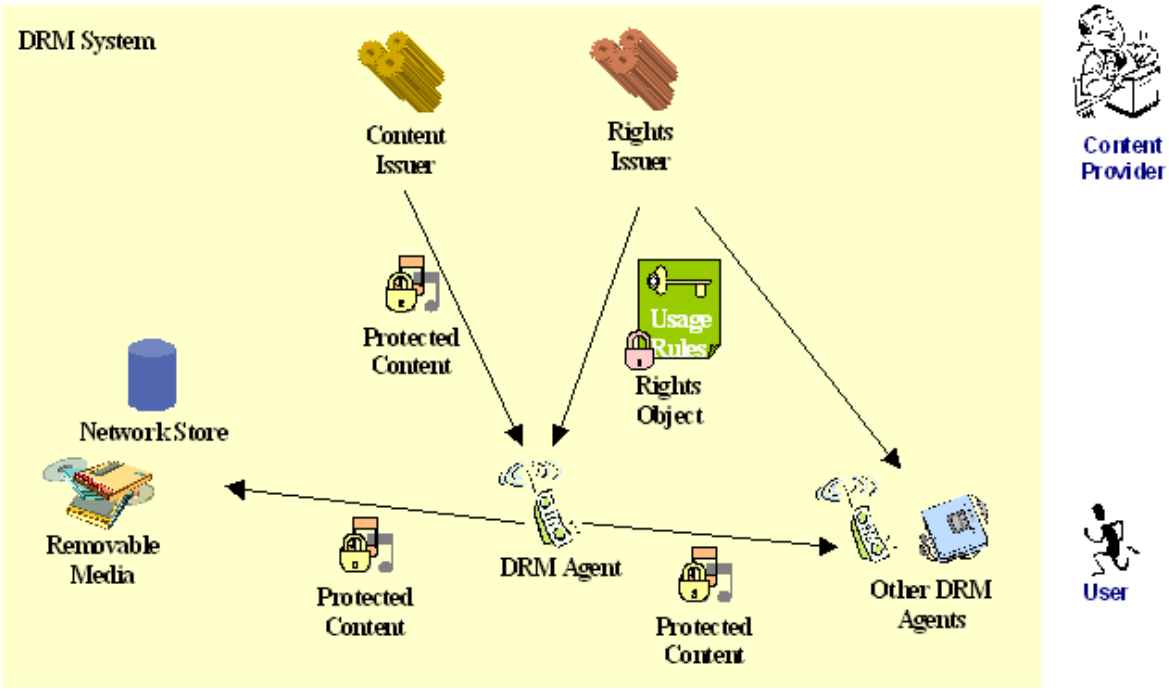


Figure 5.1.3.2.1.2.1: OMA's DRM Architecture [51]

5.1.3.2.2 Mobile Broadcast (BCAST)

5.1.3.2.2.1 3GPP

According to [18] the MBMS is an unidirectional point to multipoint bearer service in which data is transmitted from a single source entity to multiple recipients.

MBMS also enables an IMS application located on an application server to send multimedia to a set of IMS users in the service area by means of MBMS bearer service.

3GPP has defined two modes of operation [52]:

- The broadcast mode: unidirectional point-to-multipoint transmission of multimedia data (e.g. text, audio, picture, video) from a single source entity to all users in a broadcast service area.
- The multicast mode: allows the unidirectional point-to-multipoint transmission of multimedia data (e.g. text, audio, picture, video) from a single source point to a multicast group in a multicast service area.

In [53] the following requirements on an application level are listed:

- Service classes:
  In case of roaming a user shall be able to enjoy services as follows:
  - A user shall be able to activate services that are provided locally in the visited network, as allowed by the user's home environment (e.g. local tourist information).
  - A user subscribed to a service class in the HPLMN shall be able to enjoy equivalent services in the same service class as provided by a visited PLMN without explicit subscription in the VPLMN (e.g. weather forecast).
  - A user subscribed to a service class in the HPLMN shall be able to have access to home contents provided via a visited PLMN without explicit subscription in the VPLMN (e.g. enjoy subscribed service while roaming).
- Service Interworking:
  - The user shall be able to manipulate content delivered over MBMS and forward it using other services (e.g. MMS, Speech Call- and IMS signalling, Hyperlinks, etc.).
  - When interacting with user profiles, MBMS User Services shall use the mechanisms described in [54] (Generic User Profile).
- Content storage in the UE:
  - It shall be possible for the UE to store content delivered to it over MBMS and provide it to the user at a later time.
- Data formats and types:
  - Media types shall be supported independent of specific data types and formats.

  As a minimum MBMS User Services shall support the following media types:
  - Text.

  It shall be possible to embed hyperlinks and to decorate text within content provided by MBMS User Services.
  - Still Images.
  - Video.
  - Speech.
  - Mono/Stereo Audio.

  Data formats and types used by other multimedia services shall be supported for interoperability reasons.
- Digital Rights Management:
  - The MBMS User Service shall be able to control content distribution and MBMS content providers shall be able to invoke DRM to prevent unauthorized copying and forwarding of content.
- Notification of required capabilities:
  - The capabilities (e.g. memory size) required to receive a particular transmission shall be notified in advance by the network or service centre.

[53] defines the following user service requirements for MBMS:

- Charging:
  - The MBMS User Service shall support standardized mechanisms to transfer charging related information.
    - Charging on a subscription basis.

    - Charging for keys that that allow the user access to the data.

  - It shall be possible to charge for MBMS content the user receives while roaming in a VPLMN.

  - Some services will require an indication that MBMS content has been received. Therefore it shall be possible for the UE to provide such an indication.

- Security:

  - Any user modifiable MBMS service data (e.g. storage of deliveries in the UE, data type and format specific behaviours etc) shall only be modified by the authenticated user.

- Privacy:

  - Third parties and VASP should not be aware about user IDs for MBMS subscriptions unless explicitly allowed by the operator.

- Quality of Service:

  - It should be possible for the operator to collect statistical data such as lost frames, assigned resources, bit-rates achieved, etc.

  - It shall be possible for the operator to adapt the distribution of a MBMS user service consisting of different MBMS transport services to provide multiple QoS levels according to the QoS resources provided by the access network(s).

  - It shall be possible to base the adaptation of the distribution of a MBMS user service to the QoS resources provided by the access network(s) on:

    - the QoS resources within the same access network (e.g. UTRAN).

    - the QoS resources provided by different access networks (e.g. UTRAN and GERAN).

  - It shall be possible to adapt the distribution of an ongoing MBMS user service to persistently changed QoS resource conditions in the access network(s).

  - Adaptation of the distribution of a MBMS user service to the QoS resources in different access networks or parts of the same access network shall not affect the QoS of the MBMS user service in other access networks or other parts of the same access network.

- Subscription:

  - During the lifetime of subscription to a Multicast Service it shall be possible for the user to declare the service preferences. It shall be possible for the network to store the user settings.

- Availability:

  - The user should be able to receive MBMS user services via generic IP access systems.

5.1.3.2.2.2 OMA

The term "Mobile Broadcast" in [76] refers to a broad range of Broadcast Services,

- which jointly leverage:

  - the unidirectional one-to-many broadcast paradigm; and

  - the bi-directional unicast paradigm in a mobile environment; and

- covers one-to-many services ranging from classical broadcast to mobile multicast.

The Mobile Broadcast Services Enabler addresses functional areas:

- which are generic enough to be common to many Broadcast Services:

  - Service Guide;

- File Distribution;
- Stream Distribution;
- Service Protection;
- Content Protection;
- Service Interaction;
- Service Provisioning;
- Terminal Provisioning; and
- Notification.

- and which can be defined and implemented in a bearer-independent way.

In [76] all technologies proposed upon which this enabler is specified are:

- either based on open standards; or
- will become part of an open standard.

The purpose of the top-level BCAST architecture [76]:

- It puts the BCAST Enabler in the context of underlying Broadcast Distribution Systems (BDS), service operation and content provisioning.
- It defines the logical entities and their relations.

Figure 5.1.3.2.2.2.1 gives an idea of the functions and the protocol stack of OMA's BCAST.

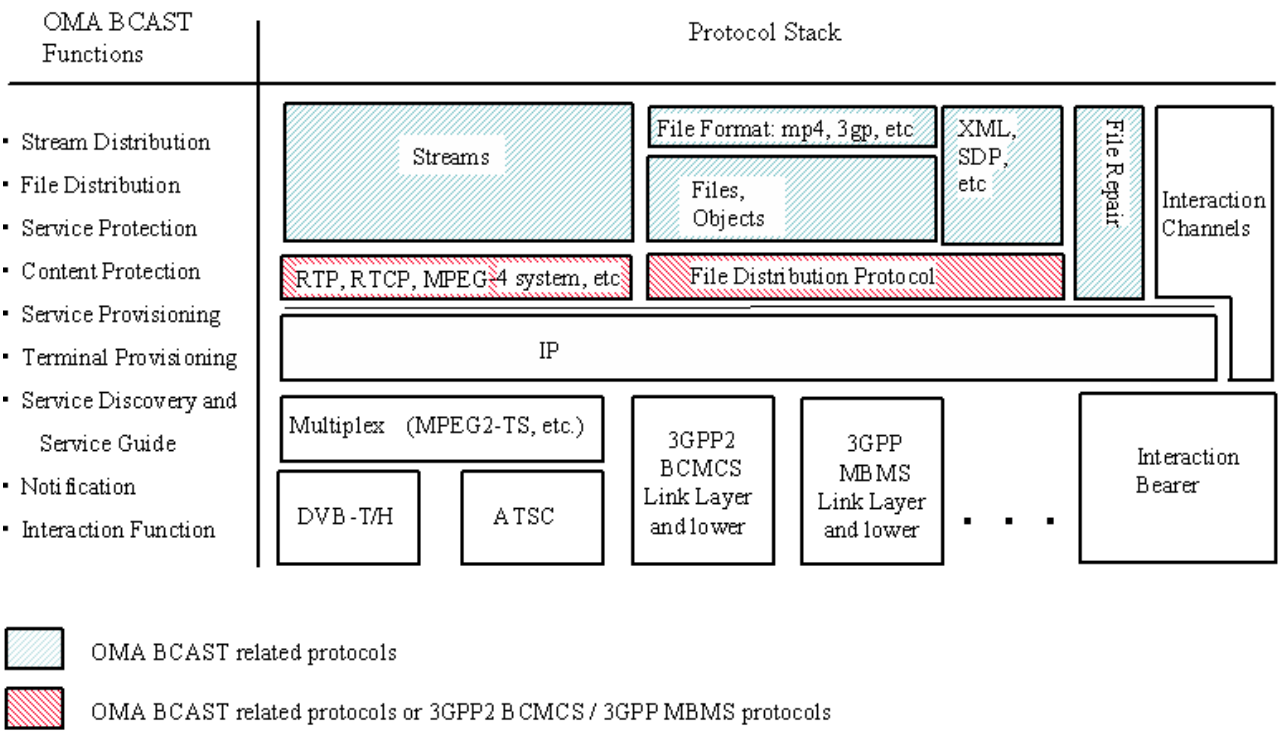


Figure 5.1.3.2.2.2.1: OMA's BCAST functions and protocol stack [76]

Figure 5.1.3.2.2.2.1 shows the OMA BCAST functions and with what protocol stack they would generally be realized. Such protocols may include:

- 3GPP MBMS protocols; or

- 3GPP2 BCMCS.

The lower layers include one-way and two-way directional bearers; hence the BCAST enabler functions might behave differently with different types of bearers.

The BCAST enabler architecture involves the following collection of logical entities over a set of reference points:

- Service Guide.
- Streaming Distribution.
- File Distribution.
- Service Protection.
- Content Protection.
- Service Provisioning.
- Terminal Provisioning.
- Interaction and Notification functions.

These functions are located in the different BCAST logical entities shown in figure 5.1.3.2.2.2.2.

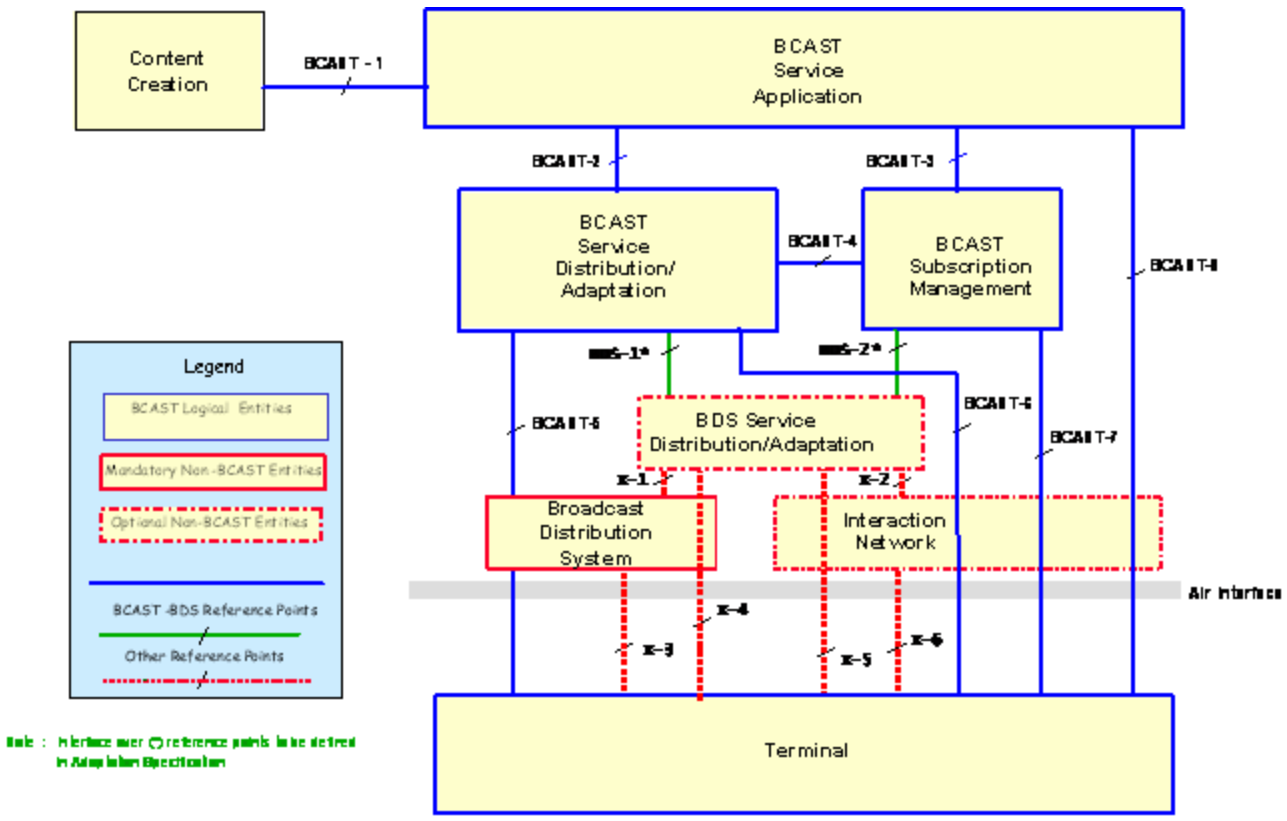


Figure 5.1.3.2.2.2.2: OMA's BCAST functional architecture [76]

Functions in OMA's BCAST architecture:

- BCAST Service Application: Represents the service application of the BCAST Service, such as, streaming audio/video or movie file download. It encompasses the functionality of:
  - media encoding;
  - content protection; and
  - interaction related to BCAST Service.

It also provides the BCAST service attributes to the BCAST Service Distribution/Adaptation and BCAST Subscription Management.

It may generate charging information.

- BCAST Service Distribution/Adaptation: Responsible for the aggregation and delivery of BCAST Services, and performs the adaptation of the BCAST Enabler to underlying Broadcast Distribution Systems. It provides the functionality of:
  - File and Stream Distribution;
  - Service Aggregation;
  - Service Protection;
  - Service Guide generation and delivery;
  - Notification Delivery; and
  - the adaptation to the underlying BDS.
- BCAST Subscription Management: Responsible for service provisioning such as subscription and payment related functions, the provision of information used for BCAST Service reception, and BCAST Terminal management.

  It provides the functionality of:
  - Notification;
  - Service Protection management;
  - Content Protection management;
  - Service Guide generation support;
  - Terminal Provisioning; and
  - interaction with the BDS Service Distribution to communicate/manage subscription information with the Terminal.

  It may send the user charging information to the BCAST service application:
- Terminal: The user device that receives broadcast content as well as the BCAST service related information, such as, service guide, content protection information.
- Content Creation: Source of content, may provide support for delivery paradigms (e.g. streaming servers); provides base material for content descriptions.
- BDS Service Distribution: Responsible for the coordination and delivery of broadcast services to the BDS for delivery to the terminal, including file and stream distribution, and Service Guide distribution. It may also include key distribution, broadcast subscription management, and accounting functionalities.
- Broadcast Distribution System: Specific support for the distribution of content over the broadcast channel. This may involve the same or different radio network from that used by the interactive channel.
- Interaction Network: Specific support for the interaction channel. This may involve the same or a different radio network from that used by the broadcast channel.

Interfaces in OMA's BCAST architecture:

- BCAST-1: Used for Content, Content attributes, notification event, etc.
- BCAST-2: Used for Content-unprotected and/or content-protected BCAST Service, BCAST Service attributes and content attributes pertaining to the program such as description, rating and genre.

- BCAST-3: Used for BCAST Service attributes and content attributes pertaining to service provisioning such as targeted user profile and location information. User preference and subscription information, User request, User reporting, notification event and maybe user charging information.
- BCAST-4: Used for Notification, Service Guide, fragments (related to provisioning, purchasing, subscription, terminal provisioning, etc.), Service keys, Terminal Provisioning object, Terminal Provisioning message, Terminal management message, etc.
- BCAST-5: Used for unprotected and/or protected BCAST Service, content-unprotected and/or content-protected BCAST Service, BCAST Service attributes and content attributes, Notification, Service Guide, Security material, all distributed over the Broadcast Distribution System.
- BCAST-6: Used for unprotected and/or protected BCAST Service, content-unprotected and/or content-protected BCAST Service, BCAST Service attributes and content attributes, Notification, Service Guide, Security material, terminal reports related to stream and file delivery, all distributed over the Interaction Network.
- BCAST-7: Used for Service provisioning, Subscription information, Terminal provisioning, Security material and device registration.
- BCAST-8: Used for User interaction, reporting, and user preference.
- BDS-1: Used for unprotected and/or protected BCAST Service, content-unprotected and/or content-protected BCAST Service, BCAST Service attributes and Content attributes, Notification, Service Guide and Security material.
- BDS-2: Used for Service provisioning, Subscription information, Device management, Security material.
- X-1: Used for Reference Point between BDS Service Distribution and BDS.
- X-2: Used for Reference Point between BDS Service Distribution and Interaction Network.
- X-3: Used for Reference Point between BDS and Terminal.
- X-4: Used for Reference Point between BDS Service Distribution and Terminal over Broadcast Channel.
- X-5: Used for Reference Point between BDS Service Distribution and Terminal over Interaction Channel.
- X-6: Used for Reference Point between Interaction Network and Terminal.

5.1.3.2.3 Dynamic Content Delivery (DCD)

5.1.3.2.3.1 OMA

The Dynamic Content Delivery (DCD) Enabler [77] is expected to enhance a mobile user's experience through the periodic delivery of personalized or customized content to a device. The content may be based on the subscription and preferences of the user, operator or service provider. It is intended to be a complementary delivery mechanism to the existing mechanisms (e.g. browsing, messaging, etc.) and provide the added benefits of:

- delivery control management; and
- an enhanced user experience.

The following figure describes the overall system of the DCD Enabler.

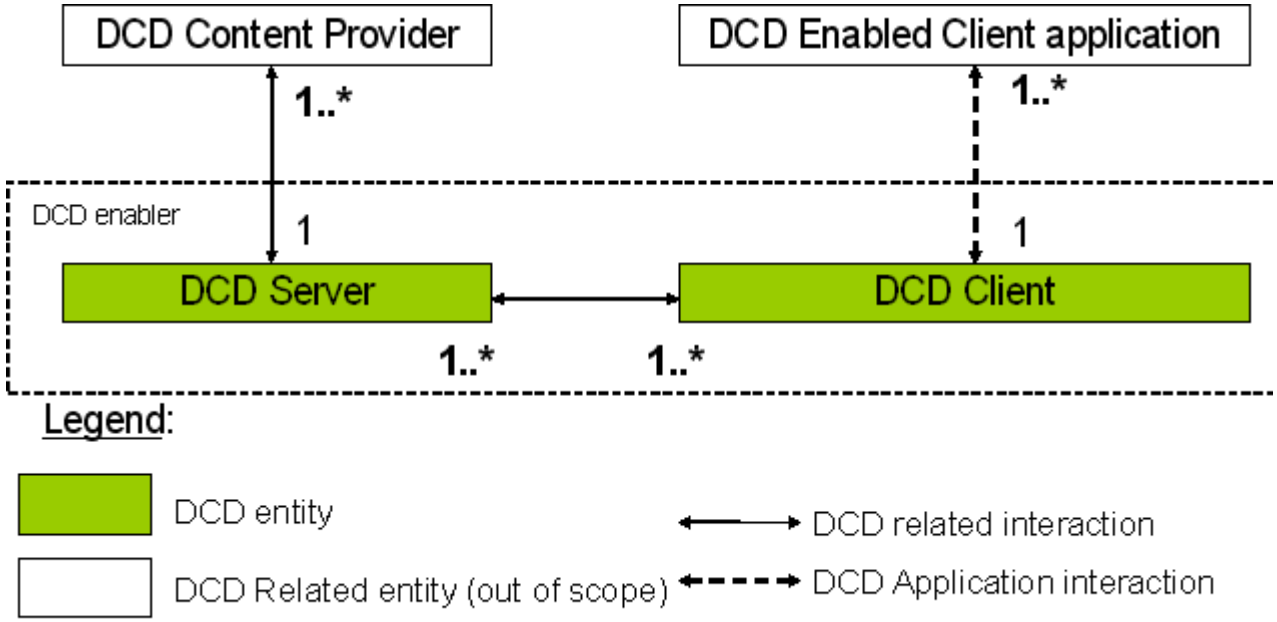


Figure 5.1.3.2.3.1.1: OMA's DCD overall picture [77]

DCD-Enabled Client Application: receives the content from a network server for rendering on the mobile device. This application enables the user:

- to interact with the content;
- initiate requests for more detailed content;
- subscribe to additional content channels; and
- launch other applications.

The DCD Client: acts as an agent that enables the DCD functionality on the handset and serves one or more DCD-Enabled Client Application(s).

The DCD Enabler enables an application and its delivery to be enhanced by making it available asynchronously and through automatic means. By way of example, with a service based on DCD, users may subscribe to services that:

- provide continually updated news;
- weather;
- traffic; or
- financial information, all of which could be personalized for the user.

These services could be tied to a user's location in order to increase the value of the content to the user. Such a service may support delivery of the DCD Content to the user no matter which mobile device is used through awareness of the user's identity, e.g. such as that stored on a smart card.

According to [77] the DCD Enabler's primarily responsibilities are for establishment and management of arrangements for periodic / on-demand content delivery between a DCD Server and a DCD-Enabled Client Application. These responsibilities integrate with, but are not limited to, the key functions of:

- Content (channel) selection / subscription;
- Content personalization and customization;
- Content storage management;
- Content charging.

The scope of personalization and customization for the DCD Enabler [78] includes the ability to control specific DCD Enabler functions based upon user profile attributes. The user profile attributes are determined from external enablers (e.g. presence and location), or managed by the DCD Enabler as data specifically related to DCD operation. Those specifically related to DCD operation include:

- statically applicable preferences which can be used for service customization;
- dynamically applicable preferences (based upon dynamically determined user profile attributes), usable for service personalization.

The following preferences are defined in [78], derived from the requirements in [77]:

- Per-channel static preferences:
  - Subscription: whether the user is given access to this channel, which includes filtering of channels in the broadcast case.
  - Delivery schedule: TTL setting for content items that are periodically updated, time-to-refresh, time of day, etc.
  - Storage space usage: minimum / maximum content storage space for the channel.
  - Manual suspension: whether delivery for the channel is currently manually suspended.
  - Automatic suspension schedule: day / time-of-day during which content delivery is suspended.
- Per-channel dynamic preferences:
  - Deliver when roaming: this conditions delivery (i.e. deliver or do not deliver) upon the user's roaming status.
  - Deliver based upon current location: this conditions delivery upon the user's location being inside a perimeter.
  - Deliver based upon Presence attribute: this conditions delivery upon the value of a specific attribute value provided by a Presence Service.

Application Profile Handling allows the DCD Client to handle the delivery of the DCD Content for a particular DCD-Enabled Client Application according to its Application Profile. The Application Profile and its Channel Metadata include, but are not limited to, the following elements:

- Application-ID: identifies the type of application, as a unique identifier for the purpose of interoperability and content routing.
- Content Packaging Format: e.g. ATOM, RSS, CDF, etc.
- Channel Management Attributes: allow the DCD Client to handle the channels in the way appropriate for this application.
- Content Storage Management Attributes: allow this type of applications to request specific content storage options or actions provided by the content storage of DCD Client, e.g.:
  - Content storage allocation and reservation in DCD Client.
  - Content retention policies in the content storage of DCD Client.

- Content Category / Type (e.g. MIME Type(s) or arbitrary string like "rss/finance/stock-quotes") to identify the types of content requested in this channel.

Data Handling and Delivery Rules - specify the static definitions and rules for representing the channel and delivering the channel content to the application, e.g. DCD Content and the Content Metadata / Schema for this channel.

5.1.3.3 IMS Application Servers

5.1.3.3.1 3GPP/3GPP2

Application servers (AS) host and execute services, and interface with the S-CSCF using SIP. This allows third party providers an easy integration and deployment of their value added services to the IMS infrastructure. Examples of services are:

- Caller ID related services (CLIP, CLIR, etc.).
- Call waiting, Call holding, Push to talk.
- Call forwarding, Call transfer.
- Call blocking services, Malicious Caller Identification.
- Lawful interception.
- Announcement services.
- Conference call services.
- Voicemail, Text-to-speech, Speech-to-text.
- Location based services.
- SMS, MMS.
- Presence information, Instant messaging.

Depending on the actual service, the AS can operate in SIP proxy mode, SIP US (user agent) mode or SIP B2BUA (back-to-back user agent) mode. An AS can be located in the home network or in an external third-party network. If located in the home network, it can query the HSS with the DIAMETER Sh interface (for SIP-AS and OSA-SCS) or the MAP interface (for IM-SSF) [56].

- SIP AS: native IMS application server.
- OSA-SCS an Open Service Access - Service Capability Server interfaces with OSA Application Servers using Parlay.
- IM-SSF: an IP Multimedia Service Switching Function interfaces with CAMEL Application Servers using CAP.

The architecture is based on the principle that the service control for Home subscribed services for a roaming subscriber is in the Home network (e.g. the Serving-CSCF is located in the Home network).

There are two possible scenarios to provide services (see figure 5.1.3.3.1.1):

- via the service platform in the Home Network;
- via an external service platform.

The external service platform entity could be located in either the visited network or in the 3rd party platform. The standardized way for secure 3rd party access to IMS services is via the OSA framework as described in [56].

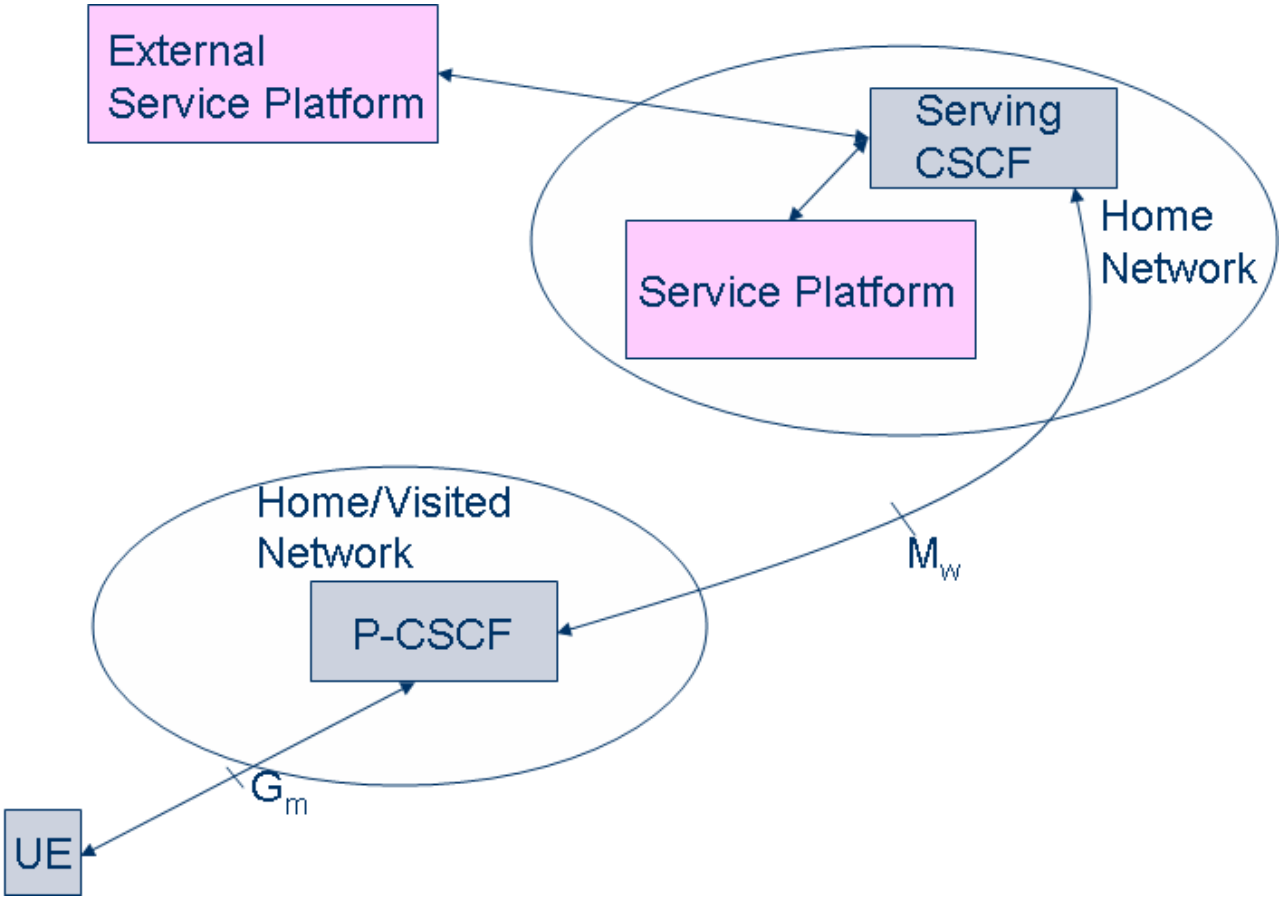


Figure 5.1.3.3.1.1: Locations of service platforms

An Application Server (AS) offering value added IM services resides either in the user's home network or in a third party location. The third party could be a network or simply a stand-alone AS.

The Serving-CSCF to AS interface is used to provide services residing in an AS. Two cases were identified:

- Serving-CSCF to an AS in Home Network.
- Serving-CSCF to an AS in External Network (e.g. Third Party or Visited).

The SIP Application Server may host and execute services. The SIP Application Server can influence and impact the SIP session on behalf of the services and it uses the ISC interface to communicate with the S-CSCF.

The ISC interface shall be able support subscription to event notifications between the Application Server and S-CSCF to allow the Application Server to be notified of the implicit registered Public User Identities, registration state and UE capabilities and characteristics in terms of SIP User Agent capabilities and characteristics.

The S-CSCF shall decide whether an Application Server is required to receive information related to an incoming initial SIP request to ensure appropriate service handling. The decision at the S-CSCF is based on (filter) information received from the HSS. This filter information is stored and conveyed on a per Application Server basis for each user. The name(s)/address(es) information of the Application Server (s) are received from the HSS.

From the perspective of the S-CSCF, The "SIP Application server", "OSA service capability server" and "IM-SSF" shall exhibit the same interface behaviour.

When the name/address of more than one Application Server is transferred from the HSS, the S-CSCF shall contact the Application Servers in the order supplied by the HSS. The response from the first Application Server shall be used as the input to the second Application Server. Note that these multiple Application Servers may be any combination of the SIP Application server, OSA service capability server, or IM-SSF types.

The S-CSCF does not provide authentication and security functionality for secure direct third party access to the IM subsystem. The OSA framework provides a standardized way for third party secure access to the IM subsystem.

If a S-CSCF receives a SIP request on the ISC interface that was originated by an Application Server destined to a user served by that S-CSCF, then the S-CSCF shall treat the request as a terminating request to that user and provide the terminating request functionality as described above. Both registered and unregistered terminating requests shall be supported.

It shall be possible for an Application Server to generate SIP requests and dialogs on behalf of users. Such requests are forwarded to the S-CSCF serving the user, and the S-CSCF shall perform regular originating procedures for these requests.

Originating requests on behalf of registered and unregistered users shall be supported.

The Application Server (SIP Application Server and/or the OSA service capability server and/or IM-SSF) may communicate to the HSS. The S_h and S_i interfaces are used for this purpose.

For the S_h interface, the following shall apply:

1) The S_h interface is an intra-operator interface.

2) The S_h interface is between the HSS and the "SIP Application Server" and between the HSS and the "OSA service capability server". The HSS is responsible for policing what information will be provided to each individual Application Server.

3) The S_h interface transports transparent data for e.g. service related data, user related information, etc.
In this case, the term transparent implies that the exact representation of the information is not understood by the HSS or the protocol.

4) The S_h interface also supports mechanisms for transfer of user related data stored in the HSS (e.g. user service related data, MSISDN, visited network capabilities, user location (cell global ID/SAI or the address of the serving network element, etc.)).

   Before providing information relating to the location of the user to a SIP Application Server, detailed privacy checks frequently need to be performed. The SIP Application Server can ensure that these privacy requirements are met by using the L_e interface to the GMLC instead of using the S_h interface.

5) The S_h interface also supports mechanisms for transfer of standardized data, e.g. for group lists, which can be accessed by different Application Servers. Those Application Servers sharing the data shall understand the data format. This enables sharing of common information between Application Servers, e.g. data managed via the Ut reference point.

The S_i interface is between the HSS and the IM-SSF. It transports CAMEL subscription information including triggers for use by CAMEL based application services.

According to [56] users are identified in the following way:

- Private User Identities: Every IM CN subsystem user shall have one or more Private User Identities assigned by the home network operator (used e.g. for Registration, Authorization, Administration, and Accounting purposes). This identity shall take the form of a Network Access Identifier (NAI) as defined in RFC 2486 [106]. It is possible for a representation of the IMSI to be contained within the NAI for the private identity.
  - The Private User Identity is not used for routing of SIP messages.
  - The Private User Identity shall be contained in all Registration requests passed from the UE to the home network.
  - An ISIM application shall securely store one Private User Identity. It shall not be possible for the UE to modify the Private User Identity information stored on the ISIM application.
  - The Private User Identity is a unique global identity defined by the Home Network Operator, which may be used within the home network to identify the user's subscription (e.g. IM service capability) from a network perspective. The Private User Identity identifies the subscription, not the user.
  - The Private User Identity shall be permanently allocated to a user's subscription (it is not a dynamic identity), and is valid for the duration of the user's subscription with the home network.
  - The Private User Identity is used to identify the user's information (for example authentication information) stored within the HSS (for use for example during Registration).
  - The Private User Identity may be present in charging records based on operator policies.
  - The Private User Identity is authenticated only during registration of the user, (including re-registration and de-registration).
  - The HSS needs to store the Private User Identity.
  - The S-CSCF needs to obtain and store the Private User Identity upon registration and unregistered termination.
- Every IM CN subsystem user shall have one or more Public User Identities (see 3GPP TS 22.228 [107]). The Public User Identity/identities are used by any user for requesting communications to other users.
  - Both telecom numbering and Internet naming schemes can be used to address users depending on the Public User identities that the users have.
  - The Public User Identity/identities shall take the form of a SIP URI (as defined in RFC 3261 and RFC 2396) or the "tel:"-URI format RFC 3966 [108].
  - An ISIM application shall securely store at least one Public User Identity (it shall not be possible for the UE to modify the Public User Identity), but it is not required that all additional Public User Identities be stored on the ISIM application.
  - A Public User Identity shall be registered either explicitly or implicitly before originating IMS sessions and originating IMS session unrelated procedures can be established by a UE using the Public User Identity.
  - It shall be possible to identify Public User Identities of a user that are linked to the same service profile and have the exact same service configuration for each and every service (i.e. "alias" Public User Identities). For such a group of Public User Identities, operations that enable changes to the service profile shall apply to all the Public User Identities within the group. This grouping information shall be made available to the HSS, AS, and UE. The information about the Public User Identities of the users that are linked to the same service profile shall be able to be provisioned in the HSS. It shall be possible to make this information available to the AS via the S_h interface, and that S_h operations are applicable to all of the IMPUs within the same service profile. It shall be possible to make this information available to the UE via the G_m interface.
  - A Public User Identity shall be registered either explicitly or implicitly before terminating IMS sessions and terminating IMS session unrelated procedures can be delivered to the UE of the user that the Public User Identity belongs to.

- It shall be possible to register globally (i.e. through one single UE request) a user that has more than one public identity via a mechanism within the IP multimedia CN subsystem (e.g. by using an Implicit Registration Set). This shall not preclude the user from registering individually some of his/her public identities if needed.

- Public User Identities are not authenticated by the network during registration.

- Public User Identities may be used to identify the user's information within the HSS (for example, during mobile terminated session set-up).

IMS group management concepts:

- The U_t reference point is used to manage groups from the UE. This does not preclude the use of other mechanisms for group management, e.g. using OSA or OA&M mechanisms.

- The U_t reference point shall support a scenario where one single Application Server (sometimes referred to as a Group and List Management Server - GLMS) is used to create groups that can be utilized for different services, possibly hosted by different ASes.

- Each group shall be addressable by a globally unique group identifier. The group identifier shall take the form of a Public Service Identifier.

5.1.3.3.2 OMA

The IMS Service Provisioning Architecture standardized by 3GPP/3GPP2, allows applications to access capabilities of the IMS. It provides two options for service provisioning, namely SIP-Application Server and OSA Gateway. IMS provides service-enabling functions and IP transport and is therefore relevant to the OMA Service Environment (OSE).

Applications may use OMA enablers or may use IMS functions directly or both.

In the OSE, OMA enabler implementations may make use of IMS capabilities, e.g. charging, authentication, service management, etc. IMS related applications/enablers can use OSE capabilities in addition to IMS capabilities.

The only IMS interfaces an OMA enabler may use are the following:

- ISC interface: The ISC interface is between the enabler server implementation and the IMS core. The ISC interface provides the OMA service enabler with SIP/SDP call control, SIP event related subscription and notification, SIP messaging, etc.

- S_h interface: The S_h interface is between the enabler server implementation and HSS in the IMS core. The S_h interface provides the OMA service enabler with read and write operations of user data related to IMS. It also provides with functionality for subscription and notification of changes in the user data related to IMS. The protocol used on the S_h interface is DIAMETER.

- D_h interface: The D_h interface is between the enabler server implementation and the Service Locator Function (SLF) in IMS core. The D_h interface is quite similar to the Sh interface and is used by the enabler implementations to get the address of the HSS that handles a particular user in networks, where there are several HSS. The protocol used on the D_h interface is DIAMETER.

- U_t interface: The U_t interface is between the enabler implementation in the terminal and the enabler server implementation. The U_t interface provides the UE with a set of operations that allow configuring user specific data in the OMA service enabler servers. The user specific data comprises, but it is not restricted to configuration management, such as configuration of presence lists and presence authorization rules. The protocol used on the U_t interface is being specified in 3GPP and is based on XCAP.

- R_o interface: The R_o interface provides the OMA service enabler with an event based charging interface to the online charging system in the IMS core. The protocol used on the Ro interface is DIAMETER.

- R_f interface: The R_f interface provides the OMA service enabler with an interface to the off-line charging system in the IMS core. The protocol used on the R_f interface is DIAMETER.

- G_m interface: The G_m interface is between the enabler implementation in the terminal and the IMS core. The G_m interface provides the OMA service enabler with SIP/SDP call control, SIP event related subscription and notification, SIP messaging, etc.

- M_b interface: The M_b interface provides the OMA service enabler with user plane packet media streams over IP via the IMS core.

In order to be able to utilize services built on IMS the enabler terminal implementation (ETI~UE) shall support the following main features in addition to SIP:

- AKA authentication within REGISTER;
- security mechanism agreement for SIP within REGISTER;
- IPsec based on AKA and on the security mechanism agreement for SIP.

In order to connect an enabler server implementation (ESI~AS) to IMS to offer services the ESI shall support the following main features in addition to SIP:

- charging using the received information from IMS;
- at least one of the modes: UAC, UAS and proxy;
- two types of third party call control when acting as a B2BUA.

IMS defines and uses several private header (P-header) extensions to SIP. The following P-headers are visible both in ETI and ESI (the corresponding terms UE and AS are used below):

- P-Access-Network-Info (carries information of the access network from UE to IMS and from IMS to ASes; visible only to trusted AS).
- P-Asserted-Identity.
- P-Called-Party-ID (carries the target public user identity from IMS to UE). The P-Called-Party-ID header field may be seen at the AS when the AS is the called party (i.e. the destination of the session), but not in other scenarios (e.g. when the AS is just a proxy in the chain of proxies in the path towards a UE).
- P-Charging-Vector.
- P-Charging-Function-Addresses.

The following P-headers are visible only in UE, but not in AS:

- P-Associated-URI (carries associated URIs to the registered Public user identity from IMS to UE).
- P-Media-Authorization (carries media authorization token from IMS to UE).
- P-Preferred-Identity (carries identity preferred by the user from UE to IMS).

The following P-headers are visible in AS, but not in UE:

- P-Asserted-Identity (carries valid and authenticated Public user identity from IMS to AS).
- P-Charging-Vector (carries charging correlation information from IMS to AS).
- P-Charging-Function-Addresses (carries offline and online charging function addresses from IMS to AS).

The Home Subscriber Server is the master database for a given user. It is the entity containing the subscription-related information to support the network entities actually handling sessions. The HSS is responsible storing the data for authenticating and authorizing the subscriber.

5.1.3.4 Store and Forward Messaging

5.1.3.4.1 Instant Messaging (IM)

5.1.3.4.1.1 OMA

Instant Messaging (IM) as described in [80] is a concept known in both the mobile and desktop worlds. Desktop IM clients, two-way SMS and two-way paging are all forms of Instant Messaging. Wireless Village IM will enable interoperable mobile IM in concert with other innovative features to provide an enhanced user experience.

Groups or chat are familiar concepts on the Internet. Both operators and end-users are able to create and manage groups. Users can invite their friends and family to chat in group discussions. Operators can build common interest groups where end-users can meet each other online.

Shared Content allows users and operators to setup their own storage area where they can post pictures, music and other multimedia content while enabling the sharing with other individuals and groups in an IM or chat session.

The following figure shows the basic architecture of the IM framework [80].

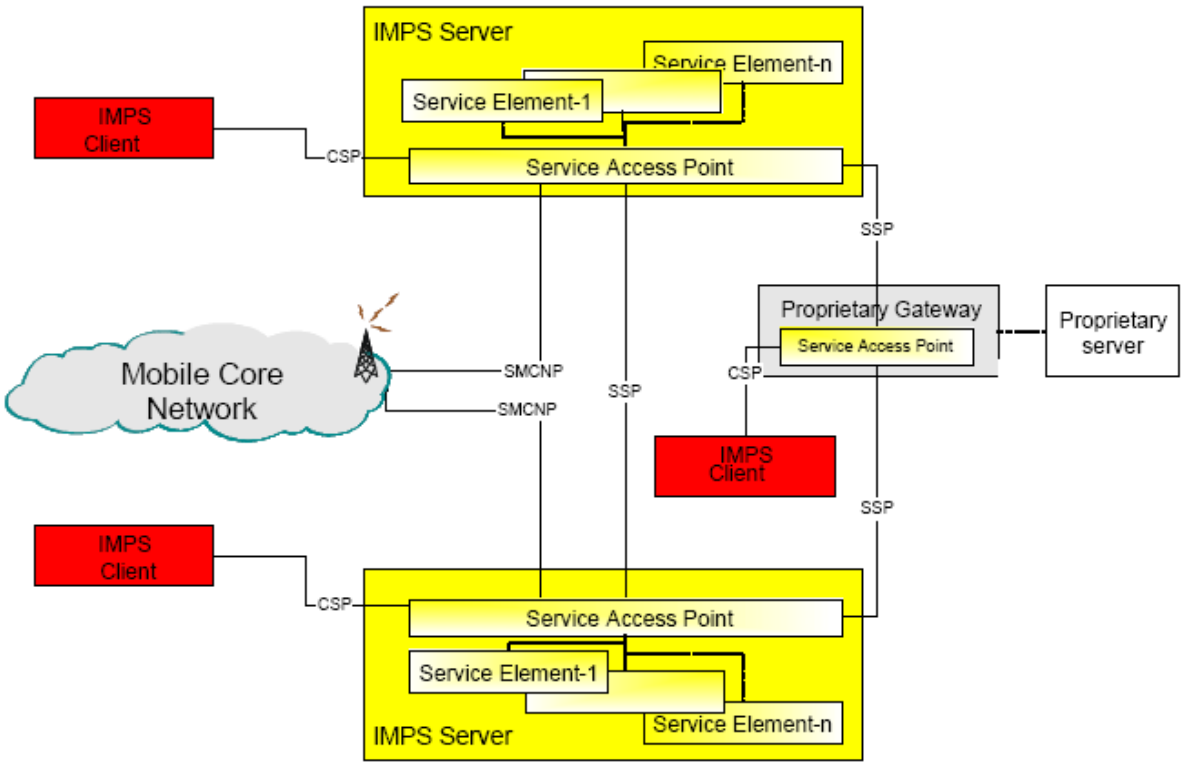


Figure 5.1.3.4.1.1.1: Architecture of OMA's IM

IMPS Server: central point in an IMPS system, composed of four Application Service Elements that are accessible via the Service Access Point:

- Presence Service Element: provides functionality for presence information management. This includes update, retrieve, set and store presence and location information. Presence information can be manipulated implicitly by the system, or explicitly by the user (for details see clause about presence).
- Instant Messaging Service Element: provides functionality for sending and receiving instant messages. An instant message may be sent to, or received from, a specific IMPS-user, or users of other instant messaging systems. It is also possible to send instant messages to a group of IMPS-users. IMPS supports several message types such as plain text, video, picture and sound.

- Group Service Element: provides functionality for use and management of groups. The groups can be private or public. A common usage of the Group Service is a chat room. It is also possible to bind content to the Groups.

- Content Service Element: provides functionality for sharing content such as images and documents between IMPS users. This allows the IMPS users to share content while sending messages or chatting in a group. In this IMPS enabler, the shared content is realized by allowing a user to send a URL of the content he or she is willing to share. There are no mechanisms to upload or download content.

Service Access Point (SAP): serves as the interface between the IMPS server and its environment. It has interfaces to the IMPS clients, other IMPS servers, the Mobile Core Network and Proprietary Gateways to non-IMPS servers. The functionality of the Service Access Point is:

- Authentication and Authorization: Authentication is used to verify the identity of an entity (user, network, or application). Authorization is the activity of determining what an authenticated entity (user, network, or application) is allowed to do. There are several types of mechanisms for authentication and authorization:

  - Application-Network Authentication / Authorization.

  - User-Application Authentication / Authorization.

  - Application-Application Authentication / Authorization.

  - User-Network Authentication (only for Authentication).

- Service Discovery and Service Agreement: Service Discovery enables the application to identify the collection of service capability features that it can use. The service discovery process includes service capability registration and service capability notification. This is done both between Client - Server and Server -Server. A Service Agreement (also known as a Service negotiation) must be established before the server can interact with the Network Service Capability or other servers' service capabilities, and provides the client with the services.

- User Profile Management: One or more User Profile(s) describe(s) how the user wishes to manage and interact with their communication services (Figure below). The User Profile information consists of various user interfaces and service related information including the list of services to which the end-user is subscribed, preferences associated with those services, service status (active / inactive), privacy status with regards to network service capabilities (e.g. user location, user interaction), terminal capabilities and terminal interface preferences etc. User Profile Management allows the application to retrieve and update the user profile.

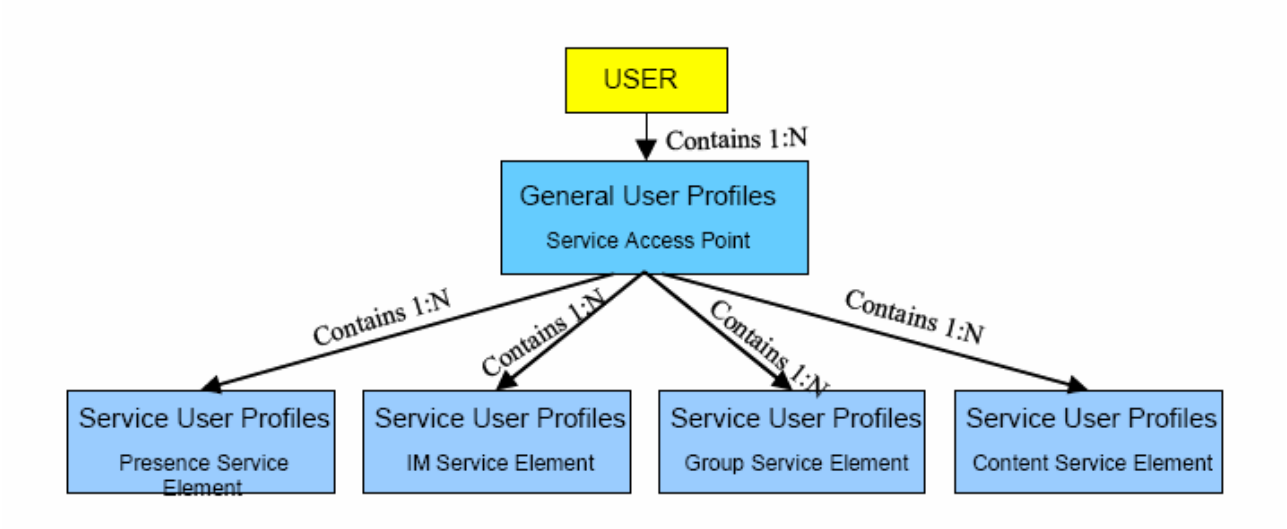


Figure 5.1.3.4.1.1.2: OMA's IM User Profile Management [80]

- Service Relay: The Service Access Point must provide the Service Relay function to route all service requests and responses among the servers using the Server-to-Server Protocol (SSP). The Service Relay requires that the SAP performs CSP to SSP conversion and may have to transcode the contents of a service request and response.

5.1.3.5 P2P and Group Communication

5.1.3.5.1 Push To Talk Over Cellular (PoC)

5.1.3.5.1.1 3GPP

According to [57] it is assumed that the PoC architecture makes use of the following IMS capabilities in the 3GPP system:

- Registration;
- IMS routing capabilities, including discovery and address resolution;
- IMS security including authentication and authorization;
- IMS charging;
- SIP compression;
- IMS group management;
- Public service identities;
- Presence Service.

PoC as a service is introduced as an application within the frame of the IP Multimedia Subsystem (IMS). Figure 5.1.3.5.1.1.1 illustrates how the PoC service elements fit into the IMS architecture.

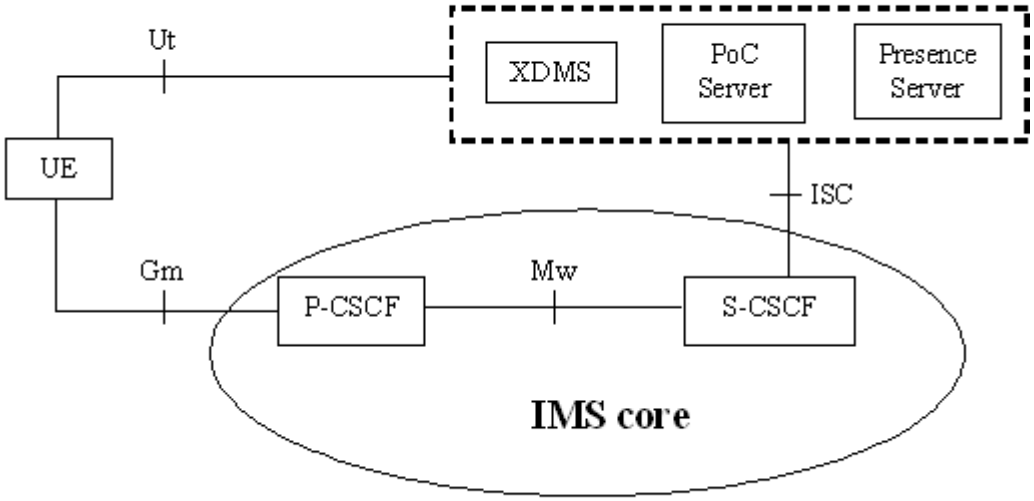


Figure 5.1.3.5.1.1.1: 3GPP's PoC Architecture [57]

The PoC server implementing the application level network functionality for the PoC service is essentially seen as an Application Server from the IMS perspective. Consequently, communications between the IMS core and the PoC server utilize the ISC interface defined in TS 23.228 [56].

The XML Document Management Server (XDMS) is used by the PoC users to manage groups and lists (e.g. contact and access lists) that are needed for the PoC service. In the IMS architecture, the Ut interface provides these functions, hence communications between the XDMS and the UE utilize the Ut interface.

A Presence Server may provide availability information about PoC users to other PoC users.

5.1.3.5.1.2 OMA

Push to talk over Cellular (PoC) provides rapid communications for business and consumer customers of mobile networks. PoC allows user voice and data communications shared with a single recipient, (1-to-1) or between groups of recipients as in a group chat session (1-to-many).

OMA-PoC seeks interoperability among the network entities to avoid market fragmentation, by realizing the PoC service in a widely acceptable and standardized manner. The figure below describes the functional entities and reference points that are involved in the support of the PoC service.

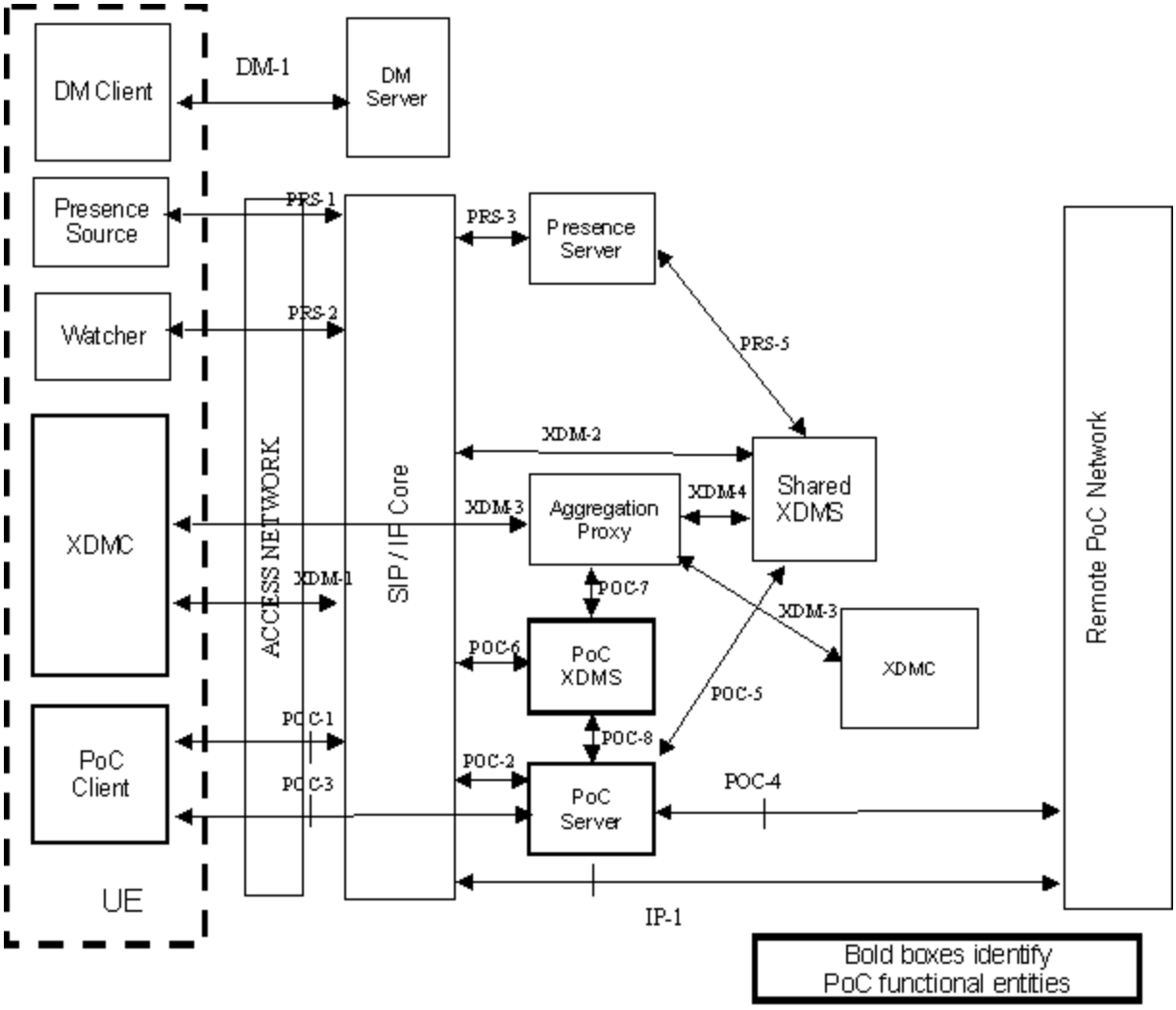


Figure 5.1.3.5.1.2.1: OMA's PoC Architecture [81]

The POC-1 reference point supports the communication between the PoC Client and the SIP/IP Core using SIP.

This reference point shall support the following:

- PoC Session signalling between the PoC Client and the PoC Server.
- Provides discovery and address resolution services.
- Provides SIP compression.
- Performs authentication and authorization of the PoC User at the PoC Client based on the PoC User's service profile.
- Provides PoC Client registration.
- Indication of capabilities for PoC.

- Relaying PoC Service Settings (Answer Mode Indication, Incoming PoC Session Barring, Incoming Instant Personal Alert Barring, and Simultaneous PoC Sessions Support) to the PoC Server.
- Provides the integrity protection and optionally the confidentiality protection of the PoC Session signalling.

The POC-5 reference point supports communication between the Shared XDMS and the PoC Server using XCAP.

The POC-5 reference point provides the following functions:

- Retrieval of URI Lists from the Shared XDMS.

The POC-6 reference point supports communication between the PoC XDM Server and the SIP/IP Core. The protocol for the POC-6 reference point is SIP.

The POC-6 reference point provides the following functions:

- Subscription to the modification of PoC-specific XML documents.
- Notification of the modification of PoC-specific XML documents.

The POC-7 reference point supports communication between the Aggregation Proxy and the PoC XDM Server using XCAP.

The POC-7 reference point provides the following functions:

- PoC-specific XML document management (e.g. create, modify, retrieve, delete).

Identification

- PoC Address: Each PoC User shall have one or more PoC Addresses either in the format of a SIP URI or a TEL URI. At least one PoC Address has to be in the format of a SIP URI. The PoC Address SHALL comply either with the specification of a SIP URI, or with the specification of a TEL URI.

  Examples of PoC Addresses are:

  - sip:joe.doe@operator.net;
  - sip:buss2.city@operator.net;
  - sip:buss2.city@poc.operator.net;
  - tel:+16195551212;
  - tel:5551212; phone-context = pbx.net.

- Private User identity: When the SIP/IP Core corresponds with 3GPP/3GPP2 IMS, the private User identity shall be used as described above.
- PoC Group Identities: A PoC Group is identified with a PoC Group Identity. The PoC Client uses PoC Group Identities for addressing PoC Group Sessions. The PoC Group Identity is associated with individual PoC Addresses of all the PoC Group members. The PoC Group Identity shall take the form of SIP URI.

  - An operator shall be able to create a static Group identity which is stored in the PoC XDMS for use in PoC Group Sessions.
  - A PoC User shall be able to create a PoC Group which is stored in the PoC XDMS for use in PoC Group Sessions.
  - The PoC User shall be able to create and store a Group List in the Shared XDMS as a URI list.

Addressing

- Phone numbers: maybe used as a user public identity. A PoC User may address another PoC User by a phone number. The PoC Client shall send the phone number to the SIP/IP Core in a TEL URI.

The phone number MAY use the international E.164] format (prefixed with a '+' sign), or a local format. The SIP Core shall interpret the phone number with a leading '+' to be an E.164 number.

- SIP URI: A PoC User may address another PoC User, Pre-arranged PoC Groups and Chat PoC Groups by a SIP URI.

Identification of inviting PoC User

The PoC Server shall maintain the PoC Address of the inviting PoC User used in the originating request (SIP URI, TEL URI, Nick Name or combination SIP URI + Nick Name). The PoC Server shall identify the Groups by SIP URI and MAY identify them by Nick Name.

In the case of a PoC Group Session the PoC Server shall provide the PoC Group Identity to the invited PoC Client(s).

The home PoC Server shall replace the Nick Name provided by the inviting PoC Client, if the Nick Name is configured in the home PoC Server of the inviting PoC User.

Talker Identification

To provide the PoC Address and Nick Name of the Participant who has been permitted to send a Talk Burst to all listening Participants in the PoC Session the PoC Server shall support Talker Identification.

Registration

General

Prior to using the PoC service the UE hosting the PoC Client shall perform SIP registration to the SIP/IP Core, which indicates the support of PoC service in the REGISTER request. The registration function is provided in the SIP/IP Core and the registration/deregistration may be visible to the PoC Server via the POC-2 reference point. After a successful registration a PoC User is able to use a registered PoC Address:

- to originate PoC communication including session and session unrelated procedures;
- to receive PoC communication including session and session unrelated procedures.

When the SIP/IP Core corresponds with 3GPP/3GPP2 IMS then it is possible for the network on behalf of PoC UE to register additional PoC Addresses during a SIP registration of a single PoC Address. Registering multiple PoC Addresses at once is called implicit registration. The PoC Address that is used in the registration shall be SIP URI while the PoC Addresses to be registered implicitly may be SIP URIs or TEL URIs.

5.1.3.6 Data Synchronization

5.1.3.6.1 OMA

With the emergence of mobile computing and communications devices, users have access to their personal or professional information and applications, from multiple places (home, work, travel, etc.) and devices (mobile phones, PDA, computers, network, etc.). As the information they want may not always be on the device they carry, and they cannot be permanently connected to network to access their data, the OMA DS Enabler [82] provides a common data synchronization framework and XML-based format, or representation protocol, for synchronizing data on networked devices. The OMA DS Enabler is designed for use between mobile devices that are intermittently connected to the network and network services that are continuously available on the network. The OMA DS Enabler is specifically designed to handle the case where the network services and the device store the data they are synchronizing in different formats or use different software systems.

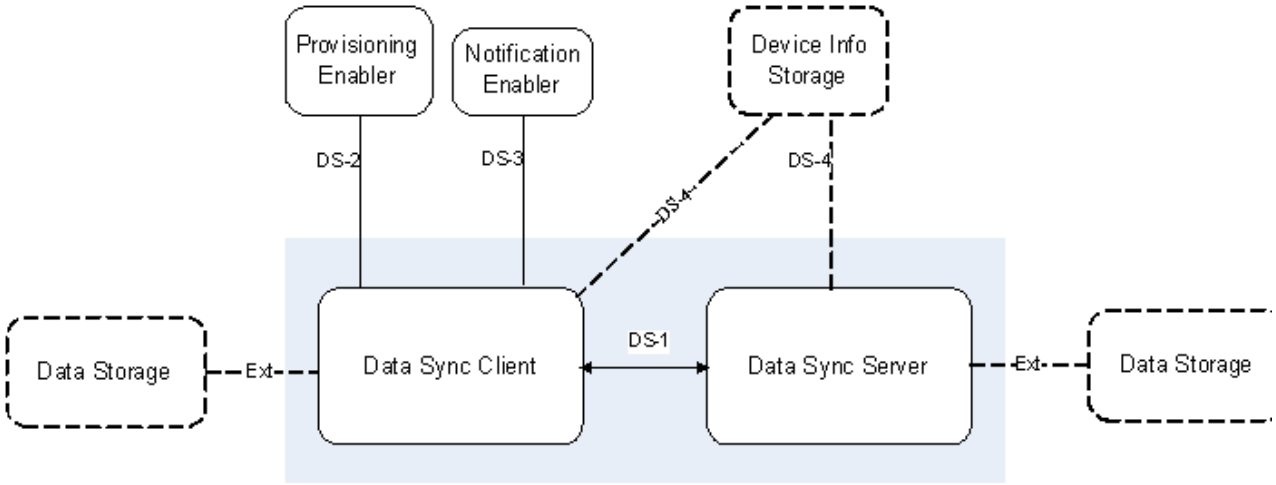


Figure 5.1.3.6.1.1: OMA's DS Architecture [82]

Functional entities:

- Data Sync Client: entity that contains a synchronization client agent and that usually sends the data synchronization commands, possibly including payload data to the Data Sync Server. It shall also be able to receive responses from the Data Sync Server and to receive some data synchronization commands from the server side.
- Data Sync Server: entity that contains a synchronization server agent and synchronization engine and which usually receives the data synchronization messages (operations) possibly including payload data from the Data Sync Client. The Data Sync Server shall also be able to send the responses to the commands if needed and to send some data synchronization messages as commands to the client.
- Notification Enabler: entity used for notification. The Data Sync Server or other applications can use this notification capability to cause the Data Sync Client to initiate a connection to the Data Sync Server.
- Provisioning Enabler: entity used to provision synchronization settings for data sync client.
- Client and Server Data Storage: used for storing data relevant to data synchronization, such as emails, contacts, calendars, short messages, etc.
- Device Info Storage: used as an optional external storage for device information.

Interfaces:

- Interface DS-1: Data Sync Client - Data Sync Server: used for the Data Sync Client and the Data Sync Server to interact with each other for data synchronization. This interface is transport-independent. Hence the transportcan be HTTP, OBEX, etc.
- Interface DS-2: Provisioning Enabler - Data Sync Client: used to provision synchronization settings for the data sync client.
- Interface DS-3: Notification Enabler - Data Sync Client: used to notify the data sync client to cause the Data Sync Client to initiate a connection to the Data Sync Server.
- Interface DS-4: Data Sync Client/Server - Device Info Storage: used for the Data Sync Client or Server to retrieve the other side's device information.
- Interface Ext: Data Sync Client/Server - Data Storage: used for the Data Sync Client or Server to access Data Storage, such as email data storage, calendar data storage, or contact data storage. This interface is not defined in the OMA DS Enabler.

5.1.3.7 Gaming Service

5.1.3.7.1 3GPP

The purpose of [58] is to help 3GPP TSG RAN WG2 define, describe and improve the support for gaming using HSDPA/HSUPA (HS-DSCH/E-DCH), focusing on minimizing delay and the service interruption time in case of handover. The latency of radio, core network, and terminals should be included in the present document with evaluations of the various complexity issues affecting both real time gaming (such as RT Shooting and RT auto racing) and less than real time gaming (such as chess and other less demanding gaming). Inclusion of 2 way RT gaming plus 2 way synchronized voice should also be included in the present document. All evaluations shall include complexity analysis and any end-user complexities and relevant issues.

HSDPA and HSUPA are very important features for operators to carry efficient multimedia services in conjunction with IMS. Gaming is an increasingly important application that requires better performance to satisfy the user expectation. There is a need to enhance the support for gaming, e.g. to focus on minimizing of delay and the service interruption time in case of handover.

5.1.3.7.2 OMA

When looking at mobile games, both from a game experience and architecture perspective, it is useful to distinguish between the following categories of games [83]:

- Messaging based games, which are games using SMS or MMS messaging protocols, and have their game logic purely on the server. Such games can only be played when users are connected to the mobile network.
- Mobile browser-based games, using for example a WAP or I-mode browser, also follow the thin client approach as described above.
- Downloadable offline games, where game logic is downloaded on the mobile device and is executing on the mobile device only.
- Downloadable online games, where game logic is downloaded and executed on the device, but here in conjunction with a game server that can be accessed over a wireless network.
- Externally delivered games, which are distributed physically, through various media (e.g. memory cards etc) and are executing on the mobile device in conjunction with a game server that is accessed over a wireless network.

In the context of mobile game service, OMA Game Service generally consists of game server and IMS service capability. The game server provides an interface to the game logic, and an interface to the game client, where both client and server store and update the game state according to the game logic. The IMS service capability provides necessary functions to offer a completeness of multi-player online game that is either within or beyond OMA standardization. Figure 5.1.3.7.2.1 depicts the context model for OMA gaming support.

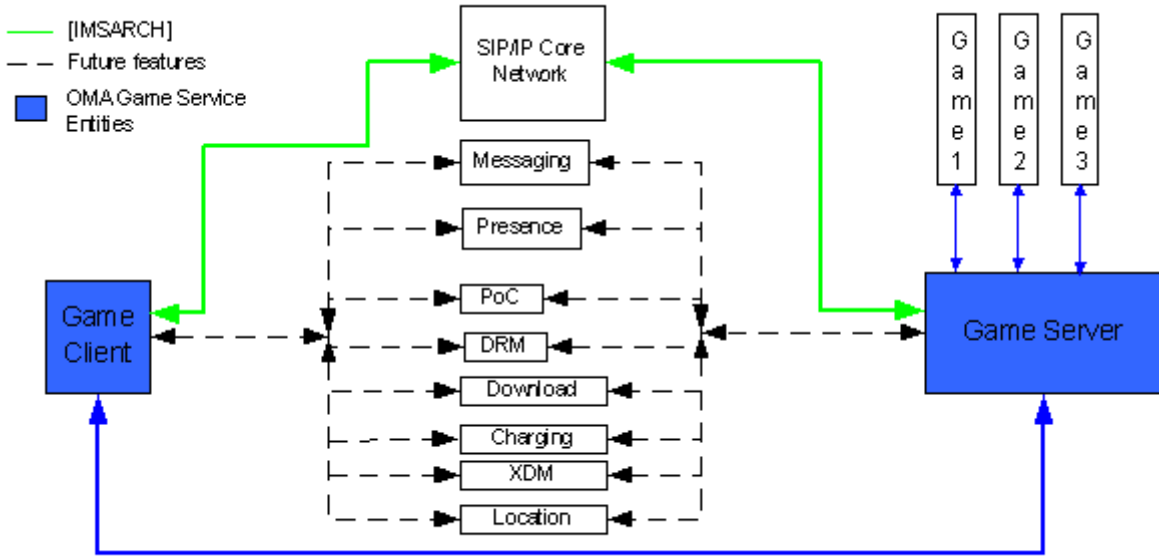


Figure 5.1.3.7.2.1: OMA's context model for gaming [83]

A domain model has been defined as shown in the figure below.

- DMR-1 represents the relationship between Application and ApplicationInstance. It is one-to-many relationship.
- DMR-2 represents the relationship between ApplicationInstance and ActorSession. It is one-to-many relationship.
- DMR-3 represents the relationship between Application and MasterApplicationInstance. It is one-to-many relationship.
- DMR-4 represents the relationship between Application and Actor. It is one-to-many relationship.
- DMR-5 represents the relationship between Actor and ActorSession. It is one-to-many relationship.
- DMR-6 represents the relationship between ActorSession and Session. It is one-to-one relationship.
- DMR-7 represents the relationship between Actor and Session. It is one-to-many relationship.
- DMR-8 represents the relationship between User and Actor. It is one-to-many relationship.

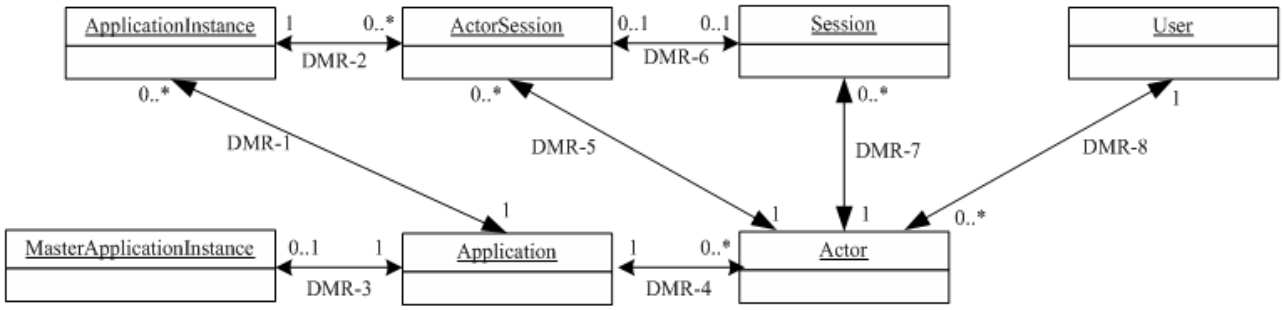


Figure 5.1.3.7.2.2: OMA's ER model for gaming [83]

5.1.3.8 IN Services

5.1.3.8.1 General Info

Under IN services one can understand the concentration of certain services (so called value added services), which exceed the pure connection services and their additional functions, within so called "intelligent network elements".

Advantages:

- Services, which are utilized and need to be controlled network wide, do not have to be built into every network node, but can be provided centrally.
- New services can be introduced into the whole network quickly and easily.

Prerequisites:

- Powerful information exchange protocol between network nodes.
- Big central database with global network information.

Services are activated via special numbers (0800, 0900,etc.) or certain events (e.g. the usage of a certain connection). This activates the service providing servers in the network, which evaluate the received information and send the result back to the transport network for the respective call set-up between the A-party and the called (B-) party (person, call centre, server, etc.).

The signalling information is directed to the IN-node using the "Intelligent Network Application Protocol" (INAP) and/or the "CAMEL Application Part". So the actual communication goal, as well as tariff and routing information can be handed over to the communication network. The figure below gives a simplified version of the network structure, so as to be able to show where the respective signalling protocols are used.

The service logic itself, as well as the data model belonging to it is provider/vendor specific. INAP, CAP and CAMEL have been standardized. Of interest for the data model of an end user will be the capability sets, which give an idea of the service logic as well as the definition of the trigger detection points and the camel subscription information.

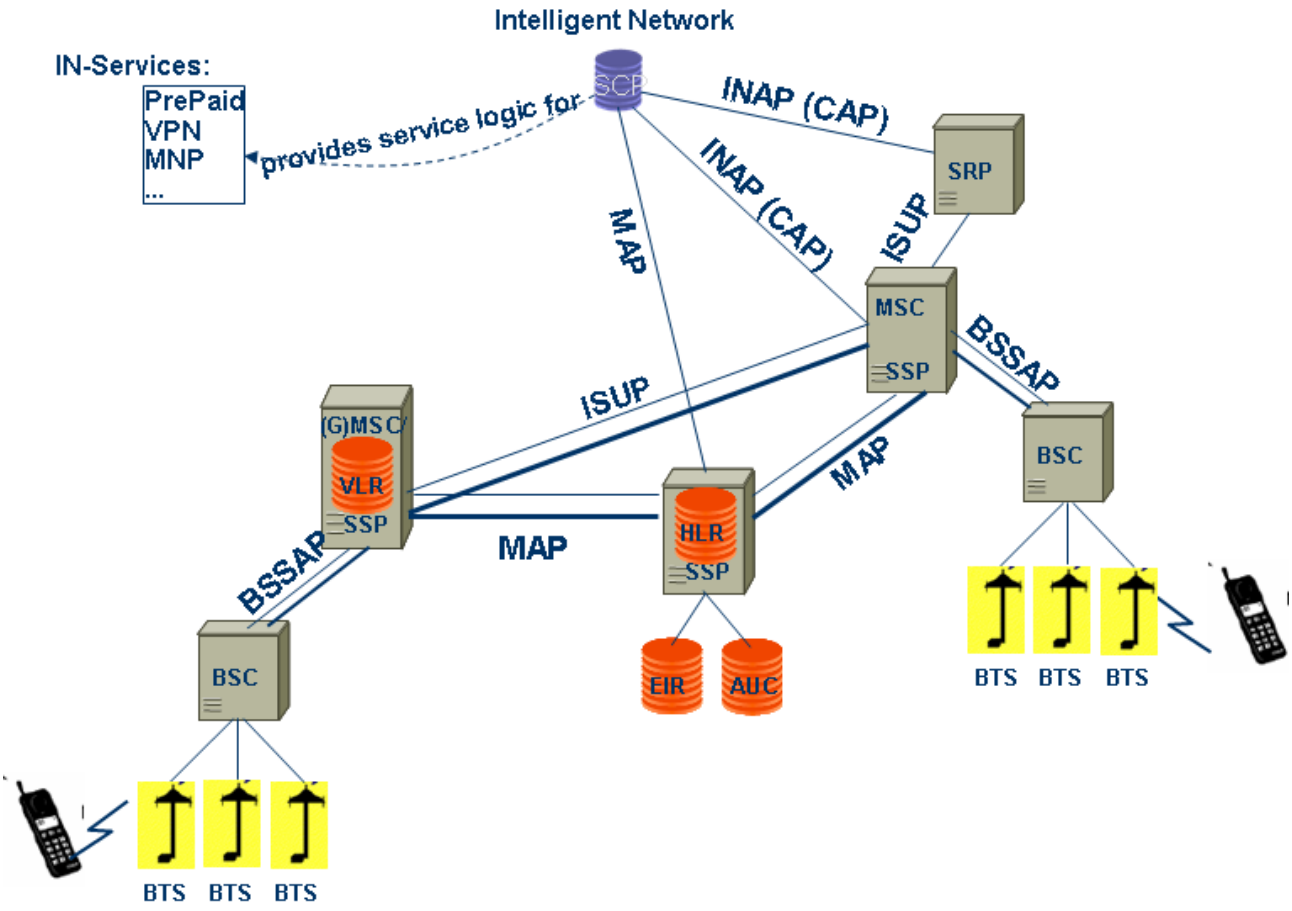


Figure 5.1.3.8.1.1: network model for IN-services in the GSM case

5.1.3.8.1.1 ITU-T

The Services

According to [90] the following descriptions of the services comprising CS1 are valid:

Abbreviated Dialling (ABD)

- This service is an originating line feature that allows business subscribers to dial others in their company using, e.g. only four digits even if the calling user's line and the called user's line are served by different switches. This capability extends switched based intercom calling beyond the switch boundary.

Account Card Calling (ACC)

- The account card calling service allows a user to make a call from any card reading telephone and have the charges for the call automatically debited to a domestic or business account number as defined by the card content.
- The account card calling service allows subscribers to place calls from any normal access interface to any destination number and have the cost of those calls charged to the account specified by the ACC number.
- This service allows the caller to be automatically charged on a telephone account subscribed with the network operator, for any type of outgoing call. The caller has to dial his card number and a PIN, then the called number.

Automatic Alternative Billing (AAB)

- The AAB service enables a user to make a call from any telephone and for the call charge to be billed to the user's account which is specific to this service, and which does not refer either to the calling line or to the called line.

- This service allows a user to call another user and ask him to receive the call at his expenses. Two steps may be defined: the calling party is welcomed to record a brief message giving the caller's name and explaining the call reason, then the called party is alerted, receives the recorded message and is asked to accept to be charged for that call.

Call Distribution (CD)

- This service allows a subscriber to have incoming calls routed to different destinations, according to an allocation law which may be real-time managed by the subscriber.

Call Forwarding (CF)

- Call forwarding allows the called user to forward calls to another telephone number when this service is activated. With this service, all calls destined to the subscriber's number are redirected to the new telephone number.

  This service is under control of the subscriber and can be activated/deactivated by the subscriber.

  When this service is activated, the subscriber's line will receive an alerting ring, "reminder ring", to indicate that the service is activated.

- This service permits the user to have his incoming calls addressed to another number, no matter what the called party line status is. The user's originating service is unaffected, even for charging.

Call Rerouting Distribution (CRD)

- This service permits the subscriber to have his incoming calls encountering a triggering condition (busy, specified number or rings, queue overload or call limiter) rerouted according to a predefined choice: the calls may be rerouted to another destination number (including pager or vocal box), rerouted on a standard or customized announcement, or queued.

Completion of Calls to Busy Subscriber (CCBS)

- This service allows a calling user encountering a busy destination to be informed when the busy destination becomes free, without having to make a new call attempt.

Conference calling (CON)

- Conference calling allows the connection of multiple parties in a single conversation. The number of parties allowed to be connected simultaneously will vary based on transmission bridging requirements to ensure Quality of Service.

Credit Card Calling (CCC)

- The credit card calling service allows subscribers to place calls from any normal access interface to any destination number and have the cost of those calls charged to the account specified by the CCC number.

- This service allows the caller to be automatically charged on a bank card account, for any type of outgoing call. The caller has to dial his card number and a PIN, then the called number.

Destination Call Routing (DCR)

- This service allows customers to specify the routing of their calls to destinations according to:

  - time of day, day of week, etc.;

  - area of call origination;

  - calling line identity of customer;

  - service attributes held against the customer;

  - priority (e.g. from input of a PIN);

  - charge rates applicable for the destinations;

- proportional routing of traffic.

- Destination call routing allows a subscriber to have incoming calls routed to different destinations, based upon the geographic locations of the calling parties. There are also optional reports which provide the subscriber with data on all their incoming calls and can include details such as date and time of call.

Follow-Me Diversion (FMD)

- Follow-me diversion allows the service subscriber to remotely control the redirection (diversion) of calls from his primary telephone number to other locations. The subscriber is allowed to update the diversion location telephone number, from a standard telephone instrument, as he moves from location to location.

- This service allows the subscriber to remotely control his call forwarding capabilities, basically the number to which the calls are forwarded, from any point in the network.

- With this service, a user may register for incoming calls to any terminal access. When registered, all incoming calls to the user will be presented to this terminal access. A registration for incoming calls will cancel any previous registration. Several users may register for incoming calls to the same terminal access simultaneously. The user may also explicitly deregister for incoming calls.

Freephone (FPH)

- This service allows a reverse charging, the subscriber accepting to receive calls at his expenses and being charged for the whole cost of the call.

- Freephone allows the served user having one or several installations to be reached from all or part of the country, or internationally as appropriate, with a freephone number and to be charged for this kind of call.

Malicious Call Identification (MCI)

- Malicious call identification allows the service subscriber to control the logging (making a record) of calls that are received that are of a malicious nature.
- This service enables a user to request that the source of an incoming call is identified and registered in the network. The following information at least is to be registered: called party number, calling party number, time and date of the request. The service may be invoked either during or after the active phase of the call, but before the called user has cleared; as an option, it may be invoked by the network on all calls that are not answered.

Mass calling (MAS)

- Using this service, the network operator can temporarily allocate a single directory number to the served user. Each time a call is made to this number by an end user, the user will be played an announcement and asked to input a further digit to indicate a preference. The choice made will be recorded and a count incremented. When the service has ceased, the network operator will supply details of the total "votes" cast for each preference will be supplied to the served user and the special number will be reallocated. Calls made to this special number may be charged at varying rates.
- Mass calling involves instantaneous, high-volume traffic which is routed to one or multiple destination(s). Calls can be routed to these destination numbers based on various conditions, such as the geographical location or time of day. The calling party will be charged for this kind of call.

Originating Call Screening (OCS)

- Originating calls may be controlled by the originating call screening capability. This allows the subscriber to specify that outgoing calls be either restricted or allowed, according to a screening list and, optionally, by time of day control. This can be overridden on a per-call basis by anyone with the proper identity code.
- This service allows a subscriber to authorize outgoing calls, through the use of a screening list. This list may be managed by the subscriber. The user may override the restriction by giving a PIN.

Premium rate (PRM)

- This service allows to pay back a part of the call cost to the called party, considered as an added value service provider.
- Premium rate allows the served user having one or several installations to be reached from all or part of the country, or internationally as appropriate, with a premium rate number. The calling party will be charged with a premium rate for this kind of call.

Security screening (SEC)

- This capability allows security screening to be performed in the network before an end-user gains access to the subscriber's network, systems, or applications. Access code abuse detection is a capability which will generate a report on the invalid access attempts: how many, over what time period, by whom, and from where. This provides an added layer of security.
- This service asks the user to dial a pin code, which allows the verification of the user identity before giving the user access to the subscriber's network, systems or application. As an option, the invalid access attempts may be registered.

Selective call forwarding on busy/don't answer (SCF)

- Selective call forwarding - busy/don't answer (SCF-BY/DA) allows the called user to forward particular pre-selected calls if the called user is busy or does not answer within Y seconds or X rings. The calls will be pre-selected based upon an SCF-BY/DA list. This list will have 1 to 5 numbers or 1 to 10 numbers with a default call forward number for calling users not in the list. There will also be remote access and time of day indicators for this capability.

Selective call forwarding

- This service permits the user to have his incoming calls addressed to another number, no matter what the called party line status is, if the calling line identity is included in, or excluded from, a screening list. The user's originating service is unaffected, even for charging.

Call forwarding on busy

- This service permits the user to have his incoming calls addressed to another number if they encounter a busy condition. The user's originating service is unaffected, even for charging.

Call forwarding on don't answer (no reply)

- This service permits the user to have his incoming calls addressed to another number, if they encounter no reply. The user's originating service is unaffected, even for charging.

Split charging (SPL)

- This service allows a split charging, the calling and the called party being each charged for one part of the call.
- This service enables a network operator to distribute the charges for a call between the two parties involved.
- Split charging allows the service user having one or several installations to be reached from all or part of the country, or internationally as appropriate, with a split charging number. Both the calling party and the served user will be charged with a split charging rate for this kind of call.

Televoting (VOT)

- This service allows the subscriber to propose a phone voting, the user being asked either to ring a specific number according to his choice, or to ring a unique number and, after prompting, to give his choice by keyboard or by voice dialogue.
- Televoting enables subscribers to survey public opinion using the telephone network. Persons wishing to respond to an opinion poll can call advertised televoting numbers to register their votes. The charging is to the discretion of the service subscriber.
- Using this service, the network operator can temporarily allocate directory numbers to the served user. Each time a call is made to one of the numbers by an end user, the user will be played an announcement acknowledging the call, and a count of calls made to this number will be incremented. When televoting has ceased, the network operator will supply details of the total numbers of calls made to each number to the served user and the special numbers will be reallocated. Calls made to these special numbers may be charged at varying rates.

Terminating call screening (TCS)

- Terminating calls may be controlled by the terminating call screening capability. This allows the subscriber to specify that incoming calls be either restricted or allowed, according to a screening list and optionally, by time of day control.

Universal access number (UAN)

- This service allows a subscriber with several terminating lines in any number of locations or zones to be reached with a unique directory number. The subscriber may specify which incoming calls are to be routed to which terminating lines, based upon the area the call originated.
- This service enables a service provider to publish a national number and have incoming calls routed to a number of different destinations based on the geographical location of the caller.

Universal Personal Telecommunications (UPT)

- UPT is a mobility service which enables subscribers to make use of telecommunication services on the basis of a unique Personal Telecommunication Number (PTN) across multiple networks at any network access. The PTN will be translated to an appropriate destination number for routing based on the capabilities subscribed to by each service subscriber.
- This service provides personal mobility by enabling a user to initiate any type of service and receive any type of call on the basis of a unique and personal network-independent number, across multiple networks, at any user-network access (fixed, movable or mobile), irrespective of geographic location, limited only by terminal and network capabilities.

User-Defined Routing (UDR)

- This capability allows the subscriber to specify how outgoing calls, from the subscriber's location, shall be routed, either through private, public, or virtual facilities or a mix of facilities, according to the subscriber's routing preference list. These lists will apply to individual lines or to several lines at the subscriber's location.

Virtual Private Network (VPN)

- This service permits to build a private network by using the public network resources. The subscriber's lines, connected on different network switches, constitute a virtual PABX, including a number of PABX capabilities, such as private numbering plan (PNP), call transfer, call hold, and so on.

- As an option, to each private user, either a class of service or specific rights and privileges may be attributed. As another option, a private user may access his private network from any point in the network keeping, after authentication, his class of service or his specific rights and privileges.

- This service permits the use of public network resources to provide private network capabilities without necessarily using dedicated network resources. The subscriber's lines, connected to different network switches, constitutes a virtual private network that may include private network capabilities, such as dialling restrictions, private numbering plan, hold, call transfer, and so on.

- A PNP may provide a group of users the capability to place calls by using digit sequences having different structures and meaning than provided by the public numbering plan, or PNP may utilize the public numbering plan's digit sequences, structures and meaning.

- VPN allows a subscriber to define and use a private numbering plan for communication across one or more networks between nominated user access interfaces. A PNP provides a group of users the capability to place calls by using digit sequences having different structures and meanings than provided by the public numbering plan.

Descriptions of targeted service features

Abbreviated dialling (ABD)

- This feature allows the definition of abbreviated dialling numbers with a VPN. For the users of the VPN, the abbreviated dialling numbers are not subjected to call restrictions, e.g. a VPN user may not be allowed to access the Off-net Calling service feature but can reach an off-net number via this feature.

- This feature allows the definition of abbreviated dialling digit sequences to represent the actual dialling digit sequence, i.e. a two digit sequence may represent a complete dialling sequence for a private or public numbering plan.

- This service feature is an originating line feature that allows business subscribers to dial others in their company using a short numbering, even if the calling user's line and the called user's line are served by different switches.

Attendant (ATT)

- This service feature allows VPN users to access an attendant position within the VPN for providing VPN service information (e.g. VPN numbers). The attendant(s) can be accessed by dialling a special access code.

Authentication (AUTC)

- This service feature allows for the verification that a user is allowed to exercise certain options in a telephone network. In other words, the request made by the user is authentic and should be granted.

Authorization code (AUTZ)

- This service feature allows a VPN user to override calling restrictions of the VPN station from which the call is made. Different sets of calling privileges can be assigned to different authorization codes and a given authorization code can be shared by multiple users.

Automatic call back (ACB)

- This service feature allows the called party to automatically call back the calling party of the last call directed to the called party.

Call Distribution (CD)

- This service feature allows the served user to specify the percentage of calls to be distributed among two or more destinations. Other criteria may also apply to the distribution of calls to each destination.

Call Forwarding (CF)

- This service feature allows the user to have his incoming calls addressed to another number, no matter what the called party line status may be.

Call Forwarding on busy/don't answer (CFC)

- This service feature allows the called user to forward particular calls if the called user is busy or does not answer within a specified number of rings.

Call gapping (GAP)

- This service feature allows the service provider to automatically restrict the number of calls to be routed to the subscriber.
- This service feature allows to restrict the number of calls to a served user to prevent congestion of the network.

Call hold with announcement (CHA)

- The call hold with announcement service feature allows a subscriber to place a call on hold with options to play music or customized announcements to the held party.

Call Limiter (LIM)

- This service feature allows a served user to specify the maximum number of simultaneous calls to a served user's destination. If the destination is busy, the call may be routed to an alternative destination.
- This service feature enables to count the running calls to the subscriber and to reject all the new calls when a threshold of simultaneous calls is reached. As an option, this threshold may be real-time managed by the subscriber.

  Associated with call volume distribution or call distribution, it allows the rerouting of the new calls.

Call logging (LOG)

- This service feature allows for a record to be prepared each time that a call is received to a specified telephone number.

Call queuing (QUE)

- This service feature allows a served user to have calls meeting busy at the scheduled destination to be placed in a queue and connected as soon as free condition is detected. Upon entering the queue, the caller hears an initial announcement informing the caller that the call will be answered when a line is available.
- This service feature enables the subscriber, when a call encounters a terminating trigger such as a busy condition or a specified number of rings to queue that call, a specific announcement being sent to the calling party.

Call transfer (TRA)

- The call transfer service feature allows a subscriber to place a call on hold and transfer the call to another location.

Call waiting (CW)

- This service feature allows the called party to receive a notification that another party is trying to reach his number while he is busy talking to another calling party.

Closed user group (CUG)

- This service feature allows the user to be a member of a set of VPN users who are normally authorized to make and/or receive calls only within the group. A user can belong to more than one CUG. In this way, a CUG can be defined so that certain users are allowed either to make calls outside the CUG, or to receive calls from outside the CUG, or both.

Consultation calling (COC)

- The consultation calling service feature allows a subscriber to place a call on hold, in order to initiate a new call for consultation.

Customer profile management (CPM)

- This service feature allows the subscriber to real-time manage his service profile, i.e. terminating destinations, announcements to be played, call distribution, and so on.

Customized recorded announcement (CRA)

- This service feature allows a call to be completed to a (customized) terminating announcement instead of a subscriber line. The served user may define different announcements for unsuccessful call completions due to different reasons (e.g. caller outside business hours, all lines are busy).

Customized ringing (CRG)

- This service feature allows the subscriber to allocate a distinctive ringing to a list of calling parties.

Destinating user prompter (DUP)

- This service feature enables to prompt the called party with a specific announcement. Such an announcement may ask the called party to enter an extra numbering, e.g. through dual-tone multi-frequency (DTMF), or a voice instruction that can be used by the service logic to continue to process the call.

Follow-me diversion (FMD)

- This service feature allows a VPN user to change the routing number of his/her VPN code via a DTMF phone. The updated number can be another VPN code or a PSTN number.

- With this service feature, a user may register for incoming calls to any terminal access. When registered, all incoming calls to the user will be presented to this terminal access. A registration for incoming calls will cancel any previous registration. Several users may register for incoming calls to the same terminal access simultaneously. The user may also explicitly deregister for incoming calls.

Mass calling (MAS)

- This service feature allows processing of huge numbers of incoming calls, generated by broadcasted advertisings or games.

Meet-me conference (MMC)

- This service feature allows the user to reserve a conference resource for making a multi-party call, indicating the date, time, and conference duration. At the specified date and time, each participant in the conference has to dial a designated number which has been assigned to the reserved conference resource, in order to have access to that resource, and therefore, the conference.

Multiway calling (MWC)

- This service feature allows the user to establish multiple, simultaneous telephone calls with other parties.

Off-net access (OFA)

- This service feature allows a VPN user to access his or her VPN from any non-VPN station in the PSTN by using a personal identification number (PIN). Different sets of calling privileges can be assigned to different PINs, and a given PIN can be shared by multiple users.

Off-net calling (ONC)

- This service feature allows the user to call outside the VPN network. Calls from one VPN to another are also considered off-net.

One number (ONE)

- This feature allows a subscriber with two or more terminating lines in any number of locations to have a single telephone number. This allows businesses to advertise just one telephone number throughout their market area and to maintain their operations in different locations to maximize efficiency. The subscriber can specify which calls are to be terminated on which terminating lines based on the area the calls originate.

Origin dependent routing (ODR)

- This service feature enables the subscriber to accept or reject a call, and in case of acceptance, to route this call, according to the calling party geographical location. This service feature allows the served user to specify the destination installation(s) according to the geographical area from which the call was originated.

Originating call screening (OCS)

- This service feature allows the served user to bar calls from certain areas based on the District code of the area from which the call is originated.

Originating user prompter (OUP)

- This service feature allows a served user to provide an announcement which will request the caller to enter a digit or series of digits via a dual-tone multi-frequency (DTMF) phone or generator. The collected digits will provide additional information that can be used for direct routing or as a security check during call processing.

- This service feature enables to prompt the calling party with a specific announcement. Such an announcement may ask the calling party to enter an extra numbering (e.g. through DTMF) or a voice instruction that can be used by the service logic to continue to process the call.

Personal Numbering (PN)

- This service feature supports a UPT number that uniquely identifies each UPT user and is used by the caller to reach that UPT user. A UPT user may have more than one UPT number for different applications (e.g. a business UPT number for business calls and a private UPT number for private calls), however, a UPT user will have only one UPT number per charging account.

Premium charging (PRMC)

- This service feature allows for the pay back of the part of the cost of a call to the called party, when he is considered as a value added service provider.

Private Numbering Plan (PNP)

- This service feature allows the subscriber to maintain a numbering plan within his private network, which is separate from the public numbering plan.

Reverse charging (REVC)

- This service feature allows the service subscriber (e.g. freephone) to accept to receive calls at its expense and be charged for the entire cost of the call.

Split charging (SPLC)

- This service feature allows for the separation of charges for a specific call, the calling and called party each being charged for one part of the call.

Terminating Call Screening (TCS)

- This service feature allows the user to screen calls based on the terminating telephone number dialled.

Time Dependent Routing (TDR)

- This service feature enables the subscriber to accept or reject a call, and in case of acceptance, to route this call, according to the time, the day in the week and the date.
- This service feature allows the served user to apply different call treatments based on time of day, day of week, day of year, holiday, etc.

IN CS-2 [91] defines an initial subset of IN capabilities that meet the following general criteria:

- IN CS-2 is a subset of the target Intelligent Network architecture;
- IN CS-2 is a superset of IN CS-1, as defined in the IN CS-1 Recommendations;
- IN CS-2 is a set of definitions of capabilities that is of direct use to both manufacturers and network operators;
- IN CS-2 provides network capabilities defined to support the set of IN CS-2 benchmark services or service features. These capabilities can also be used for the support of other services that may, or may not, be standardized by ITU-T.

The IN CS-2 architecture could be applied for PSTN, ISDN, and mobile networks.

Three types of services have been identified in IN CS-2:

- telecommunication service;
- service management service; and
- service creation services.

The last two types of services are first introduced in IN CS-2.

According to [91] the following descriptions of the services additional to CS1 comprising CS2 are valid:

Telecommunication services

Mobility service features (UPT, FPLMTS)

These service features are aimed at, but not limited to, supporting UPT and FPLMTS.

Personal mobility features (UPT): Personal mobility allows a user to appear at any network access point and initiate telecommunication services.

- User authentication (UAUT): This feature confirms the identity of a user with the network and the identity of the network with a user. UAUT takes place during interactions between the network and a user.
- User registration (UREG): This feature enables a user to register on a terminal access for the purpose of receiving or placing calls.
- in-call registration: means by which a user registers from the current terminal address for incoming calls to be presented to that terminal address.
- Outgoing call registration (OGREG): The out-call registration allows a user from the current terminal address to register for outgoing calls to be made from that terminal address.
- Secure answering (SANSW): Secure answering is a feature by which the service subscriber/user requires that incoming calls cannot be answered unless the answering party first successfully authenticates himself as the wanted subscriber.
- Follow-on (FO): This feature enables a user to make a series of service requests without going through the identification and authentication process before each service feature request.
- Flexible (call) origination authorization (FOA): The FOA feature can take effect immediately prior to the time that an IN capable switch would authorize call origination, during the call set-up process. A customized algorithm, provided by the network provider or the subscriber, can then determine whether or not the call should be originated.

- Flexible (call) termination authorization (FTA): The FTA feature can take effect immediately prior to the time that an IN capable switch would authorize call termination, during the call set-up process. A customized algorithm, provided by the network provider or the subscriber, can then determine whether or not the call should be authorized.

- Provision of stored messages (PSM): When the service subscriber registers the location, the network automatically informs the subscriber of the service and sends the voice messages which were stored before.

- Multiple terminal address registration (MTAR): This service feature enables a user to be registered for incoming calls on more than one terminal, with calls being offered to the terminals according to a certain algorithm (e.g. in sequence if there is no answer after a user-determined time (i.e. a user-configurable hunt group), and simultaneously).

- Intended recipient identity presentation (IRIP): This service feature allows identification at the receiving terminal of the intended recipient of an incoming call. It is required to enable Secure Answering (SANSW) to be offered when there is more than one UPT user registered for incoming calls on the one terminal.

- Blocking/unblocking of incoming calls (BUIC): This service feature enables any person, even if not a UPT user, to block and unblock calls incoming to UPT users currently registered on the third party's terminal.

Terminal mobility features (FPLMTS): Terminal mobility provides a tetherless link between the user's terminal equipment and fixed network access points, thereby providing freedom of movement for the user during the use of telecommunication services and service features.

- Terminal authentication (TAUT): The TAUT feature is initiated within the mobility processes of location management (i.e. terminal location registration), call origination, call delivery and at other times as initiated by the network or terminal. In support of security, the feature ensures the validity of the terminal and the network. Also, the feature enables the establishment of a private control and communications channel between the network and a terminal. Authentication process should occur when a terminal authenticates either in its home network or visited network.

- Handover (HOV): The handover (HOV) service feature enables a mobile terminal to change network access areas/points within a network or to an other network, while maintaining the call(s) and/or signalling relationship(s).

- Terminal location registration (TLR): Terminal location registration is used when terminals notify the system of their location.

- Terminal attach/detach (ATDT): The detach feature is used by the terminal to notify the network whether the terminal is temporarily not reachable. The network will modify the status information of the terminal.

- Terminal paging (TPAG): This service feature enables the determination of the current location of a user or of a mobile terminal. It pages the terminal in the terminal location registration area based on the stored terminal location information, and determines the visited cell by the response from the terminal.

- Radio paging (RPAG): This service feature enables one-way personal selective calling with alert. The RPAG feature enables a user to send a message, either voice, tone, or alphanumeric, to a selected pager terminal or a group of terminals.

- Emergency calls in wireless (ECW): The ECW service feature allows emergency calls to have priority over all other calls to ensure service. Emergency calls can be readily connected without dropping other active calls and without the requirement of successful terminal authentication, privacy or user authentication.

- Terminal equipment validation (TEVA): The TEVA feature should be considered as a part of the mobility processes of location management (i.e. terminal location registration), call origination, call delivery and at other times as initiated by the network or terminal. The feature enables FPLMTS network operator to identify stolen, lost, suspicious or non-type-approved terminal equipment and then track or prevent the use of this terminal equipment. A blacklist of the identities of individual stolen, lost or suspicious terminal equipment and a white list of the identities of type-approved terminal equipment will be needed.

- Cryptographic information management (CIM): Cryptographic information management is a service feature which manages the secret information associated with cryptographic security mechanism including: the enhanced authentication mechanism, the integrity mechanism, and the encipherment mechanism.

Other services

- Internetwork Freephone (IFPH): This service allows the served user having one or more installations to be reached from a specific network other than his/her network with a freephone number, and to be charged for this kind of call. The subscriber's network configuration is defined per subscriber direction using customer-specific information resident in multiple networks.

- Internetwork Premium rate (IPRM): This service provides two-way interactive communication between callers in one network and service/information providers in another network. The calling party is charged with a premium rate for this kind of call.

- Internetwork Mass calling (IMAS): This service is designed to accommodate large volumes of simultaneous calls to a single directory number in another network. It can provide one-way, non-interactive communication between each caller in a given network and a service/information provider in another network.

- Internetwork televoting (IVOT): This service allows a service/information provider in one network to conduct voting or polling over the phone. The caller in another network votes by placing a call to a specific number corresponding to a voting/polling choice. The service provides communication between each caller in a given network and a service/information provider in another network.

- Global Virtual Network Service (GVNS): The global virtual network service is a global switched VPN service supported by multiple networks (e.g. offered to customers over PSTN and/or ISDN).

- Completion of Call to Busy Subscriber (CCBS): This service enables a calling user encountering a busy destination to have the call completed when the busy destination becomes not busy, without having to make a new call attempt.

- Conference calling (CONF): This service enables a group of users to be connected into a multi-party call.

- Call Hold (HOLD): This service allows a user to place a call on hold and play an announcement to the held party, and to initiate a new call. The user can subsequently resume participation in the original call.

- Call Transfer (CT): This service allows a user to place a call party on hold and to be offered dial tone to provide a destination number (optionally service logic can provide the destination number). Upon successful call set-up, the subscriber is released and the held party is connected to the new destination in a two-party active call.

- Call Waiting (CW): This service allows a user to notify a subscriber of the occurrence of a call termination attempt, while that subscriber is participating in an active call.

- Hot line (HOT): The hot line service allows a user to place calls without providing, in the call request, the called party information required by the network to route the call. This routing information is stored in the network by prior subscription.

- Multimedia (MMD): This service allows a subscriber to receive or send an integrated communication consisting of mixtures of voice, data, image, and video information. A key capability will be the ability to synchronize and control delivery of information from disparate sources (e.g. voice and data).

- Terminating Key Code Screening (TKCS): This service enables a subscriber to screen incoming calls by means of a user-defined key, i.e. pin code.

- Message Store and Forward (MSF): This service enables a user to send a message to be distributed to one or several destination users. Different types of messages (such as voice, data, and fax) may be supported and different methods of delivery and/or times of delivery (such as only to pre-subscribed mail-box holders or direct to any access) may be specified.

- International telecommunication charge call (ITCC): This service allows the holders of a telecommunication charge card to make use of a variety of telecommunication services provided by the card acceptor (visited network) and have the charges billed to the customer's account number by the card issuer (home network).

Other service features

- Automatic Call Back (ACB): This service feature allows the called party to automatically call back the calling party of the last call directed to the called party.

- Call Hold (HOLD): This service feature allows a user to interrupt his/her connection to an existing call, without releasing that call. Some of the resources which were dedicated to that call (e.g. bearer capability) become available for other uses.
- Call Retrieve (CRET): This service feature allows a user to re-establish his/her connection to a call previously placed on hold.
- Call Transfer (CT): This service feature allows a user who is a party in two separate calls, to cause the other two parties to those calls to be connected to each other, releasing him/her from both.
- Call Toggle (CTOG): This service feature is applicable to a user who has one active call and one on hold. It allows him/her repeatedly to select the currently held party as the new connection, the previously connected party being automatically put on hold.
- Call Waiting (CW): This service feature informs a user already engaged in a call that another party is trying to establish a connection to him/her.
- Meet-Me Conference (MMC): This service feature allows the user to reserve a conference resource for making a multi-party call, indicating the date, time, and conference duration.
- Multi-Way Calling (MWC): This feature allows the user to establish multiple, simultaneous telephone calls with other parties.
- Call Pick-Up (CPU): This service feature enables a user to associate a call request to an already alerting call. The alerting call awaits answer while the user originating call pick-up signals to the network a desire to connect to the alerting call. The network then connects the call parties.
- Calling Name Delivery (CND): This service feature gives to the network operator the capability to display/announce the name of the calling party to the calling name delivery user (the called party) prior to answer, thus allowing this user to screen or distinctively answer the call.
- Services On-Demand (SOD): This service feature enables a user to request new services while initiating or involved in a call, e.g. multi-way calling at a pay phone. This includes the capability to invoke new services for the duration of the call.
- Message Waiting Indication (MWI): This feature enables a user to be informed that messages for his attention are waiting.
- Feature Use Charging (FUC): This feature enables the service provider to apply a certain charge to the use of any specified feature.
- Internetwork Service Identification (INSI): This service feature permits the receiving network, in an internetwork call, to receive from the originating network an indication of the service used in the received call.
- Internetwork Rate Indicator, Forward (INRI-F): This service feature is the ability to provide across networks, in the forward direction, an indication of the rate either being charged or to be charged for the presented call.
- Internetwork Rate Indicator, Backward (INRI-B): This service feature is the ability to provide across networks, in the backward direction, an indication of the rate either being charged or to be charged for the received call.
- Real Time Flexible Rating (RTFR): This service feature is the ability to vary in real time, for a given call, the billing rate, or the party being charged. This could be done at subscriber's direction, during a call or during call set-up.
- Originating Carrier Identification (OCI): This service feature permits the receiving network, in an internetwork call, to receive an indication identifying the "originating carrier" (i.e. the originating network/network operator).
- Terminating carrier identification (OTC): This service feature permits the receiving network, in an internetwork call, to receive from the originating network, an indication identifying the network where the call is destined to, or "terminating carrier" (i.e. the terminating network/network operator).
- Resource Allocation (RAL): This service feature enables the allocation, in advance and for a certain period of time, of pooled resources (e.g. conference bridges) required for a service.

- Delivery of Complementary Information (DCI): This service feature enables a calling user to supply to the network complementary information (e.g. an account number and a password) associated with the call set-up information.

- Service Indication (SIND): This service feature enables the called party to receive an indication concerning the presented call (for instance, an application to the freephone service would be the indication that the charge is to be supported by the called party; an application to the call forwarding service would be the forwarding number).

- Service Negotiation (SNEG): This service feature enables the parties involved in a call to negotiate the bearer services, teleservices and supplementary services to be provided for the call, depending on the services subscribed by the parties, the terminal and network capabilities, etc.

- Call Forwarding (CF): This feature is listed here for inclusion in IN CS-2 because some useful capability had not been fully included in IN CS-1.

- B-ISDN Multiple Connections Point-to-Point (BI-MCPP): This service feature enables a user to make a call between two points involving multiple connections, e.g. voice, audio, video, and/or data. This service feature may make use of B-ISDN point-to-point connection service feature (BI-PPC) and need other service features such as multi-connection.

- B-ISDN Multi-Casting (BI-MCAST): This service feature enables the network to set up multiple connections among multiple parties where the connections are point-to-multipoint unidirectional. This service feature may make use of B-ISDN point-to-multipoint connection service feature (BI-PMC) and/or B-ISDN multipoint-to-point connection service feature(BI-MPC) and need other service features such as leaf control.

- B-ISDN Conferencing (BI-CONF): This service feature enables the network to set up multiple connections among multiple parties where the connections are multipoint to multipoint. This service feature may make use of B-ISDN multipoint-to-multipoint connection service feature (BI-MMC) and other service features such as third party control.

- Call Connection Elapsed time limitation (CCEL): This service feature allows a calling party to make calls and communicate with one or more parties within a duration time predefined on a subscription basis. A tone or an announcement may be provided to the parties (i.e. calling and called parties) to indicate that the call will be cleared in a short time.

- Special Facility Selection (SFS): This service feature enables a call to be routed via a special facility (e.g. a virtual leased line) under the determination of service control.

- Concurrent Features Activation with Bi-control (CFA-BC): This service feature enables a call to be influenced by some features at two different point concurrently, such as originating side and terminating side. With this feature, a set of features is pre-defined in one service logic and controlled by its context with bi-control relationship.

  - Customized Call Routing with Public networks (CCR-PU): this service feature permits the public network to access other public networks for call processing and routing information.

  - Customized Call Routing with Customers (CCR-CU): this service feature permits the public network to access customers systems for call processing and routing information.

- Internetwork Service Profile Interrogation (ISPI): This service feature enables a user to interrogate (read only) the current contents of the user's service profile.

- Internetwork Service Profile Modification (ISPM): This service feature enables a user to modify (read and write) the appropriate user's service profile parameters that are allowed to be modified.

- Internetwork Service Profile Transfer (ISPT): This service feature enables service profile information to be transferred to other service profile storage locations in other networks.

- Reset of UPT registration for incoming calls (IRUR): This service feature enables any person (the third party), even if not a UPT user, to reset any UPT registrations for incoming calls on the third party's terminal.

- Mobility Call Origination (MCO): The MCO feature covers both mobile call origination and UPT call termination. It is initiated within the mobility process of call origination. This feature does not require any location registration of terminal/users and allows a provision of customized authentication of terminal/user for call origination. This feature is independent of the registration states of the user and other users at the terminal.

- Mobility Incall Delivery (MID): The MID feature covers both mobile user call termination and UPT incall delivery.

- Data communication between different protocol terminals (DCPT): This service feature enables a mobile terminal to handle data communication between different protocol terminals in the intra-network or internetwork environment. This service feature enables a mobile terminal to handle data communication between different protocol terminals in the intra-network or internetwork environment.

- Charge Determination (CDET): This service feature enables the calculation of charges related to a call. The charged party(s) may include FPLMTS subscribers, UPT subscribers and/or other calling parties. Charges may be based on usage and chargeable events/procedures (e.g. location update and service profile management). Two methods of charge determination are possible.

  - off-line charging.

  - on-line charging.

- Charge Card Validation (CCV): This service feature provides the ITCC service an authentication feature to compare user-side information, provided to the visited network, with information stored in the home network.

- Call Disposition (CD): This service feature provides the ITCC service the means to verify that the card has enough spare credit (e.g. the card usage value has not been exceeded) to give the permission to make the call.

- User Service Interaction (USI): This service feature enables a user to interact with, and thus to send or receive information to or from, a service in association with a call involving this service.

- Enhanced Call Disposition (ECD): This service feature provides a means to cut down the call as soon as the card usage is exceeded.

Service management services

Definition

- Service control service enables a subscriber to directly change the value of the parameters of his/her subscription to a telecommunication service and a service monitoring service after the service provisioning.

- Service control parameters are what a subscriber can directly control regarding a subscription to a telecommunication service and a service monitoring service. The service control parameters available for control within this subscription are specified by service customization parameters.

- Service monitoring service enables a subscriber to get information about the usage of a subscription to telecommunication service after the service provisioning.

- Service monitoring data are what a subscriber can directly monitor regarding a subscription to a telecommunication service.

- Service customization service provides the capability to select the type of telecommunication service feature, service control service, and service monitoring service to be provided to the subscriber after provisioning.

- Service customization parameters define the services, parameters, and data which a subscriber can manipulate as part of his/her subscription to a telecommunication service, service control service, and service monitoring service.

Service management processes are the following types of activity performed by network operators/service providers:

- Service deployment is the introduction of a service into the IN-structured network in a subscriber independent way.

- Service provisioning is the initial installation and deployment of necessary resources and data in appropriate network elements to provide a service subscription to a specific subscriber.

- Management during the service utilization contains service monitoring, service maintenance, service traffic management, audit administration, and billing activities.

The capabilities of service management will not be reflected in the end-user model and are thus not described further.

Service creation services

This paragraph intends to provide a short list of targeted service creation services. But as they are of no consequence to the end-user model there will be not description.

- Service specification services
  - feature interaction detection;
  - cross-service feature interaction detection;
  - feature interaction rule/guidelines generation;
  - service and SIB cataloguing;
  - created service resource utilization.
- Service development services
  - creation interface selection;
  - creation initiation;
  - editing;
  - combining;
  - data population rule generation;
  - SMP service creation: Permits the creation of the SMP functions that are required to support the telecommunication services being created (e.g. OAM&P service logic programs for the SMP). Support is supplied as for all other services;
  - syntax and data checking;
  - service and SIB archiving;
  - service configuration control;
  - SIB configuration control;
  - network configuration tracking capability.
- Service verification services
  - SCE testing;
  - created service simulation;
  - created service live testing.
- Service deployment services
  - SMP-created service data and service logic program update;
  - Service distribution;
  - SIB distribution;
  - Data rule distribution;
  - Multiple SMP support;

- Network tailoring;
- Network element capability specification;
- Network element function/capability assignment.

- I.5.6 Service creation service management services
  - SCE access control;
  - SCE usage scope control;
  - SCE recovery;
  - SCE release management;
  - SCE capability expansion;
  - SCE conversion;
  - cross-SCE service maintenance;
  - SCE-to-SCE system consistency;
  - SCE service/modular/system transference;
  - conversion of created services;
  - service management interaction.

IN CS-3 [92] defines a set of IN capabilities that meet the following general criteria:

- IN CS-3 is a subset of the target Intelligent Networks architecture;
- IN CS-3 is a superset of IN CS-2, as defined in the IN CS-2 Recommendations;
- IN CS-3 is a set of definitions of capabilities that is help to both manufacturers and network service providers/operators; and
- IN CS-3 provides network capabilities defined to support the set of IN CS-3 benchmark services and service features. These capabilities can also be used to support other services that may, or may not, be standardized by ITU-T.

Service features of IN CS-3 according to [92].

Basic features

- CCBS support (CCBS): Call Completion to Busy Subscriber support by IN functionality to enable for example CCBS in combination with call-related IN number translation services/features like Number Portability, Personal Number. These IN services can be invoked either at local exchange level or at transit exchange level.
- Correlation of Call Detail Record (CDR) Information from Multiple Entities (CICME): It shall be possible for a network or service provider to collect CDR information from different physical entities in the network involved in the same call, and be able to correlate the information in the billing systems.
- Carrier Selection Handling (CSHND): For IN initiated calls and terminal initiated calls that are handled in IN it shall be possible to have control over carrier selection. This can be done on a per-call basis or by subscription or default. This is an extension of an IN CS-2 capability.
- IN Calling Line presentation restriction (ICLPR): It should be possible for an IN service subscriber to offer the IN number as COLP number, but restrict presentation of the number.
- Inter-Network Service Indicator (INSIN): Permits the receiving network, in an inter-network call, to receive from the originating network, an indication of the service used in the received call.

- Language Selection for User Interaction (LASUI): Based on e.g. subscriber preferences, user interaction towards a subscriber can be performed in a certain language. If the preferred language is not available, user interaction will fallback to a default language.

- Line Restrictions Override (LRORI): Switch-based line restrictions are implemented in almost all networks. Presently a violation of line restrictions is modelled as an error which leads to the PIC O_exception. It should be possible to allow a per-call basis overriding of these restrictions after entering a password.

- Menu driven user interaction (MEDUI): Display of information by the user's terminal, with the possibility to perform menu driven user interaction. Service to user information is presented graphically, while the user communicates towards the service via the dial-pad.

- Modem Detection During User Interaction (MDDUI): When performing prompt and collect user information, e.g. when offering a random call service via IN (using network initiated call followed by connection to a SRF), one of the possible error conditions from service perspective is that the dialled number is connected to an analogue fax or other modem. The SRF detects this, and informs service logic that a modem was encountered.

- Screening Service with an Open Numbering Plan (SCONP): A screening service can be provided in an open numbering plan environment, that is, a numbering plan with variable number length. This implies that the SCF cannot always know how many digits are to be expected still.

- Simultaneous User Interaction (SIMUI): When party A calls party B, party A can initially hear, for example, a Ring Back Tone from party B's local exchange. As soon as party B answers, an announcement is played immediately to both party A and B. These announcements are not necessarily the same.

- Time announcement and disconnect (TADIS): The user receives an announcement that he will be disconnected after a certain period, and is subsequently disconnected after that period. This could for example be used in combination with prepaid charging method, where this feature is activated on credit limit expiry.

- Triggering on Call Failure Condition (TRCFC): If a Call Failure condition is detected early by a service logic in a certain node (e.g. by user profile consultation, rather than late through an ISUP Release message), it should be possible to use this as a trigger for services located in a different node.

- VPN Node Interface (VPNNI): Private networks (e.g. PBXs) can exchange VPN information (PSS1) via the signalling in the public network (via the Application Protocol transport Mechanism of ISUP). Service providers shall be able to monitor and control the use of this capability.

- The public network can terminate the VPN PINX context, and provide outgoing gateway PINX functionality depending on the functionality supported by (or required to reach) the called party, or depending on e.g. subscriptions.

Interworking between IN and IP networks

- Request-to-Call-Back CSN (RTCBC): A user is able to initiate a telephone call by clicking a button during a Web session. The call can be first set up in the direction of the requester of the call, or first be set up in the direction of the party the requester wants to be connected to. E.164 addressing for both A-party and B-party is assumed, and both parties are assumed to be connected to the Switched Circuit Network.

- Request-to-Call CSN (RQTCC): A user is able to initiate a telephone call by clicking a button during a Web session. The requested call is to be set up between two parties identified by E.164 addresses, which are connected to the Switched Circuit Network. The requester him/herself may or may not take part in the call to be set up.

Personal and terminal mobility support

- UPT registration with smart card (SCREG): a UPT user can register with the telecommunications network by using a smart card.

- UPT Originating Call without registration (UOCWR): a UPT user registers him/herself from a certain terminal, and can from then on make UPT calls without explicit per-call identification. In the meantime other users can use the phone for their calls as well, without being identified as the UPT user.

- User Identity Confirmation (USIDC): feature enabling a user to confirm its identity to a network. This confirmation can be requested by the network prior to service invocation, or in an early phase of the service offering, call related or call unrelated.

- Network Identity Confirmation (NWIDC): feature enabling a network to confirm its identity to a user. This shall be provided to the user in case of user registration in the case of a roaming user. It can also be provided prior to service invocation, or in an early phase of a service offering, call related or call unrelated.

- Non-Repudiation (NOREP): the capability of the network or service provider to provide a proof of use towards a user of his services and resources. Some capabilities are provided in present day systems, like storage of data including PIN codes in the SCF/SDF.

- Call Forwarding on Not Reachable Condition (CFNRC): enables a served user to have the network redirect calls which are addressed to the served user's directory number to another directory number, in case the served user is not reachable. The CFNRC IN service operates on all calls. After the CFNRC service has been activated, calls are forwarded only if the served user is not reachable via the dialled directory number, e.g. user's cordless terminal is not reachable.

IN support for B-ISDN

- Point-To-Point Communication - Connection Type 1 (PTPCO): The possibility to set up either unidirectional or bidirectional point-to-point connections between two points involved in the call.

Number Portability

- Service Provider Portability for geographical numbers (SPPGN): Number Portability for geographic numbers enables subscribers/ customers/companies to retain their well-known directory numbers if they want to change service provider.

- Service Provider Portability for non-geographic numbers (SPPNG):Number Portability for non-geographic numbers as nationwide freephone and premium rate services enables subscribers/customers/ companies to retain their valued freephone and premium access numbers if they want to change service provider.

- Location Portability (LOCNP): Location Portability enables subscribers to retain the same directory numbers when moving from one location to another.

Network capabilities of IN CS-3 according to [92].

Basic features

- ASE-Support (ASESP): IN connection establishment support for TC-based supplementary services of which the ASE is located in the CCF/CUSF.

- Carrier Identification Transfer (CAIDT): When the network requests connection setup support from IN, and when IN requests the network to set up a call, it shall be possible to transfer some carrier identification information. This capability already exists in IN CS-2, but is an enhancement due to ISUP enhancements.

- Call Initiation towards SRF (CISRF): It shall be possible to initiate a call towards a remote SRF, while passing the SCF_ID and Correlation_ID information in order for the SRF to report back to the SCF.

- Call Reference for Call Detail Record (CRCDR): The possibility to convey a unique call reference ID between the SCF and SSF, for both network and user initiated calls. The call reference shall be globally unique. This Call Reference shall appear in Call Detail Records produced by SSF and SCF.

- Geodetic Information Support (GEOIS): In ISUP a new parameter with detailed location information will be defined. The location information related to the calling party can be made available to the service logic.

- Information Exchange Between Service Logic Programs (IEBSL): This capability enables the exchange of information between different Service Logic Programs which are subsequently invoked on the same call. The SLPs might be located in different SCPs, and might be invoked from different SSPs.

- Inter SCP Service to Service Information (ISSSI): In case the SCF functionality is distributed, e.g. over different operator domains, two different SCPs shall be able to exchange Service to Service Information (SSI) within an established SCF-SCF relationship. The mechanism to exchange service specific data shall be bidirectional, flexible and generic.

- Inhibition Of Call Waiting Indication (IOCWI): The ability for a service logic to inhibit the invocation of the switch based call waiting service.
- Logical Referral plus Language Choice for Voice User Interaction (LRLCV): For all voice user interaction it is possible to refer to the message in the SRF via a logical reference, and select the language via a separate parameter. This includes voice user interaction related to call gapping and filtering.
- Modem Detection Request (MODDR): When requesting the SRF to perform a prompt and collect user interaction, the SCF requests the SRF to perform a check on the presence of a modem (e.g. analogue fax), and to stop user interaction and report back when this situation occurs.
- Multiple points of control (MPCTR): More than one service logic programs are allowed to act on the same (half) call (Retriggering in same SSP).
- Multiple points of control User Interaction (MPCUI): An SCF shall be able to request an SSF to connect a resource (for User Interaction) on one leg of call already involved in another User Interaction. The SSF shall be able to either disconnect the bearer of the existing User Interaction and connect the bearer to the requested User Interaction or reject the request based on conditions previously established for the initial User Interaction.
- Non-call-related USI (NCRUS): Support for the transport of User to Service Information (USI), also for non call related IN invocation.
- The call unrelated support for transfer of a number in a private numbering plan where such a number is used in the interaction between two public network services (e.g. CCBS, GVNS).
- SCF Control Less Digits Received (SCLDR): Allows the SCF to receive a report of collected digits, when complete called party number has been determined in the CCF/SSF and the SCF does not know the exact number of digits to be collected, e.g. due to an open Numbering Plan.
- The SCF requests the SSF for a certain number of additional digits, while indicating the SSF not to clear the call if a timeout occurs before the requested number of digits is received, but to give control over the call-back to the SCF.
- INAP interworking with Server Display Script Services (SDSSI): The SCF controls Server Display Script Services (SDSS) information exchange between the user terminal and the SDSS application.
- The SDSS protocol on the analogue interface (V23) is presently used to enhance the User Interface ergonomy of PSTN supplementary services located in the switch.
- Terminal Alerting before data transmission (TABDT): Before sending data to a terminal, e.g. SDSS information, an alerting signal is sent to the terminal (and acknowledged). The role of this signal is to notify the terminal equipment that data transmission is expected, while avoiding unwanted bell tinkle.
- Timed Disconnect (TIMED): It shall be possible to instruct the SSF to release the call after an indicated amount of time.
- USIServiceIndicator as DP criterion (USITR): It shall be possible to use a certain value of the USIServiceIndicator as one of the Trigger Detection Point criteria, for both call related and call unrelated service triggering.
- VPN notification (VPNNO): It shall be possible for an SSF to notify an SCF providing an IN VPN service that the use of the network capability to transport PSS1 signalling enhancements to basic call is present in the received call request message.
- VPN control (VPNCO): An SCF providing an IN VPN service shall be able to instruct the SSF to prohibit or allow the use of the network capability to transport PSS1 signalling enhancements to basic call. When this control is used, the VPN with the PSS1 APM is correctly terminated, and the SCF and SSF shall cooperate to provide outgoing gateway PINX functionality according to PSS1 information flows. If this control is not used Transit PINX is the default functionality.

Personal and terminal mobility support

- Dynamic TriggerDetectionPoint activation/deactivation (DTDPA): It shall be possible to activate/deactivate several existing TDPs in the SSF. Hence more than one TDP may exist at the same DP. It shall be possible to activate/deactivate these TDPs on a per-call basis.

- Dynamic TriggerDetectionPoint loading (DTDPL): It shall be possible to create a new TDP in the SSF by downloading SSF triggering information associated with the newly created TDP. The TDP can either be active immediately, or require explicit activation later. In case of terminal mobility or user mobility this capability can be used to implement dynamic geographic placement of statically armed DPs.

- SCP address transfer (SCPAT): A requesting Functional Entity in the visited network shall be able to address the Home Networks SCP. Relevant in case of home based services.

Interworking between IN and broadband networks

- Point-To-Point Connections (APTPC): Only simultaneous call and connection setup, bidirectional point-to-point connections are supported, multimedia communication shall be supported at call/connections setup.

- Network Initiated Point-to-Point Connection (NIPTP): Establishment and release of point-to-point bidirectional connection via invocation of B-ISDN signalling.

- ATM Traffic Capabilities Control (ATMTC): For network initiated B-ISDN connections IN shall be able to control the Quality of Service at call setup. The presently defined QoS classes and associated parameters as specified in ITU-T Recommendation I.356 [109] shall be supported for the ATM Traffic Capabilities ATM Block Transfer (ABT), DBR, SBR and ABR, as defined in ITU-T Recommendation I.371 [110].

- ATM Traffic Capabilities Notification (ATCNG): The possibility to report to the SCF a notification of the traffic parameters for the indicated, modified and negotiated ATM Traffic Capabilities. The notification is only provided in InitialDP and connect message.

- Support for AESA Addressing (ASEAA): Apart from the native E.164 numbering, the non-E.164 ATM Service Endpoint Addressing as presently defined by ITU-T Study Group 2 shall be supported in the operations relevant for IN number translation requests.

- SCF triggering from B-ISDN Signalling (ATMTR): Trigger processing and parameter population rules appropriate for DSS2 and B-ISUP support shall be provided.

There shall be only one control relationship to B-ISDN Signalling per half call.

Number portability

- Number Portability ISUP Enhancements Support (NPTIES): For the support of Number Portability new ISUP parameters are defined, containing either Directory Number (DN) or Network Routing Number (NRN), depending on network choice. It shall be possible to perform a NP database query via INAP and to provide the appropriate Routing Number for a ported number via INAP to the SSF.

- Network Routing Number Trigger (NRNTR): It shall be possible to trigger on the Network Routing Number and it shall be possible to make this parameter available to IN services, and/or change it by IN services.

5.1.3.8.1.1 ETSI (INAP:)

[63] defines the Intelligent Network Application Protocol (INAP) required for support of Capability Set 1 (CS1). It supports interactions between the following three Functional Entities (FEs), as defined in the Intelligent Network (IN) functional model:

- Service Switching Function (SSF);

- Service Control Function (SCF);

- Specialized Resource Function (SRF).

The scope of this ETS is the further development of the INAP for both the Integrated Services Digital Network (ISDN) and Public Switched Telecommunications Network (PSTN). It is intended as a guide to implementers and network operators to ensure interworking between different manufacturers' equipment for the IN CS1 defined interfaces (SCF-SSF and SCF-SRF).

[64] defines the Intelligent Network Application Protocol (INAP) required for support of Capability Set 2 (CS2). It supports interactions between the following five Functional Entities (FEs), as defined in the Intelligent Network (IN) functional model:

- Service Switching Function (SSF);
- Service Control Function (SCF);
- Service Data Function (SDF);
- Call Unrelated Service Function (CUSF);
- Specialized Resource Function (SRF).

The further development of the INAP for each of the Integrated Services Digital Network (ISDN) and Public Switched Telecommunications Network (PSTN) and Public Land Mobile Networks (PLMN) is covered by the present document, which is intended as a guide to implementers and network operators to ensure interworking between different manufacturers' equipment for the following IN CS2 defined interfaces:

- SCF-SSF;
- SCF-CUSF;
- SCF-SRF;
- SCF-SDF;
- SCF-SCF; and
- SDF-SDF.

The scope of the IN Distributed Functional Plane (DFP) architecture (see [65] and supporting protocol for IN capability set 3 (IN CS-3) is driven by the requirements of the services desired for IN CS-3, and constrained by the capabilities of the embedded base of network technology. The functionality required to support IN CS-3 services includes functionality to provide:

- end user access to call/service processing;
- call-related service invocation and control;
- end user interaction with service control;
- service management;
- Call Party Handling;
- Internetworking;
- Security;
- Out-Channel User Interaction;
- call unrelated service invocation and control; and
- Feature Interactions.

5.1.3.8.1.2 3GPP

CAP (CAMEL Application Part)

[81] specifies the compatibility mechanisms that shall be used for CAP concerning INAP as specified by ETSI and ITU-T.

Two major categories of compatibility are handled by these mechanisms:

- compatibility with the ITU-T Recommendation Q.1228 [51] version of CS2 INAP and the specification EN 301 140-1 version of CS2 INAP [26];
- compatibility with future versions of CAP.

Organization of end-user data:

The following data related to CAMEL is specified in [2] and represents the way that 3GPP supports IN systems. These are data stored in the HLR, VLR and SGSN. Data stored in the SCP are not subject to standardization at the moment.

- Subscriber Data stored in HLR:
  - Originating CAMEL Subscription Information (O-CSI).
  - Terminating CAMEL Subscription Information (T-CSI) and VMSC Terminating CAMEL Subscription Information (VT-CSI)).
  - Location information/Subscriber state interrogation.
  - USSD CAMEL subscription information(U-CSI).
  - Supplementary Service invocation notification(SS-CSI).
  - Translation Information flag (TIF-CSI).
  - Mobility Management event notification (M-CSI).
  - Mobile Originated Short Message Service CAMEL Subscription Information (MO-SMS-CSI).
  - Mobile Terminating Short Message Service CAMEL Subscription Information (MT-SMS-CSI).
  - GPRS CAMEL Subscription Information (GPRS-CSI).
  - Dialled service CAMEL Subscription Information (D-CSI).
  - Mobility Management for GPRS event notification (MG-CSI).
- Other Data stored in the HLR:
  - Negotiated CAMEL Capability Handling.
  - Supported CAMEL Phases.
  - Offered CAMEL4 CSIs.
  - UG-CSI.
  - gsmSCF address for CSI.
- Subscriber data stored in VLR:
  - Originating CAMEL Subscription Information (O-CSI).
  - VMSC Terminating CAMEL Subscription Information (VT-CSI).
  - Supplementary Service invocation notification(SS-CSI).
  - Mobility Management event notification (M-CSI).

- Mobile Originating Short Message Service CAMEL Subscription Information (MO-SMS-CSI).
- Mobile Terminating Short Message Service CAMEL Subscription Information (MT-SMS-CSI).
- Dialled service CAMEL Subscription Information (D-CSI).
- Translation Information flag (TIF-CSI).

- Data stored in SGSN
  - Mobile Originating Short Message Service CAMEL Subscription Information (MO-SMS-CSI).
  - Mobile Terminating Short Message Service CAMEL Subscription Information (MT-SMS-CSI).
  - GPRS CAMEL Subscription Information (GPRS-CSI).
  - Mobility Management for GPRS event notification (MG-CSI).

5.1.4 Generic User Profile (GUP)

5.1.4.1 General Ideas

Because of:

- the several domains within the 3GPP mobile system core and access technologies (which lead to a wide distribution of data associated with the end-user); and
- new functions both in terminals and networks (which leads to an increase in data related to Users, Services and User Equipment);

difficulties for Users, Subscribers, network Operators and Value added service providers to create, access and manage the user-related data located in different entities can be expected.

Thus 3GPP defines a Generic User Profile [54] in order to provide a means to enable harmonized usage of the user-related information originating from different entities. It represents a collection of User-related data which influence individual user experiences services where a community of entities share this data. The 3GPP Generic User Profile can be stored in the home network environment and/or Value Added Service Provider equipment.

The 3GPP Generic User Profile will be accessed by different stakeholders:

- Subscriber: The subscriber may hold subscriptions for one user (e.g. in the case the subscriber is identical with the user) or several users (e.g. in the case of a company - the subscriber - holding subscriptions for it's employees - the users)
- User: The user may or may not be identical with the Subscriber.
- Value Added Service Provider.
- Home Network Operator.
- Roamed-to Network Operator.
- Regulator.

GUP will be managed either:

- by one (centralized); or
- by different stakeholders (de-centralized), such as the:
  - user;
  - subscriber;
  - value added service provider; and

- network operator by a standardized access mechanism.

The 3GPP Generic User Profile allows data exchange between applications within a mobile operator's network and between mobile operator's network and value added service providers.

The 3GPP Generic User Profile may be also be used by different applications in a standardized way.

For each user, one User Profile exists, which may consist of several 'components' distributed in the home network and value added service provider's environment. Within the home network, the components may be distributed in various network nodes. Only one master of the component exists, but one or more copies of the master component may exist. The home operator shall be able to copy master components, which are located outside the home network to the home network. Within the home network, functionality exists that is able to locate GUP components, thereby making applications unaware of the actual location of the components. The administration and management of the data associated with this functionality is under the control of the home network. Although GUP does not attempt to provide an actual classification of the data it may contain, one may consider categorizations such as:

- Authorized and subscribed services information: generally owned by the home operator and allow management and interrogation of subscription information and would typically consist of:
  - authorized services that the subscriber may subscribe to;
  - services the subscriber actually has subscribed to.
- General user information: Data, owned by the user, which are not specific to individual services, but may be useful for any service. These would be data like:
  - settings (e.g. name, postal address), preferences (e.g. language);
  - Registered Service Profiles of the user, indicating the currently active Service Profile of the user.
- PLMN specific user information: Data, owned by the home operator, which are not specific to individual services, but may be useful for any service. These typically would be data like:
  - addresses (e.g. MSISDNs, URLs) of the user;
  - WAP parameters (e.g. standard WAP gateway);
  - GPRS parameters (in UE and HSS);
  - Preferred access technologies (The preferred access technology, second preferred access technology etc. e.g. UTRAN, GERAN, WLAN, etc.).
- Privacy control data of the user: specific to individual services and which control privacy settings of that service. These could e.g. be
  - Privacy settings for standardized services like the Presence service or Push service.
  - Privacy settings of non-standardized services.
- Service specific information of the user: Data, owned by the user or value added service provider, which are specific to individual services (standardized or non-standardized). These could e.g. be:
  - Service customization data of the user.
  - Service authentication- and authorization data (for "single sign on") like keys, certificates, passwords, etc.
- Terminal related data: data, which relate in particular to the user's terminals (ME and UICC). These could e.g. consist of:
  - Terminal capabilities of the terminal currently in use (e.g. User Interface capabilities, communication capabilities, available services, service capabilities, etc.).
  - Data for initial configuration and/or reset of the ME.
  - Backup data for recovery of the ME configuration including service specific data.

- Charging and billing related data: consists of information necessary for the user related charging and billing. This data could e.g. consist of:

  - The billing policy.

The following data categories are not considered to be useful for the 3GPP Generic User Profile:

- Run Time Data.: Data that are created during the initiation of the session, call or application execution and if they are only available during the lifetime of such session, call or application execution then they are considered as Run Time data.

- Historic/Statistic Data.: User/system behaviour information (e.g. statistics on the usage preferred web pages; duration, number of calls, error rate).

The GUP reference architecture [11] as shown (see figure 5.1.4.1.1) consists of:

- GUP Server: functional entity providing a single point of access to the Generic User Profile data of a particular subscriber. The reference architecture does not specify or limit the physical location of the GUP Server enabling flexibility in the implementations. The GUP Server shall be located in the home operator network of the targeted subscriber. The GUP Server may support two modes of operation:

  - Proxy Mode.

  - Redirect Mode.

- Repository Access Function (RAF): The Repository Access Function (RAF) realizes the harmonized access interface. It hides the implementation details of the data repositories from the GUP infrastructure. The RAF performs protocol and data transformation where needed.

- GUP Data Repositories: Each GUP Data Repository stores the primary master copy of one or several profile components. The RAF provides for the standardized access to the GUP Data Repository. The storage formats or the interface between the RAF and GUP Data Repository are not specified by GUP.

- Rg and Rp reference points:

  - Rg: This reference point shall allow applications to create, read, modify and delete any user profile data using the harmonized access interface. The GUP Server locates the data repositories responsible of the storage of the requested profile component(s) and in case of proxy mode carries out the requested operation on the data.

  - Rp: This reference point shall allow the GUP Server or applications, excluding external applications (e.g. located in a third party application or in the UE), to create, read, modify and delete user profile data using the harmonized access interface. Rp is an intra-operator reference point.

- Applications: The applications that may apply GUP reference points Rg and Rp may be targeted for different purposes e.g. for value added services or subscription management. Both operator's own applications and third party applications are covered. The latter ones shall apply Rg reference point.

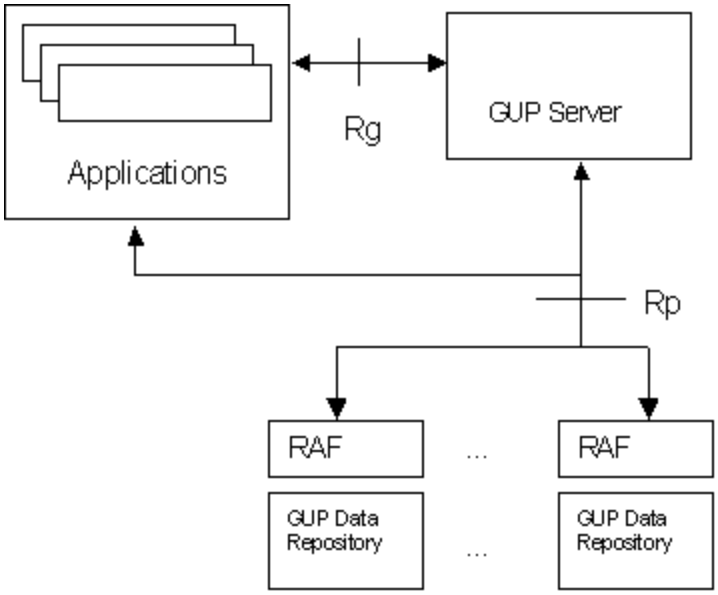


Figure 5.1.4.1.1: GUP Architecture according to 3GPP [11]

The following is a short excerpt of the description of the information model for GUP [11]. A Generic User Profile consists of independent components. A GUP Component may contain (i.e. reference) other GUP components e.g. to enable reuse of data.

The GUP Component has a unique identity within the Generic User Profile. In addition to the component type the component identity contains either a subscriber identity or more generic identification depending on which kind of component is in question. A GUP Component can be retrieved through one RAF, and it may consist of a number of GUP Components, Data Element Groups and/or Data Elements.

A GUP Component contains zero or more Data Element Groups. The Data Element Group contains indivisible Data Elements and/or Data Element Groups. The nested Data Elements Groups allow deeper hierarchical structures. The Data Element Group in the lowest hierarchical level contains one or more Data Elements. The Data Element Groups inside a GUP Component may be of the same or different types.

Alternatively the GUP Component may contain zero or more Data Elements without the Data Element Groups. A GUP component shall have at least one Data Element Group or Data Element.

A Composite Datatype is used to define the structure of the whole GUP Component. The structure includes definition about what kind of Data Element Groups and/or which Data Elements belong to the defined GUP Component as well as the data types and valid values of the data.

Figure 5.1.4.1.2 illustrates the basic concepts of the GUP Information Model.

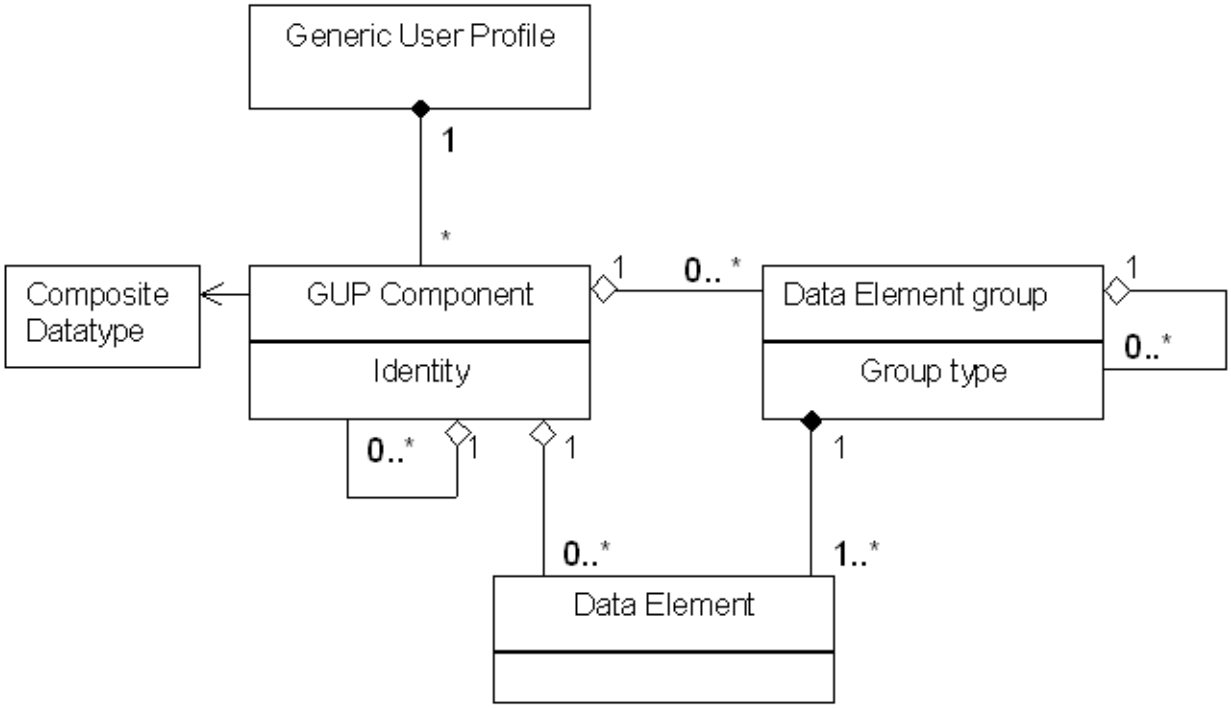


Figure 5.1.4.1.2: GUP Information Model according to 3GPP [11]

[55] shows, how a model can be specified. The essential contents of the present document describe the functionality, semantics and the WSDL/XML definitions of the interfaces. Additionally the special characteristics of the SOAP and http usage are defined. It is worth noting that part of the data is passed in the SOAP headers but the most GUP specific data is placed in the SOAP message body.

The protocol architecture of the Rg reference point is depicted in figure 5.1.4.1.3.

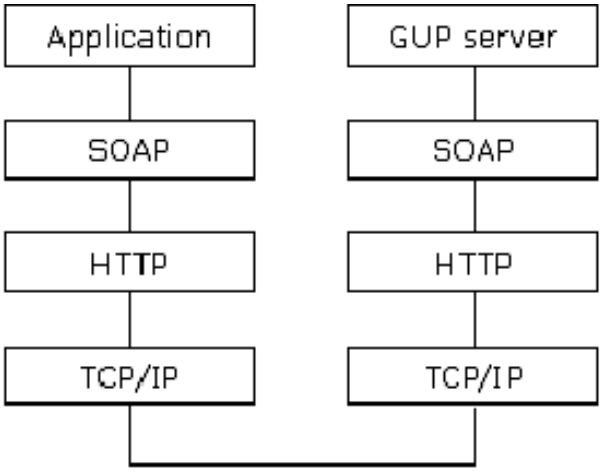


Figure 5.1.4.1.3: GUP Rg reference point according to 3GPP [55]

The protocol architecture of the Rp reference point is depicted in figure 5.1.4.1.4.

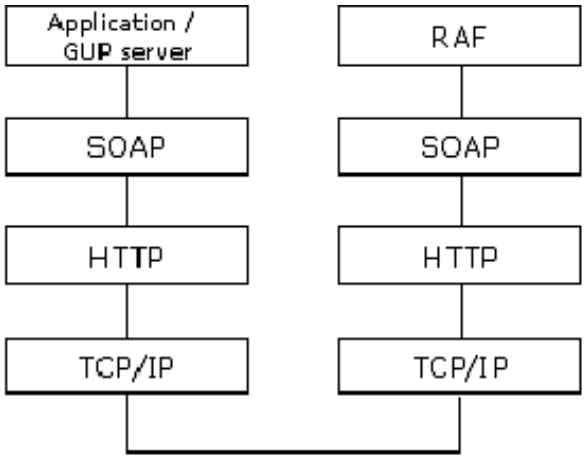


Figure 5.1.4.1.4: GUP Rp reference point according to 3GPP [55]

- Application layer:
  - Application level interface specification. All the operations and data are described by XML elements and attributes in an XML Schema and WSDL.
  - The standard XML Schema is defined by W3C in "XML Schema Part 1: Structures", Recommendation and "XML Schema Part 2: Datatypes," Recommendation.
- SOAP (Session layer):
  - SOAP is an XML based messaging protocol that provides support for remote procedure calls by messaging.
  - A few specific header types are defined for GUP e.g. for message IDs and time stamps.
- HTTP (Transport layer):
  - HTTP defines how messages are transmitted and formatted.
- TCP/IP (Network layer):
  - TCP/IP handles network communications between network nodes. GUP does not define any special requirements for this layer.

5.1.5 Management Applications

5.1.5.1 Subscriber Management

5.1.5.1.1 ITU-T

In [94] ITU-T describes its management philosophy and lists the tasks for each of the management layers it defines. ITU-T does so by identifying functions and function sets.

In the annex of [94] some scenarios are described, which show, how the functions and function sets are related to each other. As one topic ITU-T deals with customer administration.

- Service activation:
  - Scenario 1: This scenario incorporates many activities of all FCAPS areas associated with service activation. As a result, ITU-T regards it more of a reference scenario than a view of an actual sequence of activities.

This flow is triggered by a customer request for service. While the scenario explicitly illustrates a request to activate new service, the flow is similar for making changes to existing service and discontinuing service. The request may be made by a person or via a machine-to-machine interface.

- Scenario 2: ITU-T assumes that all equipment is in place and that activation will occur at the time of assignment (i.e. immediately). As with scenario 1, this flow is triggered by a customer request for service. While the scenario explicitly illustrates a request to activate new service, the flow is similar for making changes to existing service and discontinuing service.

- Service change:
  - Scenario 3: this scenario shows how a customer may make changes to the services under his control and how those changes may affect the network. A customer with network management capabilities initiates a request to activate existing capacity that has been designated for his use.

- Status of service information:
  - Scenario 4: A customer with network management capabilities initiates a request to see the status of their network.
  - Scenario 5: A similar flow could be initiated by Notification of state changes in NEs and would be used to provide automatic notification of network information to the customer. The NE would initiate the flow and the information about the state change would flow up.

- Trouble report:
  - Scenario 6: A customer reports a trouble to Trouble Administration. The service and underlying infrastructure is tested and reported, if appropriate to fault correction. This scenario is somewhat complex, with some branching of the flow. The scenario ends with clearing of the fault.

5.1.5.1.2 3GPP

According to [6] SuM shall permit Service Providers and Operators to provision services for a specific customer service subscription.

Specific areas of attention are:

- Subscription information is distributed across in a number of locations.
- Service Providers and Operators have to be able to provision, control and monitor the subscription information.
- SuM has to link together features across multiple Operators' Operations Support Systems (OSSs).
- SuM will need to manage subscription information in e.g. the OSSs, HSS, UE, OSA, MMS and IMS subsystems.
- The common components between the GUP and the subscription profile.

Specific attention is drawn to the alignment with TMF. 3GPP's SuM, in particular the configuration of resources, aligns with subset of the TOM model in the area of fulfilment.

Architecture:

[7] defines the architecture for Subscription Management (SuM), which can be found in figure 5.1.5.1.1.1.

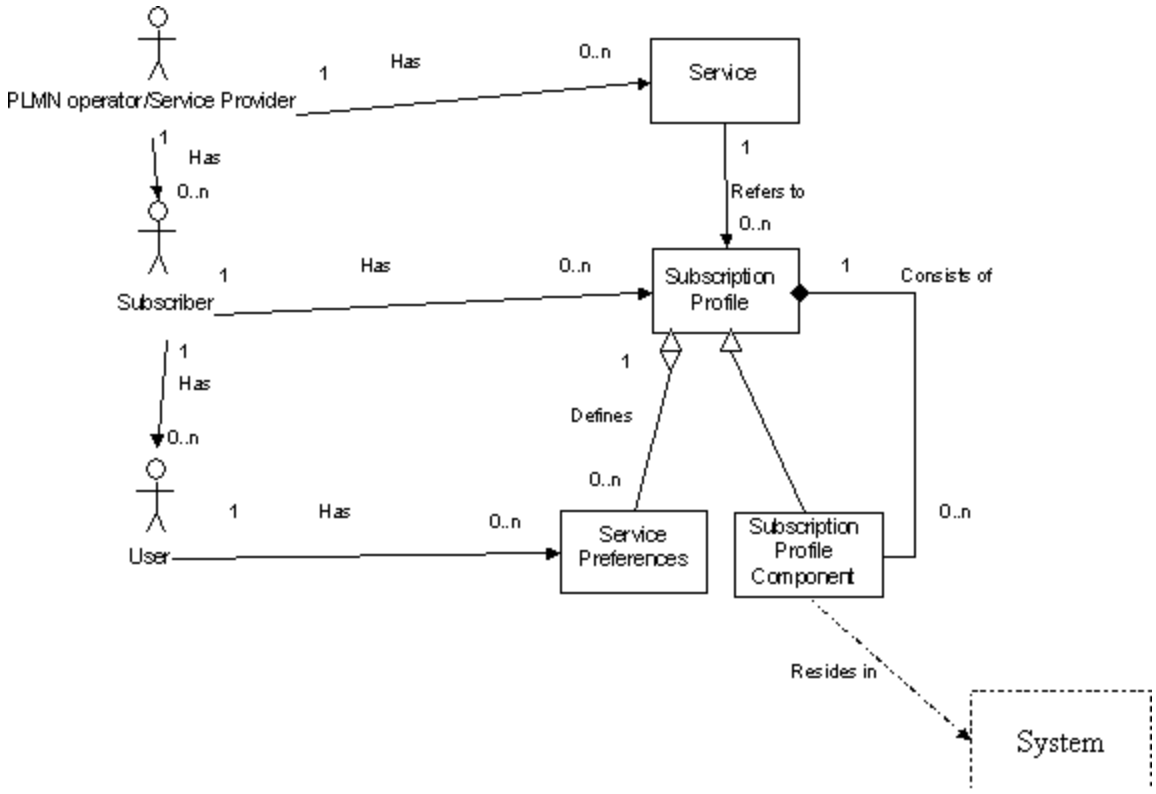


Figure 5.1.5.1.1.1: SuM functional entities according to 3GPP [7]

In [7] 3GPP deals with the SuM - OSF functionality contained in the Core Network Basic Entities Domain and specifically with the one of the Common CN Domain. Subscription Profile Components are located in the NEs' OSFs within the Common CN Domain or their NEs' OSFs in the NE management systems as shown in figure 5.1.5.1.1.2.

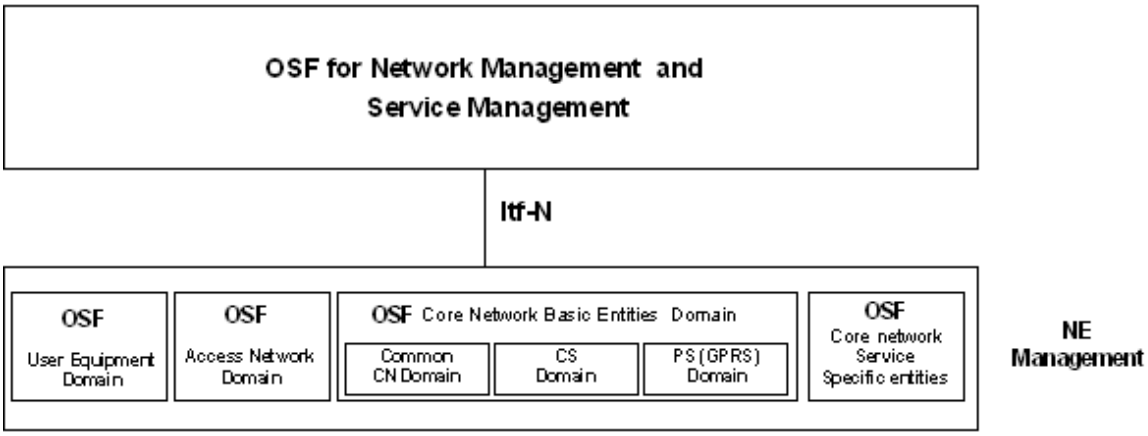


Figure 5.1.5.1.1.2: PLMN Telecom Management Domains according to 3GPP [7]

According to [7] access to the Subscription Profile Components are based on the IRP (Integration Reference Point) manager-agent concept.

An IRPAgent implements and supports this (SuM) IRP. The IRPAgent can reside in an Element Manager (EM) or a Network Element (NE).

An IRPManager using this SuM-IRP shall choose one of the two System Contexts defined.

According to [7] IRP security shall be achieved by controlling access to the network and management systems .

[7] suggests the reuse of GUP stage 3 for SuM IRP Solution Sets where possible. An interpretation of the relationship of Itf-N realization (for SuM) to the GUP reference architecture.

[9] defines the Network Resources Model (NRM) for the SuM IRP. In detail the meaning of Mandatory and Optional IOC attributes and associations between IOCs is defined for the following Solution Sets to the IRP.

Solution Sets to the SuM IRP:

- The IRPManager shall support all Mandatory attributes/associations. The IRPManager shall be prepared to receive information related to Mandatory as well as Optional attributes/associations without failure; however the IRPManager does not have to support handling of the Optional attributes/associations.
- The IRPAgent shall support all Mandatory attributes/associations. It may support Optional attributes/associations.

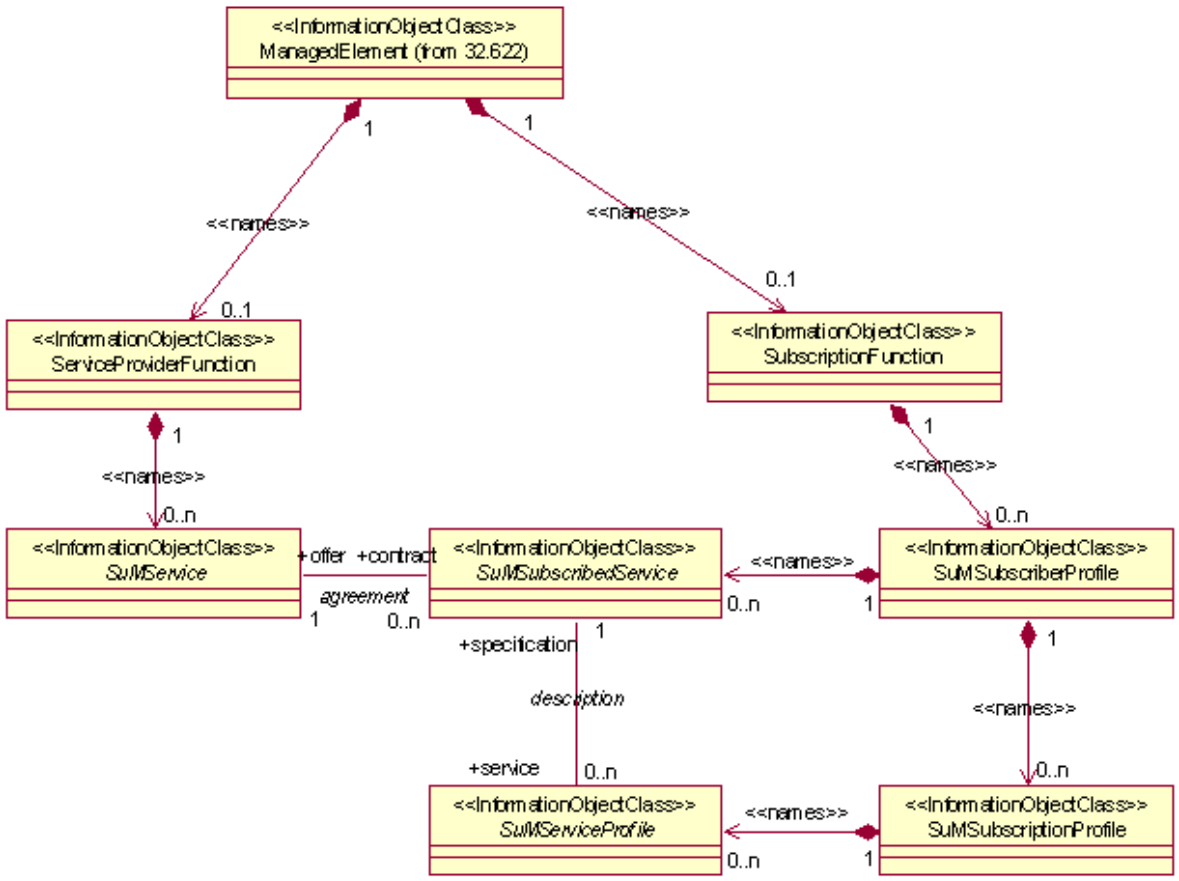


Figure 5.1.5.1.1.3: SuM NRM Containment/Naming according to 3GPP [9]

[9] defines the Naming Hierarchy and relations between the modelled entities (see figure 5.1.5.1.1.3 for an example) as well as the inheritance (see figure 5.1.5.1.1.4 for an example), which are both copies from [9].

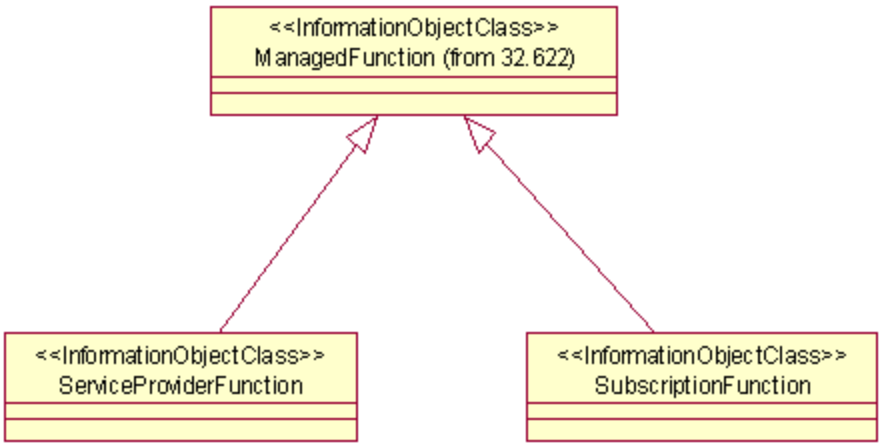


Figure 5.1.5.1.1.4: SuM NRM Inheritance Hierarchy according to 3GPP [9]

5.1.5.1.3 3GPP2

Subscription management in [28]. treats the various topics related to subscription management in the functional parts they belong to.

Architecture

AAA functionality:

- Authentication Function: provides Authentication of terminal devices and subscribers.
- The Authorization Function: provides authorization of requests for services and/or bandwidth, etc. and has access to the Policy Repository, the Directory Services, Subscriber Profiles, and the Device Register.
- The Accounting Function: gathers data concerning the services, QoS, and multimedia resources requested and used by individual subscribers.

Data Base:

The DB is a network component that may support both the Multimedia and Legacy MS Domains. The information in the core network DBs may include but is not limited to:

- EIR;
- Dynamic Subscriber Information;
- Network Policy Rules; and
- Subscriber Profile data;
- The Legacy MS Domain Support.

The HLRe manages the subscriber profile for both:

- voice services (e.g. Call Forwarding, Three Way Calling, Message Waiting Notification); and
- data services (e.g. Priority). Subscriber profile information may be accessed from the HLRe or may be downloaded to a serving system as needed.

The HLRe manages subscriber location and/or accessibility information. This includes updating the dynamic subscriber information database with current domain information (e.g. MSCe address) and with MS status information (e.g. SMS pending flag). The HLRe interacts with the location database to update or retrieve current location information.

The MRFC, in conjunction with the MRFP, provides a set of resources within the core network that are useful in supporting services to subscribers. The MRFC, in conjunction with the MRFP, provides multi-way conference bridges, announcement playback services, tone playback services, etc.

The MRFC controls allocation, de-allocation, and modification of the usage of resources of the MRFP.

Reference Point m4 is the management interface between OSF-EML / OSF-NML/OSS and 3GPP2 NAM Databases, such as Network Policy Rules and Subscriber Profile (applicable definitions provided by S.S0028-A).

The MS is a wireless terminal used by subscribers to access the Legacy MS Domain or the IP Multimedia Domain services over a radio interface. MSs include portable units (e.g. hand-held units), units installed in vehicles, and somewhat paradoxically, fixed location MSs. The MS is the interface equipment used to terminate the radio path at the subscriber. A MS is a ME with a programmed UIM.

The Legacy MS Domain provides support for existing MSs (e.g. analog, IS-95-A, IS-95-B, cdma2000) in an IP core network environment. This domain supports the features and capabilities provided in a legacy network in a manner transparent to the user. New features and capabilities supported by the IP core network may be made available to subscribers where they are supported by the MS capabilities.

Services supported on the SCP make use of information stored in the Databases component of the core network, including subscriber information, and may interact with service applications.

The Service Management System (SMS) provides overall service management functionality for the network. Service providers and third party application developers may use different versions of the SMS. The SMS interacts with the SCE and other entities to perform service provisioning, monitoring, testing, deployment, and subscriber data management functions.

5.1.5.1.4 TISPAN

According to TISPAN [25] Subscription Management is a key feature that allows:

- service providers and operators to provision their TISPAN NGN network entities with the data necessary for delivering services for a specific subscriber; and
- subscribers to configure their services when they have this capabilities.

Starting point of TISPAN'S Subscription Management is the 3GPP IRP concept (with slight modifications) and the 3GPP specifications on Subscription Management. TISPAN's Subscription Management also aligns with subset of the eTOM fulfilment process.

TISPAN sees Subscription Management as tool for the service providers to leverage their network resources to:

- Validate (register, authenticate, and authorize.) a request for service from a user;
- Collect, store, update, and distribute the Service Profile information for the user;
- Select the trusted network resources to manage access, distribution, and control of the profile data information for the user; and
- Direct the network resources to promptly deliver the service requested to the user according to said profile information.

Subscription management fulfils the following essential TISPAN NGN requirements [25]:

- The "User equipment Diversity" allows the users to access their TISPAN NGN services by a variety of UEs.
- The "Service Diversity" allows the users to access TISPAN NGN services provided by service providers or third party application server providers.
- The "Access Diversity" allows the users to access their TISPAN NGN services over a wide variety of network access such as xDSL, WLAN, GPRS, etc.
- Nomadism: allows the users to access their TISPAN NGN services in multiple nomadism scenarios.

At present [80] contains the specification of the requirements for the following:

- An end-to-end information model to cover all the mandatory/optional information related to subscription management that shall be provisioned on the NGN Network.

- A subscription management functional architecture which hides the complexity of the different functional entities to be configured including the CPE and the AS.
- Only Service Configuration and Activation aspects are addressed within this first release of [25].

In [25] Subscription Management is seen as the framework that offers service providers the means for efficient management of all the data related to a specific subscription.

As depicted in figure 5.1.5.1.3.1, the SuM framework is responsible for handling only the data related to the service delivery of a specific subscription. Moreover, the data provisioned thanks to the subscription management framework can also be used in other mechanisms such as monitoring, billing, etc.

Subscription Management framework, as shown in figure 5.1.5.1.3.1, involves the following entities:

- Service Provider : offers a set of services.
- Subscriber: may subscribe to one ore more services. The service provide will have then to manage the corresponding subscription by provisioning the necessary data and giving the following rights to the subscriber:
  - To become a user by using the services.
  - Give rights to its users, who will be then linked (or associated) to this subscription.
- User: use the authorized services.
- Services.

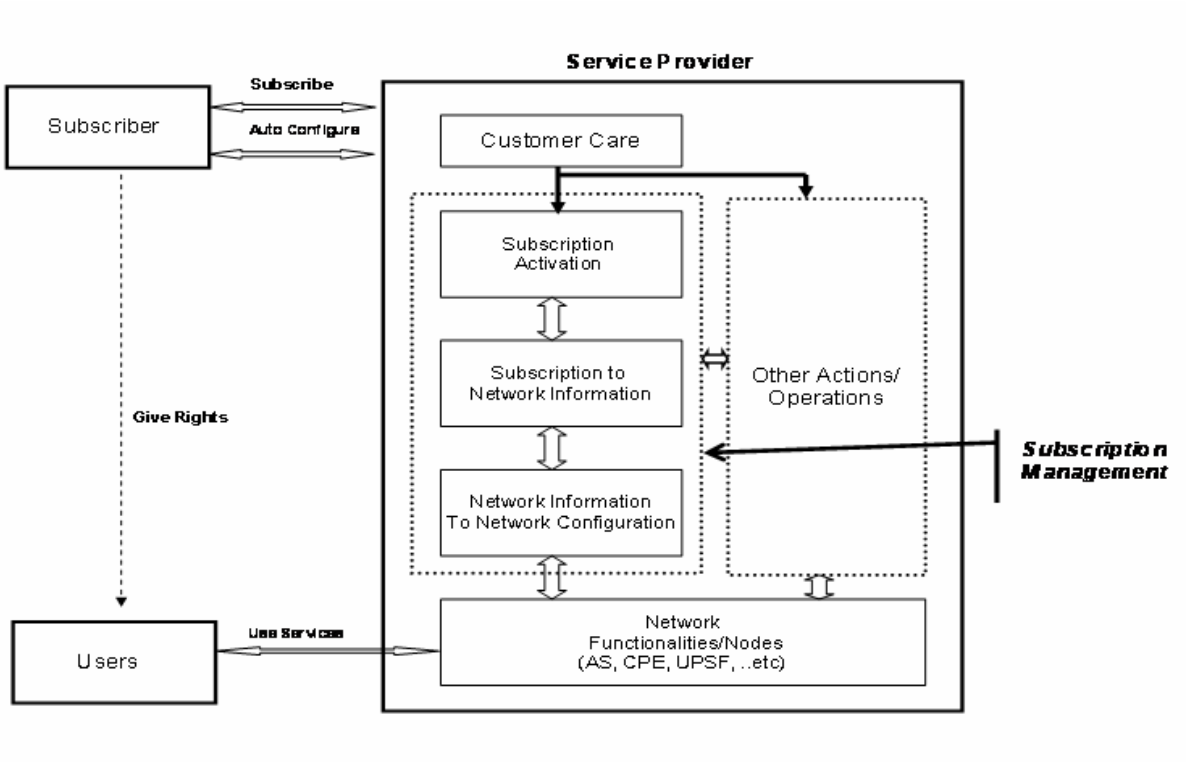


Figure 5.1.5.1.3.1: SuM Framework according to TISPAN [25]

The eTOM fulfilment process is composed of the following process:

- Selling, Marketing fulfilment response and order handling.
- Service Configuration and Activation.
- Resource Provisioning.
- S/P Requisition Management.

According to [25] Subscription Management must define the following:

- An end-to-end information model to cover all the mandatory/optional information related to subscription management that must be provisioned in the NGN Network.
- A subscription management functional architecture which hides the complexity of the different functional entities to be configured including the CPE and the AS.

For the end-to-end information model, the objectives are to describe the concepts (data, attributes and relations) necessary for the provisioning of services for a specific subscriber. The provisioned data can be either static or dynamic, but only static data will be covered within [80]. Static data are permanent or semi-permanent data. Typically static data are provisioned during the process of service and network resources configuration–and are non modifiable during a NGN session. Dynamic data are characterized by frequent changes. For example, the IP address allocated to an equipment in the access network is a dynamic data because it is allocated for a given lifetime.

Requirements on the information model

Within this 1st release of the document, SuM shall handle the following information parts:

- Information that need to be provisioned by Resource Provisioning Process on the NGN functional entities;
- Information exchanged between Service Configuration & Activation and Resource Provisioning process.

Requirement 1: The SuM information model shall be flexible in way that adding new information can be achieved easily and without modifications to the existing information and relationships.

Requirement 2: The SuM information model terminology shall be in line with all the IMS information model terminology, and SuM model relationships must be in line with IMS model relationships defined by 3GPP.

Requirement 3: The SuM Information Model shall be connected to an existing "model infrastructure".

- Examples of "model infrastructure" are:
  - the TMF Shared Information/Data Model (SID);
  - the TISPAN Management Information Model (MIM);
  - UML, etc.
- According to [25] the most promising candidate to connect the SuM Information model to is TISPAN WG8's Management Information Model (MIM).

Requirement 4: The SuM Information Model shall model the ability to grant different configuration rights for service usage to different users.

Requirement 5: All key concepts and entities must be referred by a use case.

Requirement 6: The 3GPP SuM NRM model (see above) should be re-used as much as possible.

Requirements on the functional architecture

Requirement 1: The purpose of the SuM Functional Architecture is the design of the NOSIs needed for management of a specific Subscriber, User, Service Profile and User Services.

Requirement 2: The SuM Functional Architecture shall deliver the necessary NOSIs for the Resource Provisioning and Service Activation processes.

Requirement 3: The SuM functional architecture shall hide the complexity of the different functional entities to be configured including the CPE and the AS.

Requirements on TISPAN NGN functional entities

The master NGN functional entities where subscription data are stored are the following:

- UPSF;
- AS;

- CLF;
- NACF;
- PDBF;
- CPE.

Requirement 1: The SuM Framework shall allow the creation, read, update, and deletion of subscription data within the above entities.

Security Requirements

General Requirement: The SuM solution shall comply with specific local, national, and regional security regulations.

Requirement 1: Subscription data shall be safeguarded against unapproved disclosure or usage.

Requirement 2: Access to SuM data shall only be permitted in an authorized and secure manner.

Requirement 3: Secure mechanisms shall be available for the transfer of SuM data to, from or between authorized entities. The secure mechanisms to be applied shall be appropriate to the level of confidentiality of the data, the endpoints of the transfer and the routes that are available for the transfer of the data.

Requirement 4: Audit records should be maintained for all SuM transactions to facilitate resolution of security violations.

SuM Information Model Requirements

According to [80] the SuM information model aims to define all the data, attributes and relations necessary for the provisioning of services for a specific subscriber. In order to design this information model, it is necessary to have a model that depicts all the actors and relationships between them. Figure 5.1.5.1.3 .2 shows TISPAN's SuM model.

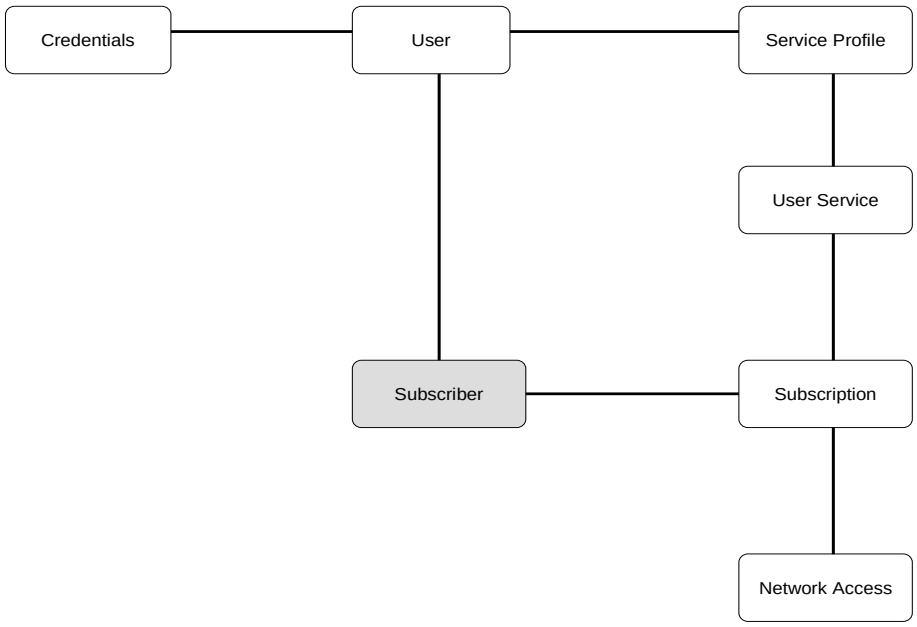


Figure 5.1.5.1.3.2: SuM Entity - Relationship Model according to TISPAN [25]

The new actors introduced within the SuM model are the following:

- Service Profile: The **Service Profile** represents the set of subscribed services associated to a user. many service profiles may be associated to a user. This concept permit to establish a link between a user and a set of services he/she is using.
- Access Network: One subscription may be used across different network accesses.

Within the SuM Model, one subscriber is linked to zero or several NGN subscription, where one NGN subscription is associated to one and only one subscriber.

A NGN subscription can be associated to zero or more physical access networks (e.g. DSL, GPRS, etc), and the same physical access network may be used by several NGN subscription.

Within one NGN subscription, a subscriber may give rights to zero or several users. One user is associated to at least one subscriber. One user is associated to at least one Subscription(s), and may be associated to several.

To access its services, users are requested to provide their associated credentials. One user can have one or more credentials , while one credential is associated to only one user.

A Service profile is a collection of service and user related data, and can be associated to one or more users. One user may be associated to multiple service profiles.

The architecture comprises the definition of all the necessary management components and interfaces between (see also figure 5.1.5.1.3.3):

- The CRM Order handling process and SM&O Service Configuration & Activation process.
- The SM&O Service Configuration & Activation process and RM&O Resource Provisioning process.
- The RM&O Resource Provisioning process and TISPAN NGN Network functional entities including CPE and AS.

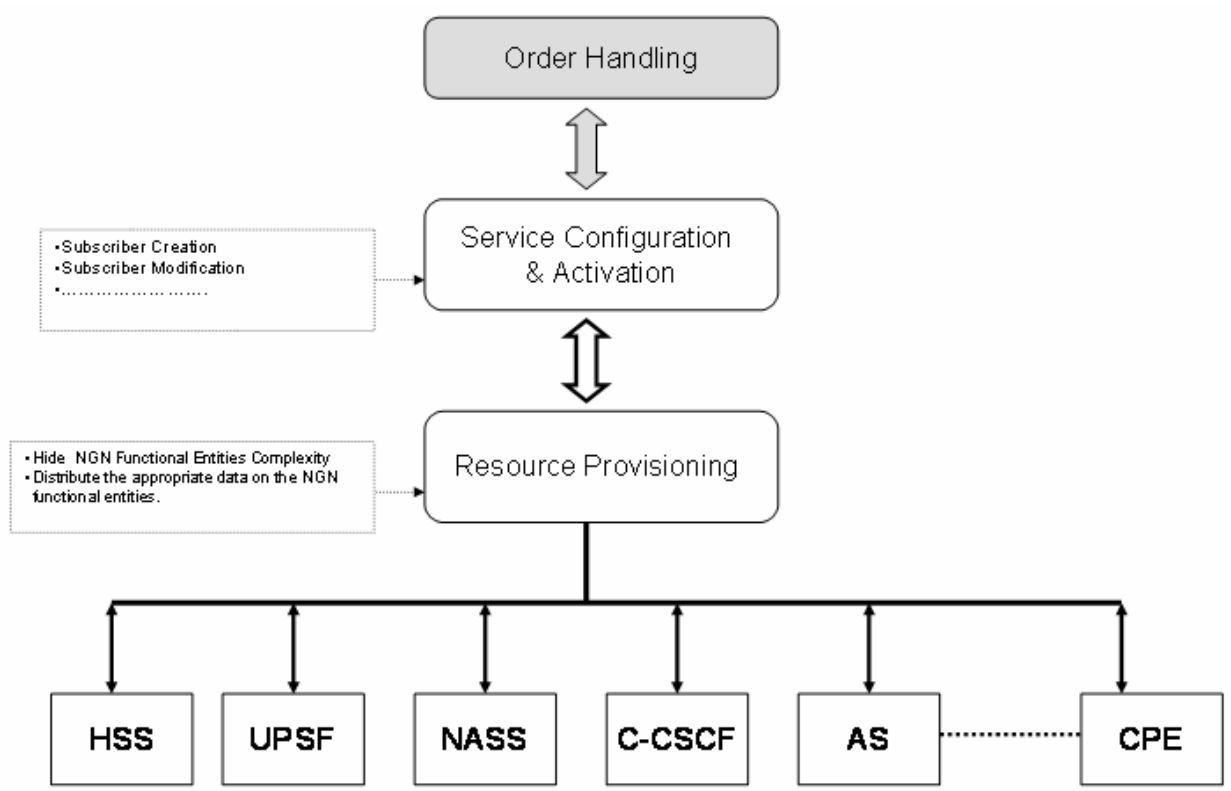


Figure 5.1.5.1.3.3: SuM Architectural Model according to TISPAN [25]

In [26] a first high level definition of an information model is given, which will be further refined in upcoming version of the document:

Subscriber

The subscriber concept used in the present document is the same as the one defined in [2]. It is not handled (stored or modified) in the TISPAN NGN network nodes. The subscriber is not in the scope of [26], and is mentioned for clearness and consistency purposes of the model.

User

- A user is described by its characteristics/attributes, possibly including various identifiers.
- A user must be immutable and, therefore, independent of any information that may change during the lifecycle of the user. In particular, it must not depend on any service, any device, network access, credential, etc.
- A user may be associated with zero or more devices, network accesses, credentials, contracts, etc.
- In addition, the change of/in devices, network accesses, credentials, contracts, etc. must not lead to a change of identities.
- A user is defined to be long lasting. Life cycle of a user identity is independent of several aspects:
  - A user is not strictly bound to a particular contract subscription.
  - A user is independent from any device.
  - A user is independent from any network access.

Credential

A credential is a physical or data element that is used by user to establish a claimed identity. Typical credentials include user names/passwords, SIM cards or smart cards, network access numbers, biometrics, etc.

Subscription

The subscription describes the commercial relationship between the subscriber and the service provider. It identifies a subscriber to one or more services.

The subscription is identified by a unique subscription identifier, which is assigned by the information system and has no semantics with regard to the service execution. It must be inserted in the call detail records generated by the S-CSCF and Application Server.

The subscription identifier remains unchanged all along the service subscription.

Network Access

The network access represents the physical entity that allows the user the attachment to the network: IP address allocation. It can be of different types: xDSL (where the typical access can be represented by a virtual circuit) or GPRS (where the typical access can be represented by a PDP context).

User Service Instance

A user service instance is a commercial service provided (offer) to a customer by a service provider. It is personalized if it is configured by the user. A service from the products and service catalogue is associated with one or more user services.

Service Profile

A Service Profile is possibly linked to a list of Services depending on the service subscription. This list may change in the following cases:

- The associated subscription account has requested new services or resigned services.
- The service operator has decided to add new services (e.g. for marketing reasons).
- The service operator has decided to restrict some services for any reason.

According to [26] these entities are correlated the following way.

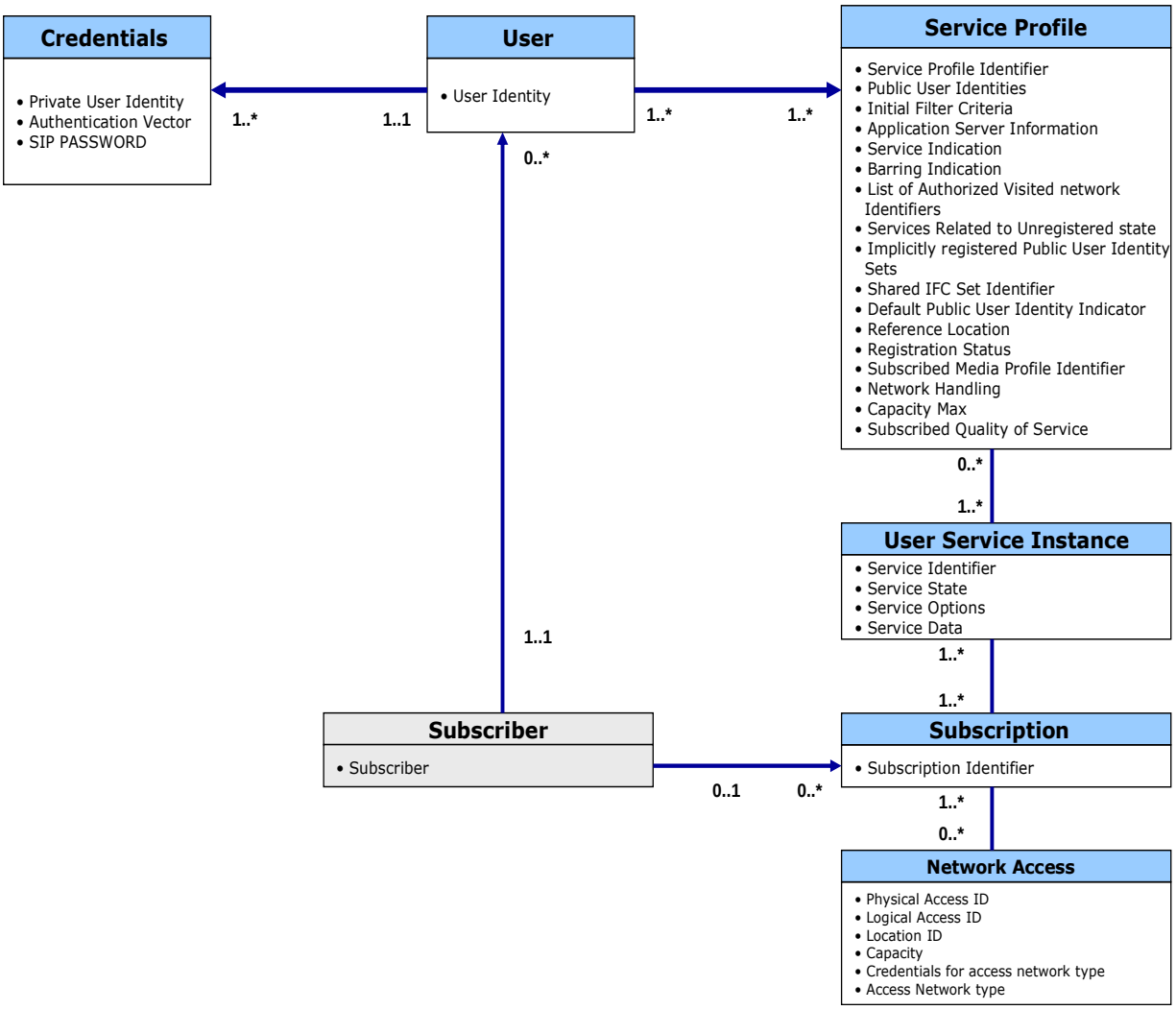


Figure 5.1.5.1.3.4: SuM Information Model according to TISPAN [26]

5.1.5.1.5 OMA

[32] identifies a set of capabilities within the IP Multimedia Subsystem (IMS) as defined by 3GPP and 3GPP2 that can be utilized by the OMA service enablers. Thus [32] also describes, which common interfaces exist between the IMS architecture and the OMA service enabling architecture, so that OMA does not have to define a duplicated set of capabilities for OMA service enablers, rather these service enablers make use of the existing IMS architecture.

According to [32] subscriber data are stored on the HSS.

The Sh interface of provides the OMA service enabler with read and write operations of user data related to IMS. It also provides the functionality for subscription and notification of changes in the user data related to IMS.

The work item General Service Subscription Management (GSSM):

The objective of this work item [84] is to specify a general service subscription management function in OSE, which is expected to cover management of all services subscriptions within an operator/service provider's domain.

According to [84] the GSSM work item will address at least the following features related to service subscription management:

- Dynamic manipulation (add, update, remove, pause, resume) of service subscription;
- Service subscription provisioning, i.e. doing all the steps needed in order to fulfil a service subscription request from a subscriber);
- Service subscription checking for requests by a subscriber for a service application (or the reverse direction);

- Definition of the service subscription models.

Two use cases shall be analysed specifically:

Use case 1: Generating service subscription by request

- The subscriber should be able to change/update his/her service subscription at any time and these changes/updates should be taken into account as soon as they are performed.
- The subscriber requests an update of his/her service subscription;
- The GSSM updates the service subscription for the subscriber and returns a response;
- Further actions could be taken to handle the service subscription update, e.g. notifying Applications or other entities, if needed; Note that the response shown in the diagram below may not be needed because often the GSSM will no know how to react on it.

Use case 2: Checking service subscription

Any other authorized enablers or entities should be able to check service subscription. Before processing a service request from a requestor (an application, a subscriber, or another enabler/entity), subscription related to this service could be checked. One of the most likely components to make use of this purpose is PEEM. This case corresponds to the PDP-PEP model defined by IETF, where PEEM/other enablers are the PEP, and GSSM is the PDP that delegates the service subscription evaluation.

- The requestor sends a service request to PEEM (or a target resource).
- The PEEM (or the target resource) asks the GSSM whether the service requests has a subscription.
- GSSM checks the service subscription and finds that the service subscription exists. The GSSM responds to PEEM (or the target resource) with positive answer.
- Processing of the service request can continue.

According to [84] the following external fora may be affected by this work item:

- TMF (TBD).
- ETSI TISPAN (as they are investigating Subscription Management (SuM)).
- 3GPP:
  - HSS may be the storage of subscription information for some IMS services in operator's networks; therefore the relationship of GSSM and HSS should be studied and clarified; other affections to 3GPP are TBD.
  - 3GPP SA5 (as they are working on Subscription Management (SuM)).

According to [85], which specifies the requirements for GSSM, OMA supports the following general service subscription concept:

Service subscription describes the commercial relationship between the subscriber and operator/service provider. Service subscription is essential for operators and service providers, since at least the following actions would pertain to service subscription information:

- Authorization for a subscription: by checking if a subscriber is permitted to subscribe to a service.
- Subscription validation: by checking if a subscriber is subscribed to a service, operator/service provider can control if the subscriber is allowed to access a service (subscriber-initiated service), or if the service application is allowed to push a content to a subscriber (application-initiated service).
- Charging: service subscription is one of the major references for charging.

Service subscription includes (among other pieces of information like service customization and other subscription parameters) the service availability for a subscriber (e.g. if the subscriber is subscribed to a WAP-based "mobile weather forecast" service).

[85] aims to specify an enabler which decouples access to service subscription from its actual representation and the location of the data by providing:

- A single point of access to service subscription functions across multiple instances of a service (e.g. multiple PoC servers).
- A unique interface to service subscription functions across multiple services (e.g. PoC, IM, etc.).

Up to now, the following use cases have been identified:

Service Subscription for Digital Newspaper Service

Short Description

A "digital newspaper service", provided to mobile network users in Beijing, delivers news information including text, pictures, and short video clips to subscribers of the service via MMS. James is an office staff working in Beijing, and he would like to view some news for killing time when he is on the way to his office by subway. He finds the digital newspaper service complies with his requirement, and tries to subscribe to the service.

Actors

- James, a mobile user of local mobile operator (acts as the subscriber of the service).
- BeijingMobileInfo.com, a Content Provider which owns the digital newspaper service applications (act as the 3rd party Content Provider of the service).
- Mobile operator offering GSSM and a service portal (acts as Service Provider).

Service Subscription Validation for Indie Music Bundle

Short Description

A Mobile Operator has recognized that independent record companies do not possess the subscription and charging infrastructure to offer music downloads to their fans as a competitive rate. To satisfy this need, the Mobile Operator has created an Indie Music Bundle service which allows fans of non-mainstream music to download content from 50 independent record companies for a single monthly fee based on a maximum number of track downloads per month.

Todd is a big fan of progressive thrash metal music and is frustrated by the lack of this genre on the major music download sites. He wants better value for his download dollar than the price per track rate and more variety than that provided by a single record company. He decides the Indie Music Bundle meets his needs and subscribes to the service level offering 10 tracks per month for $4.99.

Actors

- Todd, a mobile user and customer of the Mobile Operator (acts as the subscriber of the service).
- Blue Dog Records: A content provider which owns the rights to the music tracks.
- Mobile Operators offering a subscriber self-care service portal and GSSM (acts as Service Provider).

Service Subscription for Groups

Short Description

A "digital newspaper service", provided to mobile network users in Beijing, delivers news information including text, pictures, and short video clips to subscribers of the service via MMS. Alice and Bob are the office staffs working for the same corporation in Beijing. John is the manager of the corporation and he would like to provide his staffs the welfare of viewing some news for killing time when they are on the way to their office by subway. John registered a Group to include Alice and Bob. He subscribed the digital newspaper service for his group and every morning a multimedia message containing up-to-time news is sent to the devices of users in John's group, namely to Alice and Bob. When they are on the subway they can open the messages and view the news.

Actors

- John, acts as the principal who initiates the subscription of the service.
- Alice and Bob, act as the group user of the service.
- BeijingMobileInfo.com, a Content Provider which owns the digital newspaper service applications.
- Mobile operator acts as Service Provider.

Service Validation for a Group

Short Description

A "digital newspaper service", provided to mobile network users in Beijing, delivers news information including text, pictures, and short video clips to subscribers of the service via MMS. Alice and Bob are the office staffs working for the same corporation in Beijing. John is the manager of the corporation and he would like to provide his staffs the welfare of viewing some news for killing time when they are on the way to their office by subway. John registered a Group to include Alice and Bob. He subscribed the digital newspaper service for his group and every morning a multimedia message containing up-to-time news is sent to the devices of users in John's group, namely to Alice and Bob. When they are on the subway they can open the messages and view the news.

Actors

- Alice and Bob, act as the group user of the service.
- BeijingMobileInfo.com, a Content Provider which owns the digital newspaper service applications.
- Mobile operator acts as Service Provider.

Charging Use Case

Short Description

This charging use case elaborates further what requirements exist when it comes to charging.

Actors

- Todd, a mobile user and customer of the Mobile Operator (acts as Subscriber of the service).
- Blue Dog Records: A content provider which owns the rights to the music tracks.
- Mobile Operator offering a subscriber self-care service portal and GSSM (acts as Service Provider).

5.1.5.1.6 TMF

The NGOSS as described in [98] focuses on the specification of contracts. These represent a central concept, as they provide interfaces to NGOSS components. A component is a container of one of the two following types of contract:

- Contracts, which represent the value-added service of the component.
- Contract used to manage the service itself.

A component must support at least one contract; in the case of a customer care end-to-end application it will most probably support a larger amount of contracts.

For a more detailed introduction to TMF's concepts see clause 5.1.5.5.3. This clause deals with the definition of the notion "contract" within NGOSS [x41, x42].

Basically TMF uses UML as definition method for their NGOSS meta-model, with the addition of:

- New model elements:
  - Contract:

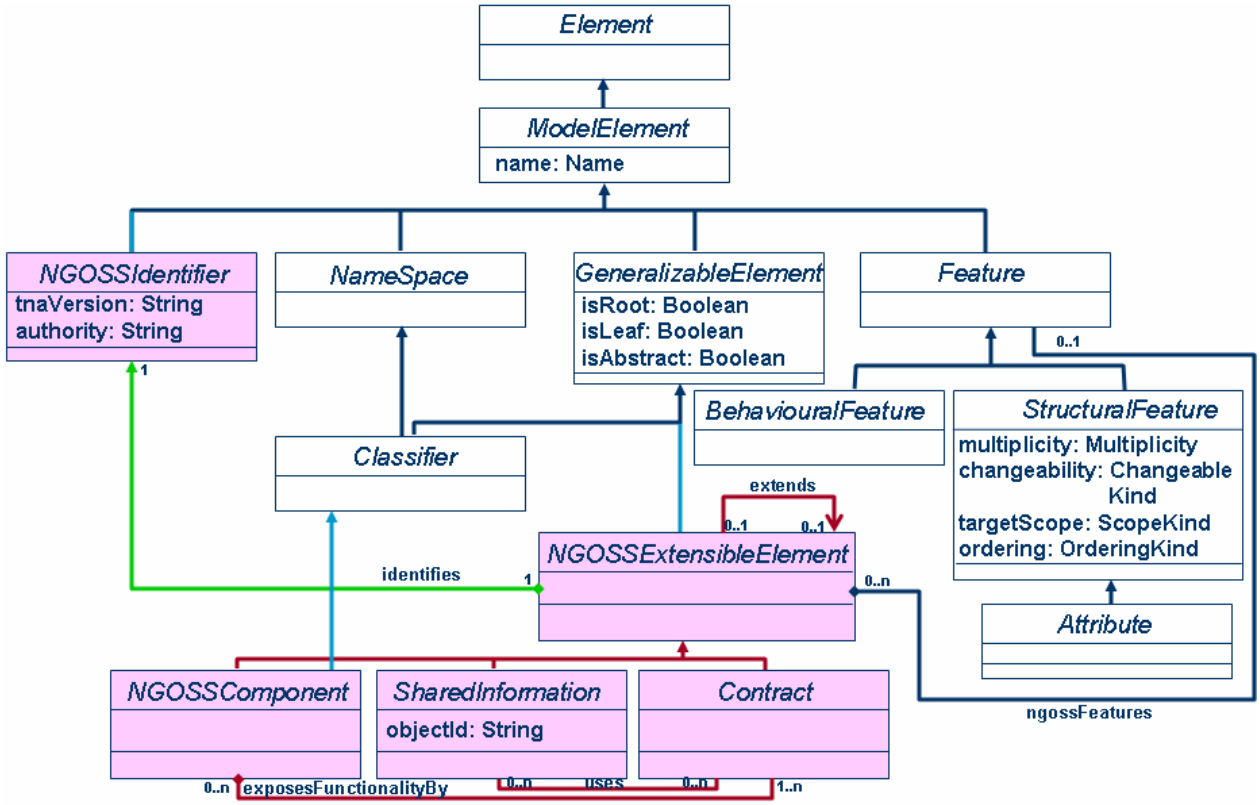


Figure 5.1.5.1.6.1: NGOSS Contract Model [95]

In TMF, the contract is the fundamental unit of interoperability for an NGOSS system.

- Defines the specification of a service to be delivered.
- Specifies information and code for the service of the bullet above.
- Used to monitor, maintain and administer the respective service.
- Has to ensure that external obligations (e.g. from SLAs) are honoured and define reactions in case of violations.
- Defines how a service is to be used (e.g. invoked):
  - Defines pre- and post conditions.
  - Semantics for using the service.
  - Policies affecting the configuration.
  - Use and operation of the service.

The functionality specified by a contract is seen differently by the different constituencies:

- Business view: specifies the high-level goals and obligations that a resource and/or service must fulfil.
- System View: specifies the architectural requirements necessary to design the contract as defined by the business view.
- Implementation view: defines configuration, programming and other factors of the components, which provide the functionality defined by the contract.
- Deployment View: provides means for:
  - Monitoring the costs.
  - Monitoring the performance.

- Monitoring all other aspects delivered by a component.
- Administering the contract to enable the contract's activation and deactivation.

- NGOSS Component: represents a standard way to package NGOSS functionality. It needs to:
  - know about; and
  - be able to use NGOSS contracts.
- NGOSS Shared Information: designed to be inherently shareable and reusable between NGOSS components. It needs to:
  - know about; and
  - be able to use NGOSS contracts.
- NGOSS Identifier: represents a standard way to uniquely identify an NGOSS element.

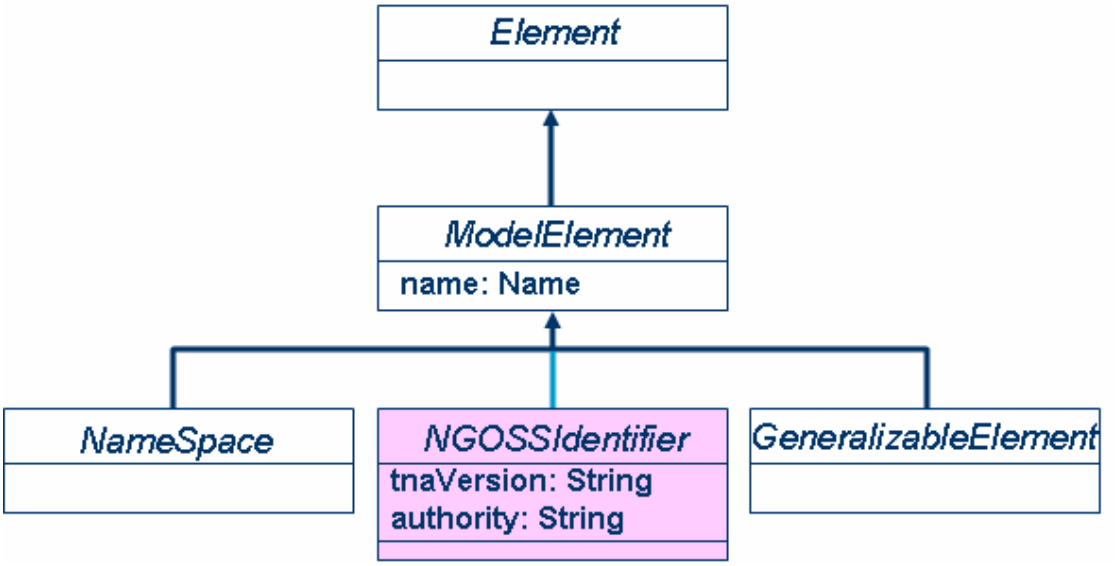


Figure 5.1.5.1.6.2: NGOSS Identifier [95]

The figure only shows the two most important attributes of NGOSS Identifier;

- tnaVersion: contains the specific version number of the NGOSS identifier.
- authority: name of the authority, which defined the entity that this class identifies.

- NGOSS Policy: represents a standardized way to control NGOSS components and processes.
- NGOSS Interaction: represents the interaction of different managed elements and thus determines the behaviour of NGOSS systems.
- Termination: used in the definition of NGOSS Contract operations.
- NGOSS Extensible Element.

- New information entities.
- New data types.

According to [96] the basic NGOSS contract description is composed of five parts:

- General Contract Part:
  - Header Part: identifies the contract in an unambiguous way:
    - Contract Name.
    - Contract Identifier.
    - Version.
    - Contract Defining Organization.
  - Descriptive Part: contains the goal of the contract and some search criteria:
    - Goal.
    - Description.
    - Comment.
    - Search Criteria.
- Business View of the contract structure:
  - Functional Part: defines the capabilities provided by the contract:
    - Associated Business Process.
    - Associated Business Policies.
    - Business Capabilities.
    - Preconditions.
    - Result Status.
    - Post-Conditions resulting from correct operation.
    - Interaction Points.
    - Interaction Roles.
    - Security.
    - Context for the capabilities.
  - Non Functional Part: defines aspects, which pose boundary conditions for the operation of the capabilities defined in the contract:
    - Deployment related fields:
      - Availability limitations.
      - Safety limitations.
    - Organization related fields
      - Business environment.
      - Organizational limitations.
      - Market limitations.
      - Financial limitations.

- Legal related fields
  - Regulatory limitations.
  - Legal limitations.
- Miscellaneous fields
  - Stakeholders.
  - Assumptions.
  - Offering periods.

- Management Part: defines the management capabilities necessary to administer and maintain the capabilities of the contract:
  - Management Activities.
  - Reponsible Management Roles.
  - Associated Management processes.
  - Associated Management policies.
  - Management Security Policies.
- View Specific Model Part: contains the model types (UML and others) necessary to support the specific view of the contract requested.

- System View of the contract structure:
  - Functional Part: defines the capabilities provided by the contract:
    - Associated System Processes.
    - Associated System Policies.
    - System Capabilities:
      - Input Entities.
      - Output Entities.
      - Pre-Conditions.
      - Termination.
      - Post-Conditions.
      - Post-Condition System Exceptions.
      - Vendor Extensions.
    - State machine ID.
    - Pre-Conditions.
    - Termination.
    - Post Conditions.
    - Interaction Type.
    - Security.
    - Context.

- Non Functional Part: defines aspects, which pose boundary conditions for the operation of the capabilities defined in the contract:
  - Operational Cost.
  - Resource Cost.
  - Service Cost.
  - QoS Mapping.
  - Geographic Constraints.
  - Resource Constraints.
  - Operational Constraints.
- Management Part: defines the management capabilities necessary to administer and maintain the capabilities of the contract:
  - Management capabilities
  - Creation Policy ID
  - Configuration Policy ID
  - Modification Policy ID
  - Installation Policy ID
  - Deployment Policy ID
  - Monitor Policy ID
  - Removal Policy ID
- View Specific Model Part: contains the model types (UML and others) necessary to support the specific view of the contract requested.

Fundamental to NGOSS based systems [98] is also the concept of a Shared Information Datamodel (SID) [99]. There, amongst other data, Service Level Agreements and Customer Details are defined.

The detailed model of a customer can be found in [100]:

- Customer: Person or organization, which obtains products and services from the enterprise or receives free offers for services. This business entity has the following attributes:
  - customerId: unique identifier (mandatory);
  - customerStatus: current condition of a customer - active, inactive, prospective (mandatory);
  - customerRank: degree of importance relative to other customers (optional).
- CustomerCreditProfile: Outline of a customer's credit worthiness:
  - creditProfileId: Identifier of the credit profile;
  - creditProfileDate: Date of establishment;
  - validFor: The period for which the profile is valid.
- CustomerCreditProfile:Reference: Source of reference to help determine the customer's credit worthiness:
  - financialInstitutionName: Name of financial institution, which holds the referenced account;
  - financialInstitutionAccountNumber: financial institution account number, which identifies the customer account;

- financialInstitutionAccountType: type of financial institution account;
- financialInstitutionContactName: the name of an individual at the financial institution, who can verify the account;
- financialInstitutionContactMedium: method, by which the contact can be reached.

- CustomerAccount: arrangement that the customer has with an enterprise that provides products to the customer:
  - ID: unique identifier;
  - name: name of an account;
  - accountType: categorization of an account (individual, joint, etc.);
  - accountStatus. : condition of the account (due, paid, etc.).
- CustomerAccountBillCycle: point in time, when a bill is produced for a customer account:
  - billCycle: the billibg cycle during which a bill fort he account is produced;
  - validFor: time period fro which the billing cycle is applicable.
- CustomerAccountContact: an individual or organization used as contact point for a customer account and accessed via some contact medium:
  - contactType: identifies the relationship of the contact to the account;
  - validFor: time period for which the account is valid.
- CustomerAccountRelationship: a significant relation between two customer accounts:
  - relationshipType: defines the type of relationship between two customer accounts;
  - validFor: time period for which the relationship is valid.
- CustomerAccountTaxExemption: proof of freedom from taxes between two customer accounts:
  - issuingJurisdiction: name of the taxing juridiction for which taxes are exempt;
  - certificateNumber: identifier of the document, which shows proof of exemption from taxesfor the taxing jurisdiction;
  - validFor: time period for which the exemption is valid.

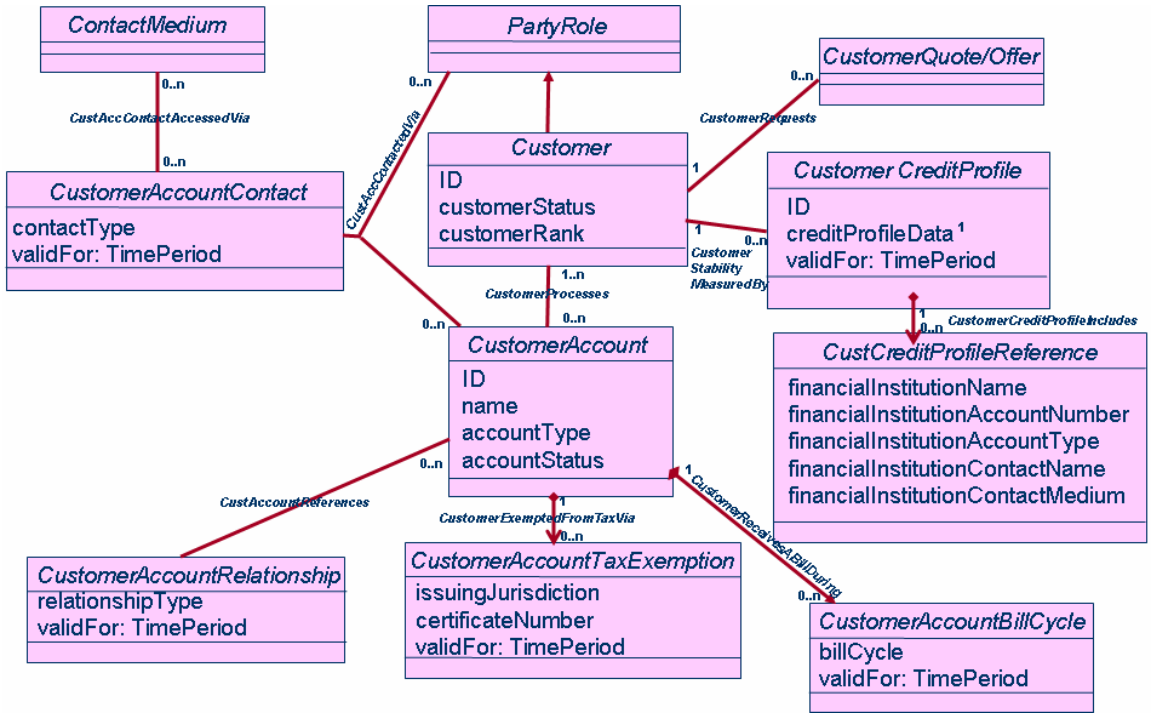


Figure 5.1.5.1.6.3: TMF SID Customer [100]

Associated with the customer is the customer's order. [100] defines the following business entities:

- CustomerOrder: communication used to procure a product. There are different types of customer orders (AccessServiceRequests, LocalServiceRequests, DirectoryServiceRequests, ProductOrders):
  - assignedPriority: the order's assigned priorityafter review;
  - assignedResponsibilityRank: target response date after review.

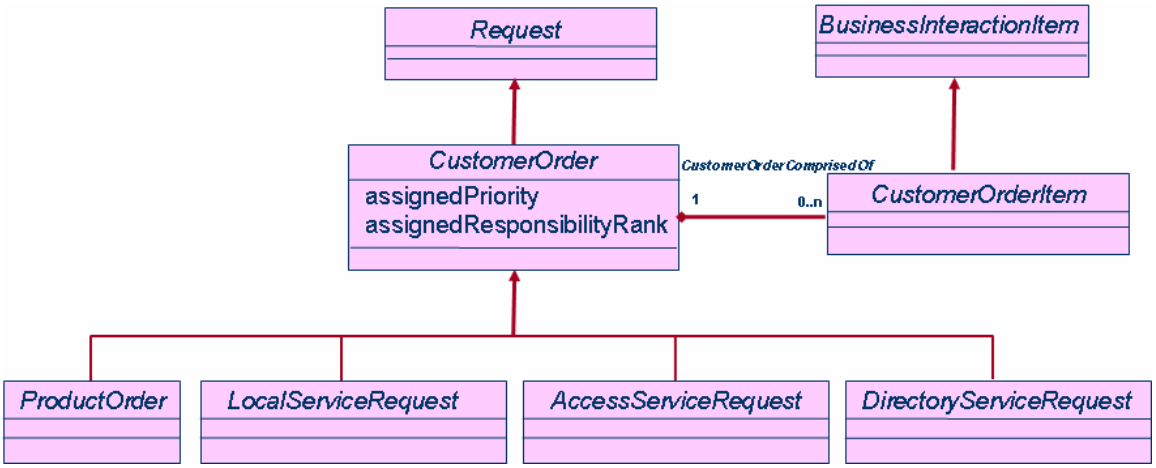


Figure 5.1.5.1.6.4: TMF SID CustomerOrder [100]

5.1.5.2 Statistics

5.1.5.2.1 ITU-T

In [94] ITU-T describes its management philosophy and lists the tasks for each of the management layers it defines. ITU-T does so by identifying functions and function sets.

The following function sets from the Performance Management (PM) area deal with the end-user, who is called customer and subscriber interchangeably in [94].

- Performance Quality Assurance: supports decision processes that establish, as the state-of-the-art expands and customer needs change, the quality measures that are appropriate to the area of (PM).

  - Subscriber service quality criteria function set: This set provides a network management query feature for offering Performance Management information to a customer, such as grades of service options, performance monitoring thresholds, or the possible conditions under which rebates are awarded when service quality goals are not met.

  - QoS performance assessment function set: This set provides access to the assessment summary of all combined QoS performance measures, by area, by type of customer, by type of service and by network components, that compares measured quality with the quality goals.

- Performance Monitoring: Performance Monitoring involves the continuous collection of data concerning the performance of specific network elements.

  Performance monitoring is designed to measure the overall quality, using monitored parameters in order to detect such degradation. It may also be designed to detect characteristic patterns of impairment before signal quality has dropped below an acceptable level.

  - Performance monitoring policy function set: This set establishes Performance Monitoring policy such as the values of threshold settings and schedules for data collection for specific kinds of circuits. These settings are to be applied during activation of such circuits. Different policies are likely to be created for special service circuits of various kinds, for message circuits, and for facilities.

    - Set PM trend analysis pattern: Manager directs the agent to assign designated values to a PM trend analysis pattern. A PM trend analysis pattern is a set of parameters of an algorithm that analyses raw PM data from a monitoring point and characterizes the data as (for example) increasing in severity over time or cyclic or associated with service customer activity.

- Performance Analysis: Performance data may require additional processing and analysis in order to evaluate the performance level of the entity.

  - Customer service performance summary function set: This set supports the generation of reports on summaries of measurements for the purpose of evaluating the performance of a particular transport service or group of services. The customer can be provided access to the summary in order to verify that guaranteed service levels have been met, or to enable the customer to evaluate their own networks.

  - Customer traffic performance summary function set: This set provides access to a scheduled or exception report of offered traffic, usage and measures of congestion on a leased circuit, a group of leased circuits, a hunt group, or a leased physical or virtual network.

5.1.5.2.2 3GPP

Following [60] any evaluation of 3G-system behaviour requires performance data collected and recorded by its NEs according to a schedule established by the EM. This aspect of the management environment is termed Performance Management.

The purpose of any Performance Management activity is to collect data, which can be used to verify the physical and logical configuration of the network and to locate potential problems as early as possible. The type of data to be collected is defined by the equivalent measurements. This clause describes the requirements of 3G-telecom management to produce this data.

Data is required to be produced by the NEs to support the following areas of performance evaluation:

- Traffic levels within the network, including the level of both:

  - the user traffic; and

  - the signalling traffic;

The following traffic types are evaluated:

- traffic load on the radio interface (signalling and user traffic);
- usage of resources within the network nodes;
- user activation and use of supplementary services, etc.

- Verification of the network configuration: Once a network plan, or changes to a network plan, have been implemented it is important to be able to evaluate the effectiveness of the plan or planned changes. Typically, the measurements required to support this activity indicate the traffic levels with particular relevance to the way the traffic uses the network.

- Resource access measurements: For accurate evaluation of resource access, each measurement result would need to be produced for regular time intervals across the network, or for a comparable part of the network.

- Quality of Service: The user of a 3G system views the provided service from outside the network. That perception can be described in observed QoS terms. QoS can indicate the network performance expected to be experienced by the user. For further detail see ITU-T Recommendation E.880. Examples are delays during call set-up, packet throughput, etc.

- resource availability: The availability performance is dependent on the defined objectives, i.e. the availability performance activities carried out during the different phases of the life cycle of the system, and on the physical and administrative conditions. For further detail see ITU-T Recommendation E.880. Examples are the recording of begin and end times of service unavailability).

The production of the measurement data by the NEs also needs to be administered by the EM. Several phases of administration of performance measurements can be distinguished:

- management of the performance measurement collection process: The administration of measurement jobs by the EM comprises the following actions:
  - Create/delete a measurement job.
  - Modifying a measurement job, i.e. changing the parameters (specifically the schedule) of a measurement job that has been previously created.
  - Definition of measurement job scheduling.
  - Suspend/resume a measurement job.
  - Setting up the requirements for the reporting and routing of results to one or more OSs (EM and/or NM). For the NM, this is limited to the control of the result file transfer.

  Retrieval of information related to measurement jobs, i.e. view the current measurement job definition.

- generation of performance measurement results: The measurement data can be collected in each NE of the network in a number of ways:
  - cumulative incremental counters triggered by the occurrence of the measured event;
  - status inspection (i.e. a mechanism for high frequency sampling of internal counters at pre-defined rates);
  - gauges (i.e. high tide mark, low tide mark);
  - discrete event registration, where data related to a particular event is captured.

- local storage of measurement results in the NE: It shall be possible for the NE to retain measurement data it has produced for deferred retrieval by the OS(s). This data will be retained at the NE under the control of the EM. The storage capacity and the duration for which the data will be retained at the NE will be Operator and implementation dependent.

- transfer of measurement results from the NE to an OS: The results of the measurement job can be forwarded to the EM in either of two standard ways:
  - the scheduled result reports generated by the NE (notifications) can be sent to the EM as soon as they are available;
  - the reports can be stored in the NE (files) and transferred to or retrieved by the EM when required.

    It shall be possible for the EM to specify the details for its result retrieval as a part of the measurement administration.
- storage, preparation and presentation of results to the operating personnel.

5.1.5.3 Charging Management

The main requirements and high-level principles for charging have been listed in clause 5.1.2.6.3 based on 3GPP TS 22.115 [48].

Several logical charging functions are needed in the network together with the reference points that are used to transfer charging information between those functions.

It has already been stated in clause 5 that the domains (e.g. PS), services (e.g. MMS) and subsystems (e.g. the IMS) affect the way in which the charging functions are embedded. However, as the functional requirements for charging are always the same, 3GPP defines a common approach for the definition of the logical charging functions, resulting in a logical charging architecture for all GSM and UMTS network domains, subsystems and services that are relevant for charging standardization (see figure 5.1.5.3.1).

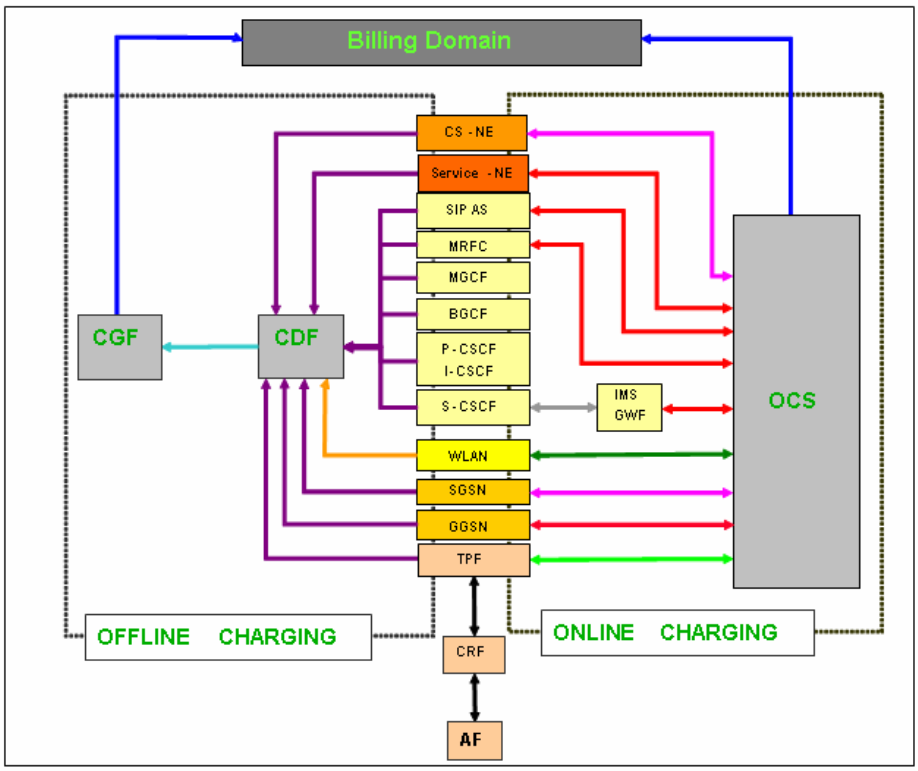


Figure 5.1.5.3.1: 3GPP Charging Management Architecture [47]

The logical functions and the reference points indicated in figure 5.1.5.3.1 will be treated separately for online and offline charging in the next clauses.

5.1.5.3.1 Offline Charging

5.1.5.3.1.1 3GPP

According to [47] charging information for network resource usage is collected concurrently with that resource usage. The charging information is then passed through a chain of logical charging functions (see below). Then CDR files are generated by the network and transferred to the network operator's Billing Domain for the purpose of subscriber billing and/or inter-operator accounting. The BD can comprise post-processing systems such as the operator's billing system or billing mediation device.

NOTE: Offline charging is a mechanism which does not affect, in real-time, the service rendered.

The following figure 5.1.5.3.1.1.1 [47] depicts:

- the logical charging functions as well as;
- the reference points between these functions and to the Billing Domain.

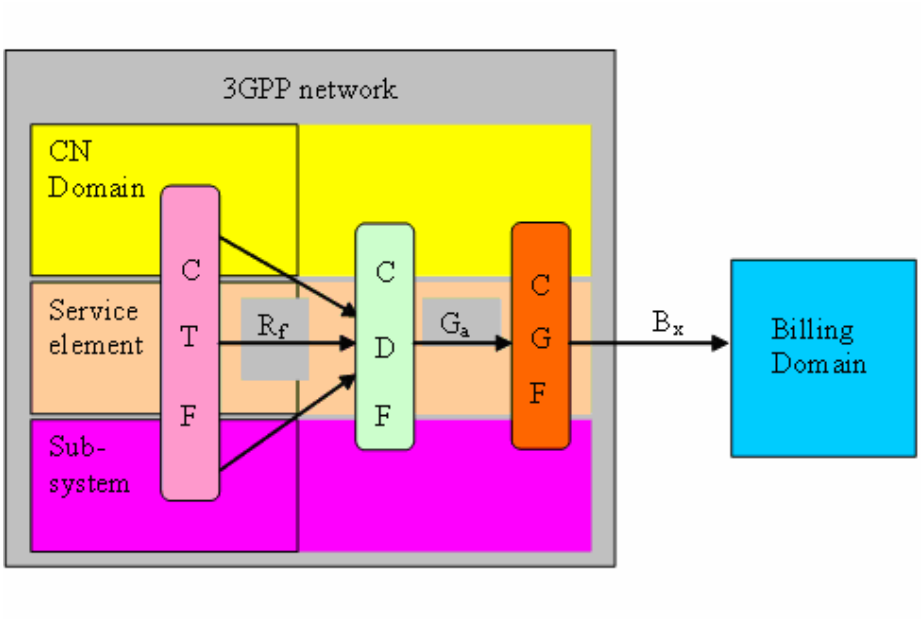


Figure 5.1.5.3.1.1.1: 3GPP Offline Charging functions and reference points [47]

- Charging Trigger Function (CTF): generates charging events based on the observation of network resource usage. The CTF is the focal point for collecting the information pertaining to chargeable events within the network element, assembling this information into matching charging events, and sending these charging events towards the Charging Data Function. The CTF is therefore a mandatory, integrated component in all network elements that provide offline charging functionality, as depicted in the figure above. It is made up of two functional blocks:
  - Accounting Metrics Collection: It is required to provide metrics that identify the user and the user's consumption of network resources and/or services in real-time. The exact behaviour and functionality of this process e.g.:
    - trigger conditions for collection of charging information;
    - information elements to collect;
    - which service events, signalling or user traffic to monitor;
    - relationship to services / bearers / sessions;
    - depends on functions / services that the NE provides.

- Accounting Data Forwarding: This process:

  - receives the collected accounting metrics;
  - determines the occurrence of chargeable events from a set of one or more of these metrics;
  - assembles charging events that match the detected chargeable events; and
  - forwards the charging events towards the Charging Data Function via the Rf reference point.

  The charging events provide information pertinent to the chargeable event, i.e. characterizing the network resource usage together with an identification of the involved user(s).

- Charging Data Function (CDF): receives charging events from the Charging Trigger Function via the Rf reference point. It then uses the information contained in the charging events to construct CDRs.

  The results of the CDF tasks are charging data records (CDRs) with a well-defined content and format. The content and format of these CDRs are specified per domain / subsystem / service in the related middle tier charging specification (e.g. 3GPP TS 32.250 for the CS domain and 3GPP TS 32.251 [111] for the PS domain, etc.).

- Charging Gateway Function (CGF): receives the CDRs produced by the CDF immediately via the Ga reference point. The CGF acts as a gateway between the 3GPP network and the Billing Domain. It uses the Bx reference point for the transfer of CDR files to the BD. The entity relationship between the CDF and the CGF is m:1, i.e. one or more CDFs may feed CDRs into a single CGF.

5.1.5.3.2 Online Charging

5.1.5.3.2.1 3GPP

According to [47] charging information for network resource usage is collected concurrently with that resource usage in the same fashion as in offline charging. In contrast to offline charging however, authorization for the network resource usage must be obtained by the network prior to the actual resource usage to occur. This authorization is granted by the Online Charging System upon request from the network.

When receiving a network resource usage request, the network assembles the relevant charging information and generates a charging event towards the OCS in real-time. The OCS then returns an appropriate resource usage authorization. The resource usage authorization may be limited in its scope (e.g. volume of data or duration), therefore the authorization may have to be renewed from time to time as long as the user's network resource usage persists.

NOTE: Online charging is a mechanism where charging information can affect, in real-time, the service rendered and therefore a direct interaction of the charging mechanism with the control of network resource usage is required.

The following figure 5.1.5.3.1.1.2 [47] depicts:

- the logical charging functions as well as;
- the reference points between these functions and to the Billing Domain.

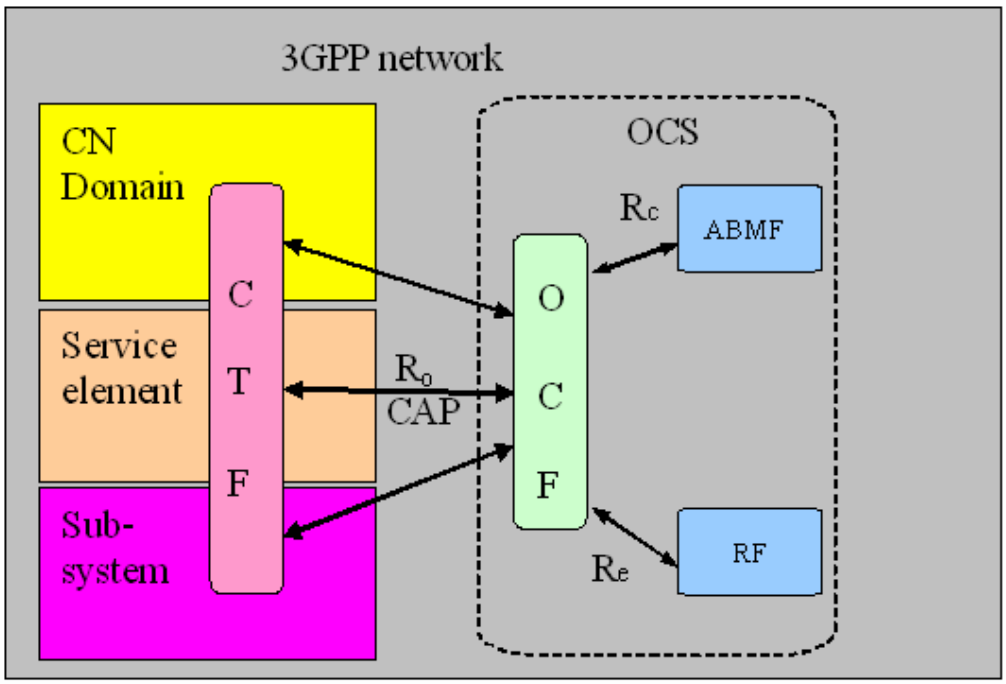


Figure 5.1.5.3.1.1.2: 3GPP Online Charging functions and reference points [47]

- CTF: Online charging is a process where charging information is collected in the network element in the same fashion as in offline charging. This implies that, from the functional perspective, the CTF defined in the clause above also creates the charging events used for online charging. While the accounting metrics used in online charging are generally the same as in offline charging (i.e. the charging mechanism is transparent to the Accounting Metrics Collection), there are some important functional enhancements concerning the Accounting Data Forwarding are required in the CTF in order to support online charging (see [47] for details).

- Online Charging System (OCS):

  - The Online Charging Function (OCF): consists of two distinct modules:

    - Session Based Charging Function (SBCF): responsible for online charging of network / user sessions, e.g. voice calls, GPRS PDP contexts or IMS sessions.

    - Event Based Charging Function (EBCF): performs event-based online charging (also referred to as "content charging") in conjunction with any application server or service NE, including SIP application servers.

  - S-CSCF online charging / IMS Gateway Function: the S-CSCF does not trigger any online charging events and thus does not include the CTF online charging enhancements already mentioned. Instead, the ISC interface is employed by the S-CSCF online charging, implying that online charging is transparent to the S-CSCF and appears like any other service controlled by a SIP application server. Therefore, if support for Ro based online charging is required, a special CTF is needed in order to mediate between the Ro based SBCF and the SIP based service control. This role is taken by the IMS Gateway Function (IMS GWF), which translates between SIP service control towards the S-CSCF and Ro credit control on the OCS side.

- Rating Function (RF): determines the value of the network resource usage (described in the charging event received by the OCF from the network) on behalf of the OCF. To this end, the OCF furnishes the necessary information, obtained from the charging event, to the RF and receives in return the rating output (monetary or non-monetary units), via the Re reference point. The RF may handle a wide variety of rateable instances, such as:

  - Rating of data volume (e.g. based on charging initiated by an access network entity, i.e. on the bearer level).

  - Rating of session / connection time (e.g. based on charging initiated by a SIP application, i.e. on the subsystem level).

- Rating of service events (e.g. based on charging of web content or MMS, i.e. on the service level).

- Account Balance Management Function (ABMF): location of the subscriber's account balance within the OCS.

5.1.5.4 Billing

5.1.5.4.2.1 3GPP

In offline charging (see [47]) the internal functions of the BD are outside the scope of 3GPP standardization. The reference point for the charging information transfer from the network to the BD forms part of the 3GPP standards.

In online charging (see [47]), the charging information is transferred from the network to the Online Charging System (OCS). The OCS, in turn, may have an offline charging reference point used to forward charging information to the BD. This BD is similar in scope and intent to the offline charging case.

5.1.5.5 System Management

5.1.5.5.1 ITU-T

In [94] ITU-T describes its management philosophy and lists the tasks for each of the management layers it defines. ITU-T does so by identifying functions and function sets.

The following function sets from the fault management (FM) area deal with the end-user, who is called customer and subscriber interchangeably in [94].

According to [94] Fault Management enables the detection, isolation and correction of abnormal operation of the telecommunication network and its environment. It provides facilities for the performance of the maintenance phases from ITU-T Recommendation M.20 [112]. The quality assurance measurements for Fault Management include component measurements for Reliability, Availability and Survivability (RAS).

- RAS Quality Assurance: RAS Quality Assurance establishes the reliability criteria, which guide the design policy for redundant equipment (a responsibility of Configuration Management), and the policies of the other function groups in this area:

  - Service outage reporting function set: This set provides access to a database of outage reports concerning an outage of services to multiple customers. The report may include the type of services affected, the number of customers affected, and the start and end times of the outage. Such reports include statistics concerning service outages by designated areas and over designated periods of time.

- Fault Localization: Where the initial failure information is insufficient for fault localization, it has to be augmented with information obtained by additional failure localization routines.

  - Network fault localization function set: The process to determine faults starts with the information received by status management from the network (e.g. alarm report, user message from customer, real-time status report by N/W carriers, etc). Based on the fault information received, the trouble ticket is opened by ticket management and consolidated with the related trouble ticket.

    Event management will analyse the fault report, and there are four opportunities for reaching the next status: diagnosed, help required, suspended or went away.

    After successful diagnosis, the problem will be "repaired", and the trouble ticket may be closed. Otherwise, the problem may be reselected. Problems, which disappear or are suspended, or when their time expires, may be changed to an "expired" status. After the problem is determined, the problem message is sent to the customer, for instance, outage equipment.

- Fault Correction: Fault Correction transfers data concerning the repair of a fault and for the control of procedures that use redundant resources to replace equipment or facilities that have failed.

  - Arrangement of repair with customer function set: This set supports contacting a customer to schedule dispatch to customer premises.

5.1.5.5.2 3GPP

[113] describes the requirements and information model necessary for the Telecommunication Management (TM) of 3G systems. It treats a 3G system as a multitude of Network Elements (NE) of various types and, typically, different vendors, which inter-operate in a co-ordinated manner in order to satisfy the network users' communication requirements. [113] consists of two parts, an NE management part and a system management part.

NE Management Part

The occurrence of failures in an NE may cause a deterioration of this NE's function and/or service quality and in order to minimize the effects of such failures on the Quality of Service (QOS) as perceived by the network users it is necessary to:

- detect failures in the network as soon as they occur and alert the operating personnel as fast as possible;
- isolate the failures (autonomously or through operator intervention), i.e. switch off faulty units and, if applicable, limit the effect of the failure as much as possible by reconfiguration of the faulty NE/adjacent NEs;
- if necessary, determine the cause of the failure using diagnosis and test routines; and,
- repair/eliminate failures in due time through the application of maintenance procedures.

According to [113] this aspect of the management environment is termed "Fault Management" (FM). Its purpose is to detect failures as soon as they occur and to limit their effects on the network Quality of Service (QOS) as far as possible.

Fault Management (FM) encompasses all of the above functionalities except commissioning/decommissioning of NEs and potential operator triggered reconfiguration (these are a matter of Configuration Management).

FM also includes associated features in the Operations System (OS), such as the administration of a pending alarms list, the presentation of operational state information of physical and logical devices/resources/functions, and the provision and analysis of the alarm and state history of the network.

Network Management Part

An operations system on the network management layer (i.e. the NM) provides fault management services and functions required by the 3G operator on top of the element management layer.

The N interface (Itf-N) may connect the Network Management (NM) system either

- to Element Mangers (EMs) or
- directly to the Network Elements (NEs)

by means of Integration Reference Points (IRPs).

In [113] the term "subordinate entities" defines either EMs or NEs, which are in charge of supporting the N interface.

The following paragraphs describe the properties of an interface enabling a NM to supervise a 3G-telecommunication network. To provide to the NM the Fault Management capability for the network implies that the subordinate entities have to provide information about:

- events and failures occurring in the subordinate entities;
- events and failures of the connections towards the subordinate entities and also of the connections within the 3G network;
- the network configuration (due to the fact that alarms and related state change information are always originated by network resources, see 3GPP TS 32.600-series [1]). This is, however, not part of the FM functionality.

Therefore, for the purpose of FM the subordinate entities send notifications to a NM indicating:

- alarm reports (indicating the occurrence or the clearing of failures within the subordinate entities), so that the related alarm information can be updated;

- state change event reports, so that the related (operational) state information can be updated. This is, however, not part of the FM functionality.

The forwarding of these notifications is controlled by the NM operator using adequate filtering mechanisms within the subordinate entities.

The Itf-N provides also means to allow the NM operator the storage ("logging") and the later evaluation of desired information within the subordinate entities.

The retrieval capability of alarm-related information concerns two aspects:

- retrieval of "dynamic" information (e.g. alarms, states), which describes the momentary alarm condition in the subordinate entities and allows the NM operator a synchronization of its alarm overview data;
- retrieval of "history" information from the logs (e.g. active/clear alarms and state changes occurred in the past), which allows the evaluation of events that may have been lost, e.g. after an Itf-N interface failure or a system recovery.

As a consequence of the requirements described above, both the NM and the subordinate entity shall be able to initiate the communication.

5.1.5.5.3 TMF

This subsection gives a general overview of the network management philosophy according to TMF and how its meta data is structured. This is intended as supplementary information to section 5.1.5.1.6.

As described in [98] TMF's architecture is based on a distributed and interface oriented architecture. The basic entity is the interface and any running system (composed of runtime entities) makes use of (supports) some these interfaces. The runtime entities are composed of components, which are organized into models.

A software component [98] merges two perspectives:

- the component as an implementation: can be deployed and assembled into larger subsystems
- the component as an architectural abstraction: express design rules that impose a standard coordination model on all components

In order to arrive at a component model and a component framework [98] defines the following notions:

- component interface: coherent set of functional capabilities (attributes and operations)
- role: expected behaviour pattern of an agent in an interaction
- component model:
    - specifies the design rules, which must be obeyed by components
    - describes how components can be composed into larger assemblies (components again)
    - defines the external visibility of a component
- component framework: provides the services and mechanisms to support and enforce a component model

One of the most important points in TMF's network management definition is the distinction between

- technology independent concepts (leading to a Technology Neutral Architecture – TNA) and
- concepts specific to one or more technologies (leading to Technology Specific Architectures – TSA)

The software entities of an NGOSS system [98], which provide services to other entities do so via interfaces, which characterize the services with the following properties:

- A description of the service in terms of
    - The meta data used to describe the interface

- The meta data used o describe the operations that may be invoked on the service
- The set of results, which may be returned upon invocation of an operation

- The behaviour of the service (optional):
  - Preconditions under which an operation may be invoked
  - Postconditions definig the state a system is left in for each response of an invoked operation.
- The service must be manageable independently

Telemanagement Forum defines the following types of services:

- Basic Framework services: needed to support Application Domains (e.g. registration, Naming Location)
- OSS Framework Services: services to support any type of distributed OSS on the chosen NGOSS component model
- OSS Application Services: services specific to a Service Provider's environment (e.g. Fault Management, Billing)

One means to develop standard NGOSS solutions according to TM Forum is by applying the eTOM (enhanced Telecom Operations Map) developed by the TM Forum. It provides a business operations framework , which characterizes all the business activities a Service Provider will use.

It should be noted that eTOM has many single-enterprise aspects, but it has been recognized that for a business-to-business approach enterprise external aspects have to be taken into account as well.

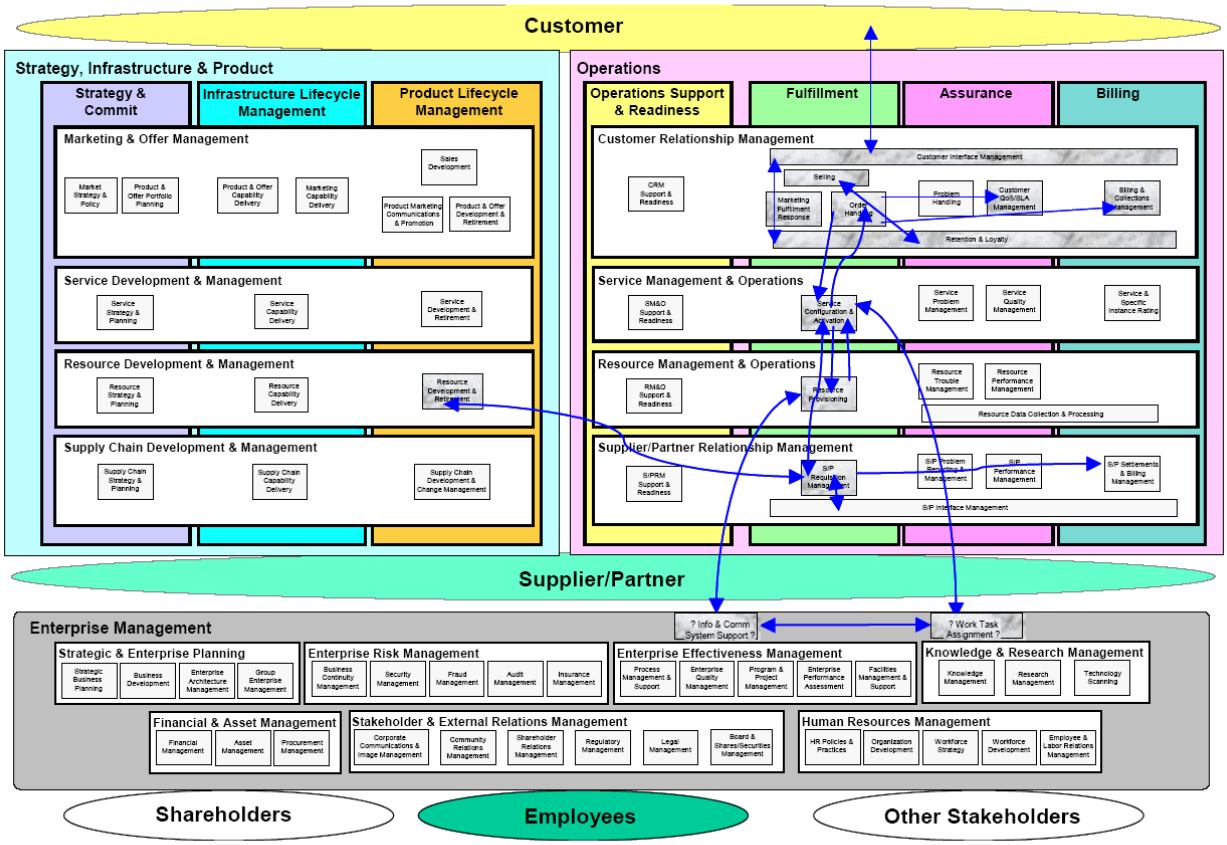


Figure 5.1.5.5.3.1: The Fulfillment process flow according to [115]

The eTOM concept is developed in different levels, each level providing more detail concerning the processes involved.

Level 0 – Conceptual View

The eTOM has three major process areas:

- Strategy, Infrastructure and Product: this bullet covers planning and life cycle management
- Operations: this bullet covers the core of operational management
- Enterprise Management: this bullet covers corporate or business management

In addition eTOM identifies four key functional process structures (horizontal rectangles in the figure above).

- Market, Product and Customer processes: processes concerning sales and channel management as well as marketing
- Service Processes: service development, service delivery, service configuration, service problem management, quality analysis, rating
- Resource Processes: development and delivery of resource infrastructure and its operational management
- Supplier/Partner Processes: deal with the interaction of the enterprise with its suppliers and partners.

Finally eTOM defines who interacts with the enterprise:

- Customers: to whom the products of the enterprise are sold
- Suppliers: provide resources or other capabilities
- Partners: operate with the enterprise in a shared area of business
- Employees: work for the enterprise
- Shareholders: have invested in the enterprise
- Stakeholders: have commitment to the enterprise other than through stock ownership

Level 1 – CxO View

There the eTOM is decomposed into a set of level 1 process groupings. One topic, dealt with in eTOM is Fulfillment. In [115] selected process flows are discussed. Figure 5.1.5.5.3.1 shows TMF's scenario for DSL end-to-end Fulfilment flows in their context with the overall eTOM level 1 model.

The figure has to be read under the following assumptions:

- There is limited pre-provisioning of infrastructure to end-users
- Part of the resources will be provided internally, part from external sources (e.g. an incumbent carrier provides the local loop)
- Multiple external suppliers are considered for the necessary external resources
- The service has moderate complexity

Most of the high level process linkages are within the level 1 Fulfilment process group, but still some interactions can be identified outside this vertical process area.

5.1.5.6 Personal Network Management (PNM)

5.1.5.6.1 3GPP

3GPP states in [86] that PNM provides a service to manage the Personal Network (PN) of a user comprising a number of registered UEs and PANs. That is, one user may possess more than one device to run multiple services. These devices have different capabilities which qualify the devices for specific applications.

Personal UE Networks and PNE (Personal Network Element) Networks are two scenarios for PNM. Personal UE Network enables the management of multiple UEs belonging to a single user. The functionality enabled is shown in figure 5.1.3.9.1.

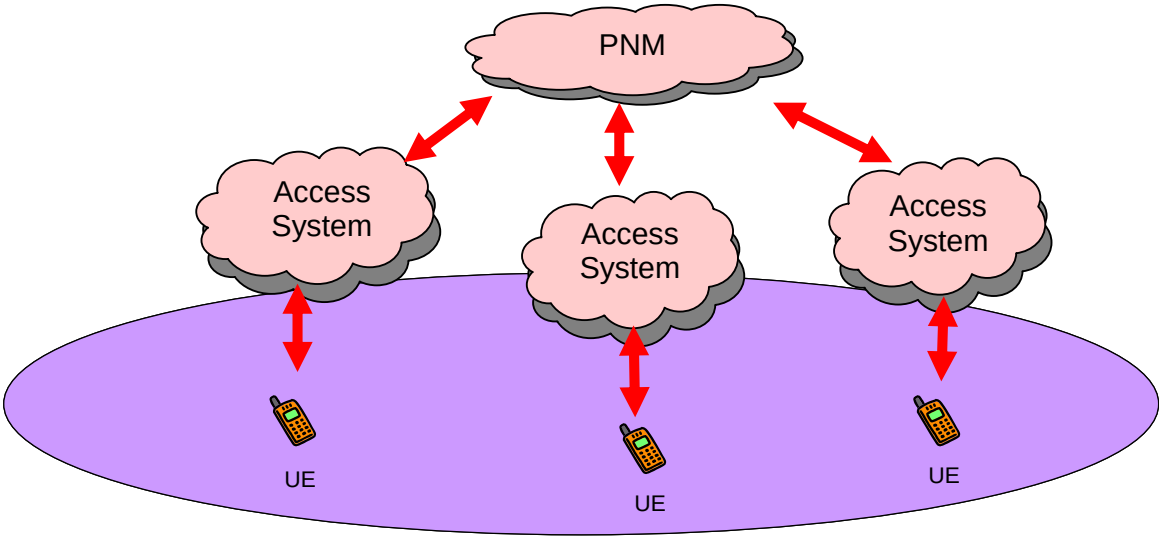


Figure 5.1.3.9.1: UEs managed by PNM e.g. UE Redirecting Service[86]

PNE Networks enable functions for the management and direct accessibility of the physically separated components of a UE, i.e. TEs and MEs. PNE Network functions comprise the management and communication of these PNEs within a PN including the redirection to UE and PAN (Personal Area Network) component.

Figure 5.1.3.9.1a illustrates the management of UE(s), UE components and TE(s), ME(s) or MT(s) and belonging to the same PAN(s).

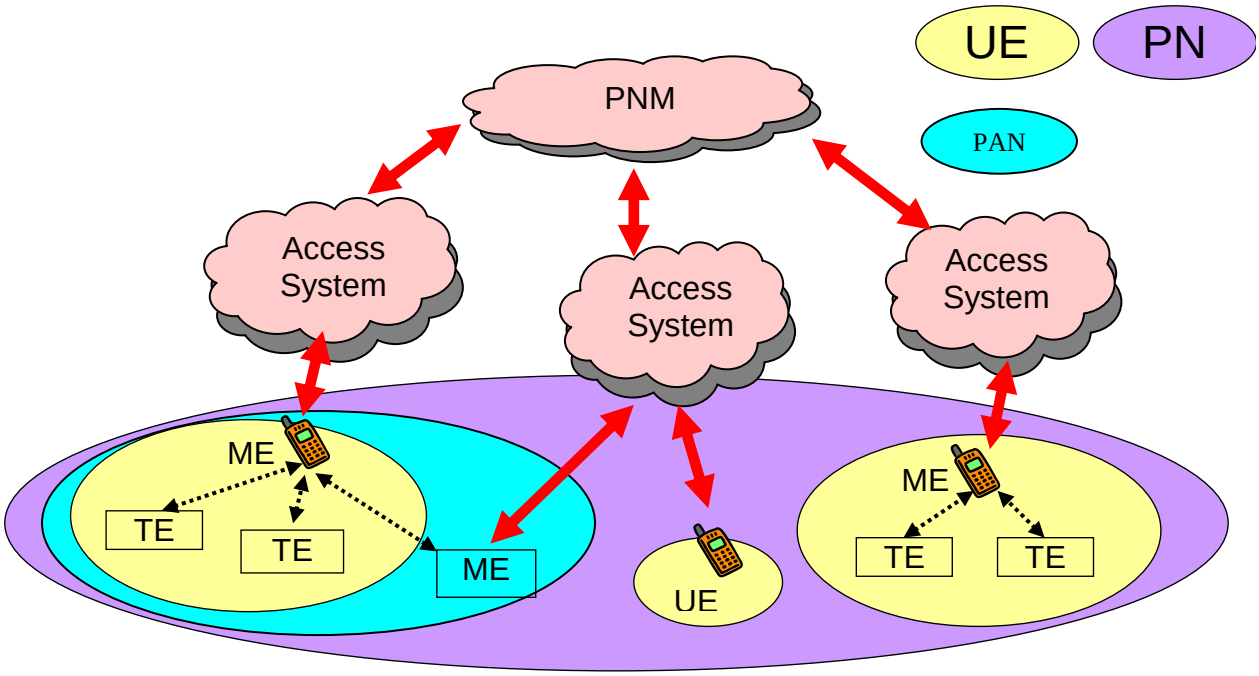


Figure 5.1.3.9.1a: Devices addressed by PAN Management

Personal UE Networks and PNE Networks both provides two services: Redirecting service and Private Network service. Redirection service is to redirect terminating services to selected UEs or physically separated UE components, while Private Network service is to maintain privacy and enable restricted access to a PN.

Figures 5.1.3.9.2 and 5.1.3.9.3 illustrate how PNM UE Redirecting Service integrates into the 3GPP architecture, including IMS architecture and CS domain architecture.

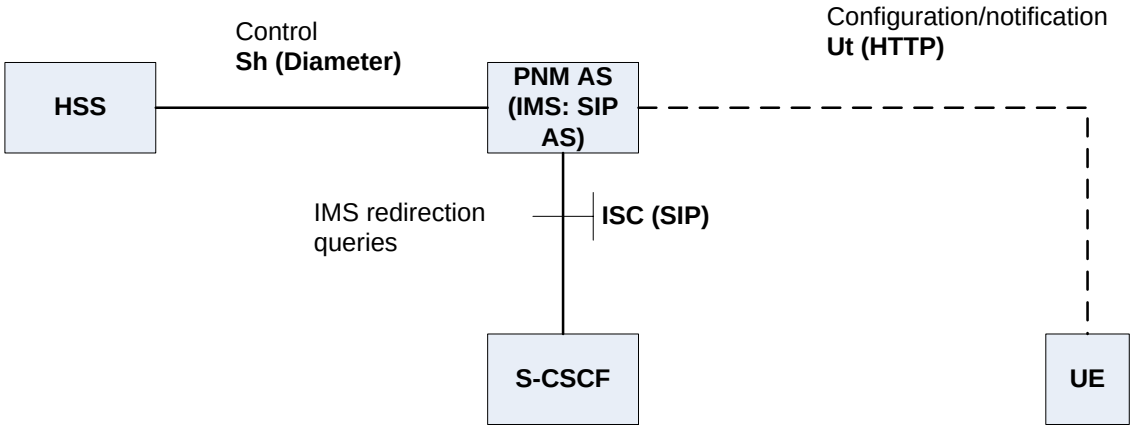


Figure 5.1.3.9.2: IMS architecture of the PNM UE Redirecting Service[61]

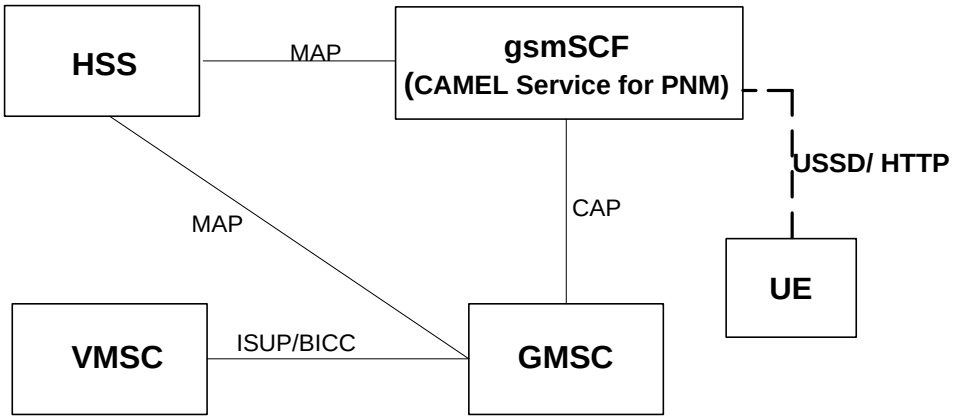


Figure 5.1.3.9.3: CS domain architecture of the PNM UE Redirecting Service[61]

The following user data may be stored and managed by PNM service:

- Public User Identity.
- Private User Identity.
- IMSI.
- PNE Identifier: is the PNE Identifier uniquely identifies each PNE of a PN within the PN. The PNE Identifier of MTs and MEs is the IMEI. Other PNEs have PNM-specific identifiers that are allocated for enabling PNM functions.
- The identity of PNM network.

5.2 Standardization documents containing subscriber/user information

This clause lists the standards, which deal with the end-user/subscriber information for the network functions introduced in clause 5.1.

Table 5.2.1: 3GPP

Number	Title
TS 23.008 V7.2.0 (2006-06)	Organization of Subscriber Data
TS 23.003 V7.0.0 (2006-06)	Numbering, addressing and identification (Release 6)
TS 23.097 V6.0.0 (2004-12)	Multiple Subscriber Profile (MSP) (Phase 2) - Stage 2 (Release 5)
TS 23.016 V6.1.0 (2004-03)	Subscriber data management; Stage 2; (Release 6)
TS 32.140 V6.3.0 (2004-12)	Subscription Management (SuM) requirements (Release 6)
TS 32.141 V6.1.0 (2004-03)	Subscription Management (SuM) architecture (Release 6)
TS 32.171 V6.1.0 (2004-12)	Subscription Management (SuM) Network Resource Model (NRM) Integration Reference Point (IRP): Requirements (Release 6)
TS 32.172 V6.3.0 (2006-03)	Subscription Management (SuM) Network Resource Model (NRM) Integration Reference Point (IRP): Information Service (IS) (Release 6)
TS 32.175 V6.2.0 (2005-06)	Subscription Management (SuM) Network Resource Model (NRM) Integration Reference Point (IRP): eXtensible Markup Language (XML) definition (Release 6)
3GPP TS 22.240 V6.5.0 (2005-01)	Service requirement for the 3GPP Generic User Profile (GUP); Stage 1 (Release 6)
TS 23.240 V6.7.0 (2005-03)	3GPP Generic User Profile (GUP); Architecture (Stage 2); (Release 6)
TR 23.941 V6.0.0 (2004-12)	3GPP Generic User Profile (GUP); Stage 2; Data Description Method (DDM) (Release 6)
TS 33.102 V7.0.0 (2005-12)	3G Security; Security architecture (Release 7)
TS 43.020 V6.4.0 (2006-06)	Security related network functions (Release 6)
TS 23.060 V7 .1.0 (2006-06)	General Packet Radio Service (GPRS); Service description; Stage 2 (Release 7)
TS 23.271 V6.13.0 (2005-09)	Functional stage 2 description of Location Services (LCS); (Release 6)
TS 25.305	Stage 2 functional specification of UE positioning in UTRAN
TS 43.059	Functional Stage 2 description of Location Services in GERAN
TS 23.141 V6.9.0 (2005-12)	Presence Service; Architecture and functional description (Release 6)
TS 23.228 V7.4.0 (2006-06)	IP Multimedia Subsystem (IMS); Stage 2 (Release 7)
TS 33.222 V7.1.0 (2006-03)	Generic Authentication Architecture (GAA); Access to network function functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (Release 7)
TS 33.102 V7.0.0 (2005-12)	3G Security; Security Architecture (Release 7)
TS 32.240 V6.3.0 (2005-09)	Telecommunication management; Charging management; Charging architecture and principles (Release 6)
TS 22.115 6.7.0 (2006-03)	Service aspects; Charging and billing (Release 7)
TS 22.140 V6.7.0 (2005-03)	Multimedia Messaging Service (MMS); Stage 1 (Release 6)
TS 23.140 V6.9.0 (2005-03)	Technical Specification Group Terminals; Multimedia Messaging Service (MMS); Functional description; Stage 2 (Release 6)
TS 22.242 V6.3.0 (2005-01)	Digital Rights Management (DRM); Stage 1 (Release 6)
TS 22.146 V8.1.0 (2006-09)	Multimedia Broadcast/Multicast Service; Stage 1 (Release 8)
TS 22.246 V8.1.0 (2006-09)	Multimedia Broadcast/Multicast Service (MBMS) user services; Stage 1 (Release 8)
TS 23.228 V7.4.0 (2006-06)	IP Multimedia Subsystem (IMS); Stage 2 (Release 7)
TR 23.979 V6.2.0 (2005-06)	3GPP enablers for Open Mobile Alliance (OMA); Push-to-talk over Cellular (PoC) services; Stage 2 (Release 6)
TR 25.zyx V0.0.1 Draft2(2006-0x)	Improved support of gaming over HSDPA/EDCH (Release 7)
TS 29.078 7.3.0 (2006-06)	Customised Applications for Mobile network Enhanced Logic; (CAMEL) Phase 4; CAMEL Application Part (CAP) specification; (Release 7)
TS 22.259 V8.1.0 (2006-09)	Service requirements for Personal Network Management (PNM); Stage 1 (Release 8)
TR 23.818 V0.8.0 (2006-11)	Optimisations and Enhancements for Realtime IMS communication (Release 7)
TS 32.111-1 V6.0.1 (2005-06)	Technical Specification Group Services and System Aspects; Telecommunication management; Fault Management; Part 1: 3G fault management requirements; (Release 6)

Table 5.2.2: 3GPP2

Number	Title
S.R0037-0 v3.0 Version Date: August 21, 2003 Version 3.0	IP Network Architecture Model for cdma2000 Spread Spectrum Systems
X.S0027-001-0 Version 1.0 Date: September, 2004	Presence Service: Architecture and Functional Description
3GPP2 S.R0064-0, Version 1.0, Version Date: 30 October 2002	Multimedia Messaging Services (MMS); Stage 1 Requirements

Table 5.2.3: ETSI/TISPAN

Number	Title
Draft ETSI DTS 188 002-1 V0.0.7 (2006-09)	Subscription Management Requirements
Draft ETSI TS 188 002-2 V0.0.3 (2006-09)	NGN Management; Management Information Model Requirements
WG8 interim meeting WG8TD08 Sophia Antipolis, 3 - 5 May 2006	Remaining Comments
ETS 300 374-1 (1994-09)	Intelligent Network (IN); Intelligent Network Capability Set 1 (CS1); Core Intelligent Network Application Protocol (INAP); Part 1: Protocol specification
EN 301 140-1 V1.3.4 (1999-06)	Intelligent Network (IN); Intelligent Network Application Protocol (INAP); Capability Set 2 (CS2); Part 1: Protocol specification
Final draft ETSI EN 301 931-1 V1.1.2 (2001-07)	Intelligent Network (IN); Intelligent Network Capability Set 3 (CS3); Intelligent Network Application Protocol (INAP); Protocol specification; Part 1: Common aspects

Table 5.2.4: IETF

Number	Title
RFC 2778 February 2000	A Model for Presence and Instant Messaging
RFC 2924 September 2000	Accounting Attributes and Record Formats
RFC 3588 September 2003	Diameter Based Protocol
RFC 3280 April 2002	Internet X.509 Public Key Infrastructure
RFC 2560 June 1999	PKIX OCSP
RFC 3060 February 2001	Policy Core Information Model
RFC 2251 December 1997	Lightweight Directory Access Protocol (v3)

Table 5.2.5: ITU-T

Number	Title
ITU-T X.509 08/2005	Information technology – Open systems interconnection – The directory: public-key and attribute certificate frameworks
ITU-T Q.822 04/1994	SPECIFICATIONS OF SIGNALLING SYSTEM No.7 – STAGE 1, STAGE 2 AND STAGE 3 DESCRIPTION FOR THE Q3 INTERFACE – PERFORMANCE MANAGEMENT
ITU-T Q.1211 03/1993	GENERAL RECOMMENDATIONS ON TELEPHONE SWITCHING AND SIGNALLING – INTELLIGENT NETWORK - INTRODUCTION TO INTELLIGENT NETWORK CAPABILITY SET 1
ITU-T Q.1231 09/1997	Q Series SWITCHING AND SIGNALLING – INTRODUCTION TO INTELLIGENT NETWORK CAPABILITY SET 2
ITU-T Q.1221 12/1997	Q Series SWITCHING AND SIGNALLING – INTRODUCTION TO INTELLIGENT NETWORK CAPABILITY SET 3
ITU-T M.3400 02/2000	SERIES M: TMN AND NETWORK MAINTENANCE: INTERNATIONAL TRANSMISSION SYSTEMS, TELEPHONE CIRCUITS, TELEGRAPHY, FACSIMILE AND LEASED CIRCUITS; Telecommunications management network; Telecommunications management network

Table 5.2.6: OMA

Number	Title
OMA-AD_IMS-V1_0-20040420-D Draft Version 1.0 – 20 Apr 2004	Utilization of IMS capabilities Architecture
OMA-TS-Presence_SIMPLE-V1_0-20060418-C Candidate Version 1.0 – 18 Apr 2006	Presence SIMPLE Specification
OMA-AD-Presence_SIMPLE-V1_0-20060110-C Candidate Version 1.0 – 10 Jan 2006	Presence SIMPLE Architecture Document
OMA-TS-MLP-V3_2-20051124-C Candidate Version 3.2 – 24 Nov 2005	Mobile Location Protocol 3.2
OMA-AD-MLS-V1_0-20050607-C Candidate Version 1.0 – 07 June 2005	OMA Mobile Location Service Architecture
OMA-TS-XDM_Core-V1_0-20060612-A Approved Version 1.0 – 12 Jun 2006	XML Document Management (XDM) Specification
OMA-TS-DM_StdObj-V1_2-20060602-C Candidate Version 1.2 – 02 Jun 2006	OMA Device Management Standardized Objects
OMA-SyncML-DMStdObj-V1_1_2-20031203-A Approved version 03-December-2003	SyncML Device Management Standardized Objects, Version 1.1.2
OMA-Security-CertProf-V1_1-20040615-C Candidate Version 1.1 – 15 Jun 2004	Certificate and CRL Profiles
OMA-TS-PoC_XDM-V1_0-20060609-A Approved Version 1.0 – 09 June 2006	PoC XDM Specification
OMA-RD-CPv12-V1_0-20050825-D, Draft Version 1.0 –25 Aug 2005	Client Provisioning v1.2 Requirements
OMA-RD-GPM-V1_0-20060824-D, Draft Version 1.0 – 24 Aug 2006	Global Permissions Management Requirements
OMA-AD-GPM-V1_0-20060828-D, Draft Version 1.0 – 28 Aug 2006	Global Permissions Management Architecture
OMA-AD-Policy_Evaluation_Enforcement_Management-V1_0 - 2006625-D, Draft Version 1.0 – 25 Jun 2006	Policy Evaluation, Enforcement and Management Architecture
OMA-MMS-ARCH-V1_2-20050301-A, Approved Version 1.2 – 01 Mar 2005	Multimedia Messaging Service, Architecture Overview
OMA-MMS-ENC-V1_2-20050301-A, Approved Version 1.2 – 01 Mar 2005	Multimedia Messaging Service Encapsulation Protocol
OMA-AD-Charging-V1_0-20060825-D, Draft Version 1.0 – 25 Aug 2006	Charging Architecture
OMA-RD_Charging-V1_0-20041118-C, Candidate Version 1.0 – 18 Nov 2004	Charging Requirements
OMA-AD-DRM-V2_0-20060303-A, Approved Version 2.0 – 03 Mar 2006	DRM Architecture
OMA-AD-BCAST-V1_0-20060329-D, Draft Version 1.0 –29 March 2006	Mobile Broadcast Services Architecture
OMA-RD-DCD-V1_0-20060530-C, Candidate Version 1.0 – 30 May 2006	Dynamic Content Delivery Requirements
OMA-AD-DCD-V1_0-20061014-D, Draft Version 1.0 – 14 October 2006	Dynamic Content Delivery Architecture
OMA-AD-IMS-V1_0-20050809-A, Approved Version 1.0 – 9 Aug 2005	Utilization of IMS capabilities Architecture
OMA-AD-IMPS-V1_3-20051011-C, Candidate Version 1.3 – 11 Oct 2005	IMPS Architecture
OMA-AD_PoC-V1_0-20060609-A, Approved Version 1.0 – 09 Jun 2006	Push to talk over Cellular (PoC) - Architecture
OMA-AD-DS-V2_0-20061011-D, Draft Version 2.0 – 11 Oct 2006	DS 2.0 Architecture
OMA-AD-Game-Services-V1_0-20060307-C, Candidate Version 1.0 - 03 Mar 2006	Game Services Architecture
OMA-RD-GSSM-V1_0-20061005-D, Draft Version 1.0 – 5 Oct 2006	General Service Subscription Management Requirements
OMA-RD-Identity_Management_Framework-V1_0-20050202-C, Candidate Version 1.0 – 02 Feb 2005	Identity Management Framework Requirements

Table 5.2.7: TMF

Number	Title
TMF Annex TMF053D, Release 4.0, Approved Version 1.1, August 2004	NGOSS Architecture, Technology Neutral Specification, Metamodel
TMF Annex TMF053B, Release 4.0, Approved Version 4.5, August 2004	NGOSS Architecture, Technology Neutral Specification, Contract Description: Business and System Views
TMF Annex TMF053C, Release 4.0, Approved Version 1.1, August 2004	NGOSS Architecture, Technology Neutral Specification, Contract Description: Behaviour and Control Services
TMF 053, Release 4.0, Approved Version 4.1, August 2004	The NGOSS Technology Neutral Architecture
GB922, Release 4.0, Approved Version 3.2, August 2004	Shared Information Data (SID) Model; Concepts, Principles, and Domains
GB922 Addendum 2, Release 4.0, Approved Version 3.2, August 2004	Customer Business Entity Definitions
GB921, Release 5.0, Enhanced Telecom Operations Map (eTOM)	The Business Process Framework; April 2005: "For the Information and Communications Services Industry
GB921 F, Release 4.5, Addendum F, Enhanced Telecom Operations Map (eTOM); The Business Process Framework; November 2004	Process Flow Examples

5.3 Basics of a Common User Data Model

5.3.1 Characteristics of an End-User

This section deals with issues coming up, when a common user data model should be built. The word "user" is meant here in the sense of an end-user as the human being, who

- uses certain services,
- enjoys certain privileges and
- has certain preferences.

The first intention is to

- give a short classification of the data, which might at some time be put into the end-user data model,
- then look at those attributes, which will in some way represent primary keys within an end-user database and analyse, which interdependencies there might be and
- finally define, which attributes are the same in different network functions or management applications introduced in the section above.

The second intention is to relate the concept of an end-user, as it is described in this section to the concept of a subscriber (here also "contract holder"), which is the one used and known today.

The third intention of this section is to show, how the building blocks of an Adaptation Layer can help in bringing many network functions on top of a centralized end-user data store.

Note: It is not the intention of this section to provide a "complete" schema definition on the basis of all data collected in the section above.

5.3.1.1 Types of Data Assigned to an End-User

In the section above - which introduced many of the relevant network functions and management applications that could profit from and contribute to a common data model - the end-user data description was generally structured according to

the type of service the data in question represented. This subsection introduces additional criteria, according to which data can be classified:

- Operator's point of view: One distinction, which is important for an operator, is the fact whether the stored data are relevant for call-setup/processing or not.
- Characterization via identities: An end-user can be characterized by primary keys like an IMSI, MSISDN, Puiblic ID, Private ID, PIN, ….
- Characterization of an end-user versus a contract holder (in 3GPP called subscriber): Here the question is addressed, which data characterize someone, who uses a service versus someone, who is subscribed to this service.

Seen from the point of view of an operator, an end-user can have three different types of data:

  - Profile data: These are data characterizing the services assigned to the end-user (these are mainly the data described in the first section of this document),
  - his privileges and
  - his preferences.

- Completely private data: These are data stored by the end-user and only seen by him or her(e.g. digital pictures).
- Private data influencing the call processing: These are data, which are also privately owned by the end-user, but will influence the way services are executed (e.g. private e-mail distribution list).

5.3.1.2 The Identity of an End-User

5.3.1.2.1 The UID

This clause highlights the relationship between an end-user, his identities and a contract holder. Please note that the results presented in this subsection are not yet standardized and are intended as suggestions as a way forward for any standardization efforts on the topic of an end-user centric data model.

The general idea is to have an object model entity called UID (user identification), which represents the root for the whole end-user model. As an example for a key the entity IMSI is shown in a 1:n relationship with the UID. This relationship expresses the fact that an end-user can have n end-user equipments providing some types of telephony or data services. In addition the end-user is using services, which someone – the contract holder or subscriber – must have subscribed to, In this case there is an n:m relation between the UID and the contract holder (e.g. the end-user has one end-user equipment plus subscription from his company and another UE plus services is subscribed by himself). As a consequence there is a third relation, namely the one between the contract holder and the respective identity, which, in case of the IMSI represents subscription information. This relation will be 1:m.

The figure below shows the relation between the UID, the contract holder and the IMSI in an UML diagram.

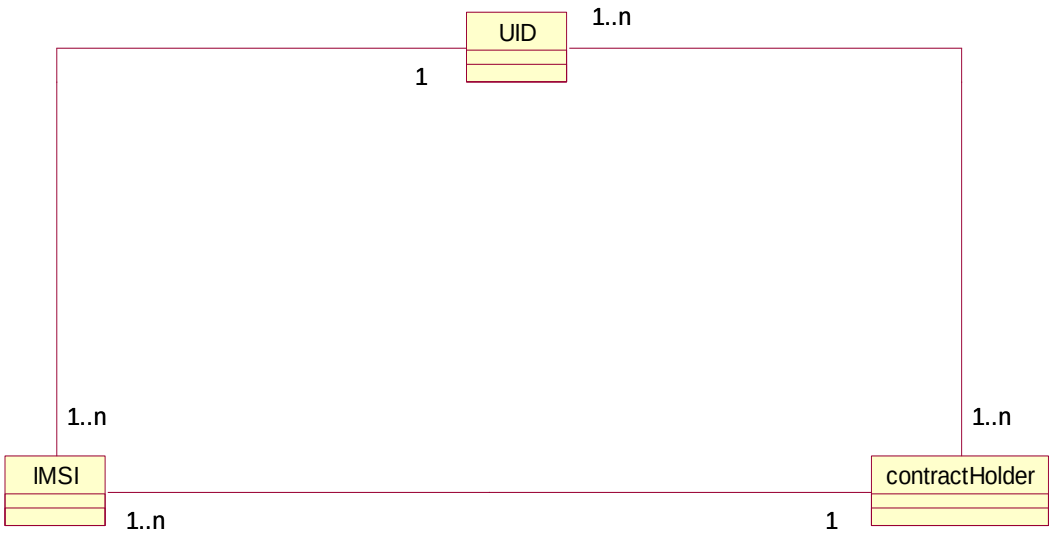


Figure 5.3.1.2.1.1: General Picture of the relationship between an end-user and a contract holder

In the next clause the relation of the end-user to his various key attributes will be discussed in detail. Finally this subsection will treat an example, which shows the connection between an end-user and a subscriber in more detail.

5.3.1.2.2 Representation of the Identity of the End-User through his Keys

Depending on the service used by the end-user, identification of the same might be achieved by different keys (examples of which can be found in [2], [3]): IMSI, MSISDN, Public Key, Private Key, etc. Each of these keys describes part of the identity of the end-user. In order to identify an end-user completely and uniquely the relations between these different keys and the UID have to be defined.

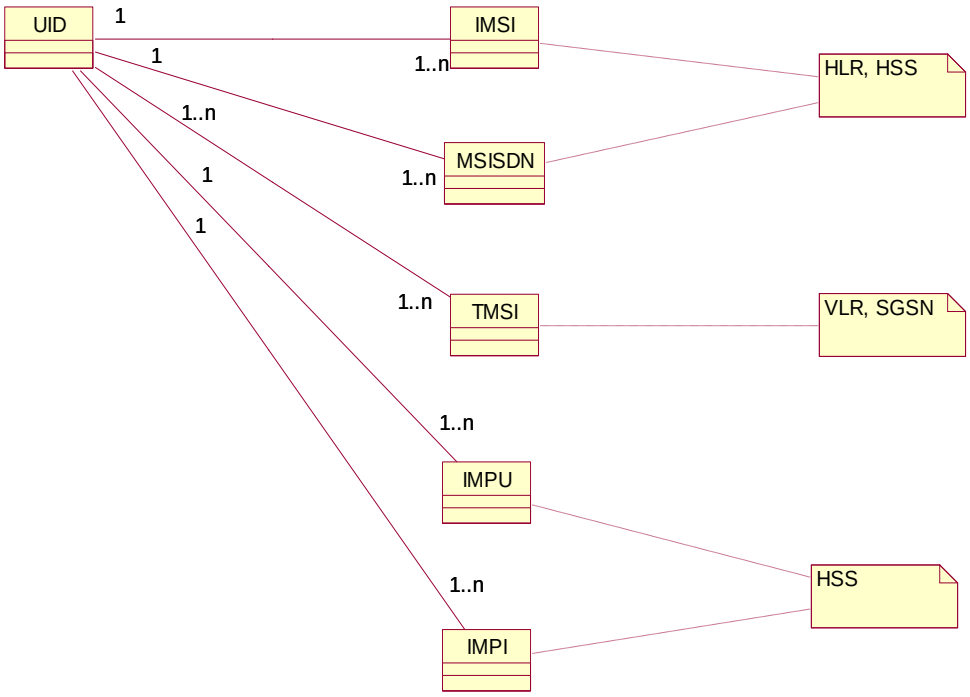


Figure 5.3.1.2.2.1: Characterization of one end-user

In clause 5.3.1.3 the relation between an end user and a subscriber has been described. Further more, the relation among the identities belonging to an end user should be considered. The relation should make the deployment and billing of end user oriented services easy.

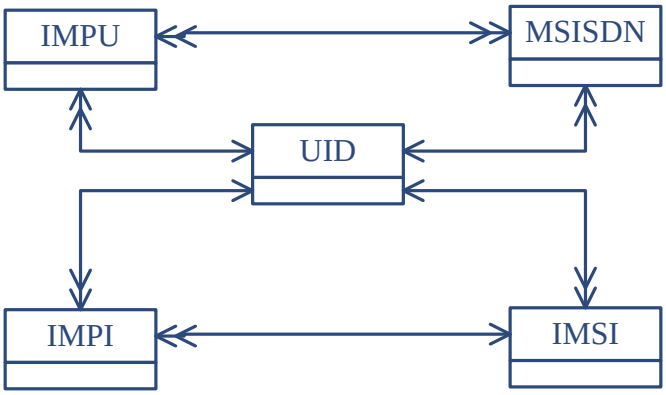


Figure 5.3.1.2.2.2: The relation among the identities of an end-user

Figure 5.3.1.2.2.2 shows the relationship among the identities of an end user: an end user (with his UID) has several private and public identities related to different services. In order to identify the information of co-located USIM and ISIM, as mentioned in the motivation statement 2 and 3 in the clause 4.1, there should be association between IMSI and IMPIs or/and between MSISDN and IMPUs. Meanwhile, the association between IMPUs and MSISDNs could help operator to provide users conbined services spanning CS, PS and IMS.

In the 3GPP area [3] the following partial identities of an end-user have been defined:

Identification of subscribers:

International Mobile Subscriber Identity (IMSI): unique, shall be allocated to each mobile subscriber in the GSM/UMTS system.

Temporary Mobile Subscriber Identities (TMSI): may be allocated by the VLRs and SGSNs to visiting mobile subscribers in order to support the subscriber identity confidentiality service. The VLR and SGSNs must be capable of correlating an allocated TMSI with the IMSI of the MS to which it is allocated.

P-TMSI: An MS may be allocated two TMSIs, one for services provided through the MSC, and the other (P-TMSI) for services provided through the SGSN.

Temporary Logical Link Identity (TLLI): used for addressing on resources used for GPRS. The TLLI to use is built by the MS

- either on the basis of the P-TMSI (local or foreign TLLI),
- or directly (random TLLI).

Local Mobile Station Identity (LMSI): defined in order to speed up the search for subscriber data in the VLR.

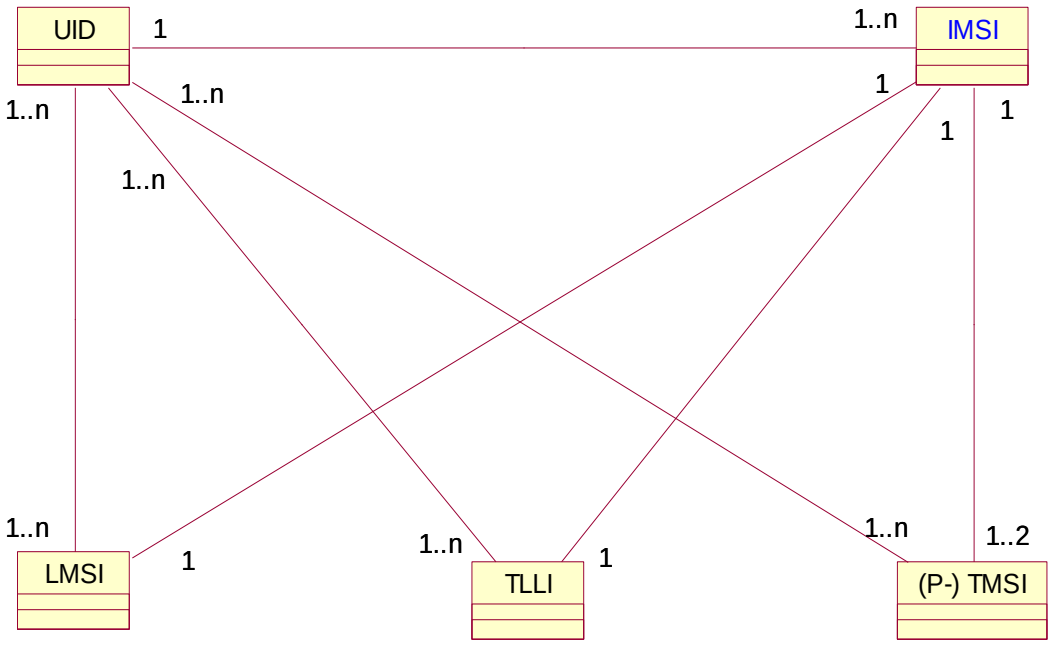


Figure 5.3.1.2.2.3: Temporary characterization of one end-user

Numbers assigned to the MS

According to [3] any numbering plan should at least (but not exclusively) support the following points:

- It should be possible for any subscriber of the ISDN or PSTN to call any MS in a PLMN.
- The numbering/addressing plan should not limit the possibility for MSs to roam among PLMNs.
- It should be possible to change the IMSI without changing the ISDN number allocated to an MS and vice versa.
- It should be possible for any subscriber of the CSPDN/PSPDN to call any MS in a PLMN.
- It should be possible for any fixed or mobile terminal to communicate with a mobile terminal using an IP v4 address or IP v6 address.

MS international ISDN numbers (MSISDN): allocated from the ITU-T Recommendation E.164 numbering plan; see also ITU-T Recommendation E.213. The composition of the MSISDN number should be such that it can be used as a global title address in the Signalling Connection Control Part (SCCP) for routeing messages to the home location register of the MS.

Mobile Station Roaming Number (MSRN): used to route calls directed to an MS. On request from the Gateway MSC via the HLR it is temporarily allocated to an MS by the VLR with which the MS is registered; it addresses the Visited MSC collocated with the assigning VLR. More than one MSRN may be assigned simultaneously to an MS.

MS international data numbers: should comply with the data numbering plan of ITU-T Recommendation X.121 as applied in the home country of the mobile subscriber.

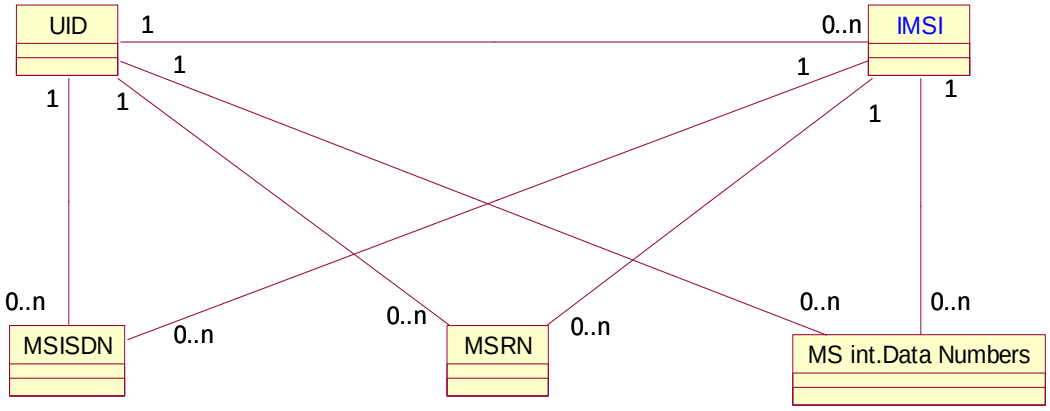


Figure 5.3.1.2.2.4: Characterization of one end-user via numbers assigned to an MS

Handover number: used for establishment of a circuit between MSCs to be used for a call being handed over. The structure of the handover number is the same as the structure of the MSRN.

IP v4/v6 address: may be allocated to an MS either permanently or temporarily during a connection with the network. One or more IP address domains may be allocated to each PLMN.

Identification of local areas and base stations

Location Area Identification (LAI): is composed as follows

- Mobile Country Code (MCC) identifies the country in which the GSM PLMN is located. The value of the MCC is the same as the three digit MCC contained in international mobile subscriber identity (IMSI);
- Mobile Network Code (MNC) is a code identifying the GSM PLMN in that country. The MNC takes the same value as the two or three digit MNC contained in IMSI;
- Location Area Code (LAC) is a fixed length code (of 2 octets) identifying a location area within a PLMN.

Routing Area Identification (RAI): is composed as follows:

- A valid Location Area Identity (LAI): as defined above.
- Routeing Area Code (RAC): fixed length code (of 1 octet) identifying a routeing area within a location area.

Cell Global Identification (CGI): concatenation of the

- Location Area Identification and
- Cell Identity: shall be unique within a location area.

Base Station Identity Code (BSIC): local colour code that allows an MS to distinguish between different neighbouring base stations. BSIC is structured as follows:

- NCC: PLMN Colour Code
- BCC: BS Colour Code

PLMN-specific Regional Subscription: defines unambiguously for the entire PLMN the regions in which roaming is allowed. It consists of

- one or more regional subscription zones. The regional subscription zone is identified by a Regional Subscription Zone Identity (RSZI) which consists of:
    - the Country Code (CC): identifies the country in which the PLMN is located;
    - the National Destination Code (NDC): identifies the PLMN in that country;

- the Zone Code (ZC): identifies a regional subscription zone as a pattern of allowed and not allowed location areas uniquely within that PLMN.

CC and NDC are ITU-T E.164 VLR or SGSN numbers. If a mobile subscriber has a regional subscription [3], the HLR shall store a list of up to ten Regional Subscription Zone Identities (RSZIs) per Network Destination Code (NDC) of the PLMN involved.

Location Number: defines a specific location within a PLMN. The location number is formatted according to ITU-T Recommendation E.164, as follows:

- The Country Code (CC) and
- National Destination Code (NDC) fields of the location number are those which define the PLMN of which the location is part.

Identities for MSCs, GSNs, and location registers

MSCs, GSNs and location registers are identified by international PSTN/ISDN numbers and/or Signalling Point Codes ("entity number") i.e.:

- "HLR number",
- "VLR number",
- "MSC number",
- "SGSN number" and
- "GGSN number"

in each PLMN.

Additionally SGSNs and GGSNs are identified by GSN Addresses:

- The Address Type, which is a fixed length code (of 2 bits) identifying the type of address that is used in the Address field.
- The Address Length, which is a fixed length code (of 6 bits) identifying the length of the Address field.
- The Address, which is a variable length field which contains either an IPv4 address or an IPv6 address.

These are the

- SGSN Address and the
- GGSN Address.

Address Type 0 and Address Length 4 are used when Address is an IPv4 address. Address Type 1 and Address Length 16 are used when Address is an IPv6 address.

HLR id: identifies an HLR (n:1 relation); consists of the leading digits of the IMSI (MCC + MNC + leading digits of MSIN).

International Mobile Station Equipment Identity and Software Version Number

International Mobile station Equipment Identity (IMEI): is composed as follows:

- Type Allocation Code (TAC): Its length is 8 digits;
- Serial Number (SNR): individual serial number uniquely identifying each equipment within the TAC. Its length is 6 digits;
- Spare digit: shall be zero, when transmitted by the MS.

International Mobile station Equipment Identity and Software Version Number (IMEISV): is composed as follows:

- Type Allocation Code (TAC): Its length is 8 digits;
- Serial Number (SNR): individual serial number uniquely identifying each equipment within each TAC. Its length is 6 digits;
- Software Version Number (SVN): identifies the software version number of the mobile equipment. Its length is 2 digits.

Identification of Voice Group Call and Voice Broadcast Call Entities

Group Identity (Group ID): identifies logical groups of subscribers

- to the Voice Group Call Service (VGCS): unique within a PLMN
- to the Voice Broadcast Service (VBS): unique within a PLMN

Note:

- There is no uniqueness between the two sets of IDs.
- VGCS or VBS shall also be provided for roaming. If this applies, certain Group IDs shall be defined as supra-PLMN Group IDs which have to be co-ordinated between the network operators and which shall be known in the networks and in the SIM

Group Call Area ID: allows grouping of cells into specific group call areas in support of both

- the Voice Group Call Service (number uniquely assigned to a group call area in one network) and
- the Voice Broadcast Service (number uniquely assigned to a group call area in one network)

Voice Group Call Reference: Specific instances of voice group calls; composed of the Group ID and the Group Call Area ID; can be specific for each network operator

Voice Broadcast Call Reference: Specific instances of voice broadcast calls; composed of the Group ID and the Group Call Area ID; can be specific for each network operator

Access Point Name (APN)

The APN is composed of two parts as follows:

- The APN Network Identifier: this defines to which external network the GGSN is connected and optionally a requested service by the MS. This part of the APN is mandatory.
- The APN Operator Identifier: this defines in which PLMN GPRS backbone the GGSN is located. This part of the APN is optional.

The APN field in the HLR may contain a wild card APN if the HPLMN operator allows the subscriber to access any network of a given PDP Type. If an SGSN has received such a wild card APN, it may either choose the APN Network Identifier received from the Mobile Station or a default APN Network Identifier for addressing the GGSN when activating a PDP context.

Identification of the Cordless Telephony System entities

Fixed Part Beacon Identity (FPBI): local identity broadcasted by every Cordless Telephony System Fixed Part (CTS-FP); contains an Access Rights Identity.

CTS-MS has:

- an Access Rights Key in order to identify a CTS-FP via FPBI
- a CTS Mobile Subscriber Identity (CTSMSI).

These operate as a pair.

CTS Mobile Subscriber Identities (CTSMSI): temporary identities which are used for paging and to request access; each CTS-MS has one or more CTSMSIs. The CTSMSI is composed of the following elements:

- CTSMSI Type:
- Significant Part:

International Fixed Part Equipment Identity (IFPEI): composed of the following elements (each element shall consist of decimal digits only):

- Type Approval Code (TAC):
- Final Assembly Code (FAC):
- Serial NumbeR (SNR):
- Software Version Number (SVN) identifies the software version number of the fixed part equipment. Its length is 2 digits.

International Fixed Part Subscription Identity (IFPSI): composed of the following elements (each element shall consist of decimal digits only):

- Mobile Country Code (MCC): The MCC identifies the country of the CTS-FP subscriber (e.g. 208 for France);
- CTS Operator Number (CON):
- Fixed Part Identification Number (FPIN): identifies the CTS-FP subscriber.

The National Fixed Part Subscriber Identity (NFPSI): consists of the

- CTS Operator Number and the
- Fixed Part Identification Number.

Identification of Localised Service Area

Cells may be grouped into specific localised service areas.

Localised Service Area Identity (LSA ID): identifies a localised service area; no restrictions are placed on what cells may be grouped into a given localised service area. The LSA ID can either be a PLMN significant number or a universal identity. This shall be known both in the networks and in the SIM.

Identification of PLMN, RNC, Service Area, CN domain and Shared Network Area

Public Land Mobile Network Identifier (PLMN-Id): uniquely identifies a PLMN, consists of

- Mobile Country Code (MCC) and
- Mobile Network Code (MNC).

CN Domain Identifier: identifies a CN Domain Edge Node within the UTRAN for relocation purposes.

- The CN Domain identifier for Circuit Switching (CS): consists of the
    - PLMN-Id and the
    - LAC
- The CN Domain identifier for Packet Switching (PS): consists of the
    - PLMN-Id, the
    - LAC, and the

- RAC of the first accessed cell in the target RNS.

CN Identifier (CN-Id): identifies a CN node uniquely within a PLMN.

Global identification of the CN node:

- CN-Id together with
- PLMN identifier.

RNC Identifier (RNC-Id): identifies an RNC node uniquely.

The Service Area Identifier (SAI): identifies an area consisting of one or more cells belonging to the same Location Area (this area is called a Service Area - used for indicating the location of a UE to the CN). The SAI consists of

- The Service Area Code (SAC) together with
- the PLMN-Id and the LAC

The Shared Network Area Identifier (SNA-Id): identifies an area consisting of one or more Location Areas (called a Shared Network Area - used to grant access rights to parts of a Shared Network to a UE in connected mode); consists of the

- PLMN-Id followed by the
- Shared Network Area Code (SNAC).

Numbering, addressing and identification within the IP multimedia core network subsystem

Home Network Domain Name: shall be in the form of an Internet domain name

If there is no ISIM application, the UE shall derive the home network domain name from the IMSI as described in the following steps:

- take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
- use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.3gppnetwork.org" domain name;
- add the label "ims." to the beginning of the domain.

An example of a home network domain name is: IMSI in use: 234150999999999; where:

- MCC = 234;
- MNC = 15;
- MSIN = 0999999999,

  This gives the home network domain name: ims.mnc015.mcc234.3gppnetwork.org

Private User Identity: shall take the form of an NAI, and shall have the form username@realm

If there is no ISIM application, the private user identity is not known. If the private user identity is not known, the private user identity shall be derived from the IMSI. With the example from above one gets: 234150999999999@ims.mnc015.mcc234.3gppnetwork.org

Public User Identity: shall take the form of either

- a SIP URI (see IETF RFC 3261) or
- a tel URL (see IETF RFC 3966).

A SIP URI for a Public User Identity shall take the form "sip:user@domain".

If there is no ISIM application to host the public user identity, a temporary public user identity shall be derived, based on the IMSI. With the example of above one gets "sip:234150999999999@ims.mnc015.mcc234.3gppnetwork.org".

Public Service Identity (PSI): identifies a service, or a specific resource created for a service on an application server. The domain part is pre-defined by the IMS operators and the IMS system provides the flexibility to dynamically create the user part of the PSIs; shall take the form of either a

- SIP URI or a
- Tel URI

The PSIs are stored in the HSS either as a distinct PSI or as a wildcarded PSI. A distinct PSI contains the PSI that is used in routing, whilst a wildcarded PSI represents a collection of PSIs (the following PSI could be stored in the HSS - "sip:chatlist!.*!@example.com").

Anonymous User Identity: shall take the form of a SIP URI ("sip:anonymous@anonymous.invalid")

Unavailable User Identity: shall take the form of a SIP URI ("sip:unavailable@unknown.invalid")

Emergency Public User Identity: shall be derived from a public user identity as follows:

- UE selects any public user identity that is a SIP URI from ISIM. If the UE does not have ISIM, UE derives a temporary public user identity from IMSI as described above.
- UE adds "sos." to the beginning of the domain part of the selected public user identity.

For example if the SIP URI for the selected public user identity is "sip:user@domain", the corresponding emergency public user identity is "sip:user@sos.domain".

Numbering, addressing and identification for 3GPP System to WLAN Interworking

Home Network Realm: shall be in the form of an Internet domain name, e.g. operator.com.

When attempting to authenticate within WLAN access, the WLAN UE shall derive the home network domain name from the IMSI as described in the following steps:

- take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
- use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>. 3gppnetwork.org" domain name;
- add the label "wlan." to the beginning of the domain name.

With the example from above one gets wlan.mnc015.mcc234.3gppnetwork.org.

Root NAI: shall take the form of a NAI, and shall have the form username@realm as specified above.

- The username part format of the Root NAI shall comply with
    - IETF RFC 4187 when EAP AKA authentication is used and with
    - IETF RFC 4186 , when EAP SIM authentication is used.
- When the username part includes the IMSI, the Root NAI shall be built according to the following steps:
    - Generate an identity conforming to NAI format from IMSI as defined in EAP SIM [51] and EAP AKA as appropriate
    - Convert the leading digits of the IMSI, i.e. MNC and MCC, into a domain name.

  The result will be a root NAI of the form:

  "0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP AKA authentication and
  "1<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP SIM authentication

Using the example above, for EAP AKA authentication: If the IMSI is 234150999999999 (MCC = 234, MNC = 15), the root NAI then takes the form 0234150999999999@wlan.mnc015.mcc234.3gppnetwork.org.

Decorated NAI: takes the form of a NAI and shall have the form 'homerealm!username@otherrealm' .

- realm part: consists of
    - 'otherrealm' is the realm built using the PLMN ID (visitedMCC + visited MNC) of the PLMN selected as a result of WLAN PLMN selection.
    - 'Homerealm' is the realm as specified using the HPLMN ID ('homeMCC' + 'homeMNC)'.
- The username part format of the Root NAI shall comply with
    - IETF RFC 4187 when EAP AKA authentication is used and with
    - IETF RFC 4186 when EAP SIM authentication is used.

  When the username part of Decorated NAI includes the IMSI, the result will be a decorated NAI of the form:

  "wlan.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org !0<IMSI>@wlan.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org", for EAP AKA authentication and " wlan.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org !1<IMSI>@wlan.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org ", for EAP SIM authentication

Using the example from above for EAP AKA authentication: If the IMSI is 234150999999999 (MCC = 234, MNC = 15) and the PLMN ID of the Selected PLMN is MCC = 610, MNC = 71 then the Decorated NAI takes the form wlan.mnc015.mcc234.3gppnetwork.org!0234150999999999@wlan.mnc071.mcc610.3gppnetwork.org.

Alternative NAI: shall take the form of a NAI, i.e. 'any_username@REALM' as specified of IETF RFC 4282. The Alternative NAI

- shall not be routable from any AAA server,
- shall contain a username part which is not derived from the IMSI,
- username part shall not be a null string.

W-APN: composed of two parts as follows:

- The W-APN Network Identifier; this defines to which external network the PDG is connected.
- The W-APN Operator Identifier; this defines in which PLMN the PDG serving the W-APN is located.

Identification of Multimedia Broadcast/Multicast Service

Temporary Mobile Group Identity (TMGI): identifies Multicast and Broadcast bearer services within MBMS uniquely; composed of three parts:

- MBMS Service ID: uniquely identifies an MBMS bearer service within a PLMN.
- Mobile Country Code (MCC): uniquely identifies the country of domicile of the BM-SC;
- Mobile Network Code (MNC): identifies the PLMN which the BM-SC belongs to.

MBMS Service Area (MBMS SA): comprises of one or more MBMS Service Area Identities (MBMS SAIs), in any case each MBMS SA shall not include more than 256 MBMS SAIs.

MBMS Service Area Identity (MBMS SAI): identifies a group of cells within a PLMN that is independent of the associated Location/Routing/Service Area and the physical location of the cell(s). A cell shall be able to belong to one or more MBMS SAs, and therefore is addressable by one or more MBMS SAIs.

Numbering, addressing and identification within the GAA subsystem

Bootstrapping Server Function (BSF) address: The UE shall discover the BSF address from the identity information related to the UICC application that is used during the bootstrapping procedure i.e. IMSI for USIM, or IMPI for ISIM, in the following way:

- In the case where the USIM is used in bootstrapping, the BSF address shall be derived as follows:
    - take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
    - use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" domain name;
    - add the label "bsf." to the beginning of the domain.

  Example 1: If IMSI in use is "234150999999999", where MCC=234, MNC=15, and MSIN=0999999999, the BSF address would be "bsf.mnc015.mcc234.pub.3gppnetwork.org".
- In the case where ISIM is used in bootstrapping, the BSF address shall be derived as follows:
    - extract the domain name from the IMPI;
    - add the label "bsf." to the beginning of the domain.

  Example 2: If the IMPI in use is "user@operator.com", the BSF address would be "bsf.operator.com ".

Numbering, addressing and identification within the Generic Access Network

Home network realm: shall be in the form of an Internet domain name. UE derives the home network realm from the IMSI in the following steps:

- take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
- use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.3gppnetwork.org" network realm;
- add the label "gan." to the beginning of the network realm.

An example of a home network realm is: IMSI in use: 234150999999999 where: MCC = 234; MNC = 15; MSIN = 0999999999, which gives the home network realm: gan.mnc015.mcc234.3gppnetwork.org

Full Authentication NAI: in both EAP-SIM and EAP-AKA shall take the form of an NAI as specified in clause 2.1 of IETF RFC 4282. The format of the Full Authentication NAI shall comply with

- IETF RFC 4187 when EAP-AKA authentication is used and with
- IETF RFC 4186, when EAP-SIM authentication is used.

Fast Re-authentication NAI: in both EAP-SIM and EAP-AKA shall take the form of an NAI as specified in clause 2.1 of IETF RFC 4282. The UE shall use the re-authentication identity received during the previous EAP-SIM or EAP-AKA authentication procedure.

Home network domain name: shall be in the form of an Internet domain name, e.g. operator.com. The UE shall derive the home network domain name from the IMSI as described in the following steps:

- take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
- use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" domain name;
- add the label "gan." to the beginning of the domain name.

Using the example of above gives the home network domain name: gan.mnc015.mcc234.pub.3gppnetwork.org

Provisioning GANC-SEGW identifier: takes the form of a fully qualified domain name (FQDN) as specified in IETF RFC 1035.

Provisioning GANC identifier: takes the form of a fully qualified domain name (FQDN) as specified in IETF RFC 1035.

Addressing and Identification for Voice Call Continuity

CS Domain Routeing Number (CSRN): used to route a call from the IM CN subsystem to the user in the CS domain.

IP Multimedia Routeing Number (IMRN): routable number that points to the IM CN subsystem. In a roaming scenario, the IMRN has the same structure as an international ISDN number. The Tel URI format of the IMRN (see IETF RFC 3966) is treated as a PSI within the IM CN subsystem.

VCC Domain Transfer Number (VDN): is a public telecommunication number, as defined by ITU-T Recommendation E.164, and is used by the UE to request Domain Transfer to the CS domain from the Domain Transfer Function within VCC.

VCC Domain Transfer URI (VDI): Tel URI (see IETF RFC 3966) used by the UE to request Domain Transfer to IMS from the Domain Transfer Function within VCC.

5.3.1.2.3 Identity Management of the End-User

In this subsection some consequences, both legal and business related, of looking at an end-user are covered. Identity Management is shown to cover these issues as a concept and the standardized version of OMA is introduced.

5.3.1.2.3.1 Motivation for analysing Identity Management

The identity of a person (in the context of this TR the end-user) comprises many partial identities [46] which represent the person in specific contexts or roles. For the 3GPP, OMA ITU-T etc many of these identities have been shown in section 5.1 Managing the identity of this end-user means managing the various partial identities.

According to [46] today's most broadly accepted definition of legal person is a human being to which the legal systems refers rights, privileges and obligations (Kelsen 1966).

Under current legislation, the identity of physical persons in legislation has no systematic regulation. It is a stratification of definitions, which do not always match with each other and has two main functions:

- To grant identification for legal purposes and
- To protect individual rights of freedom (name, identity, self determination, freedom of speech, privacy, etc.) related to a physical person.

The aspects of the human personality granted by the (constitutional) legislation of democratic legal systems, regulated by private law and also protected against unilateral unauthorised aggression by third parties are:

- The name and the identity;
- Freedom from physical constriction (habeas corpus);
- Inviolability of the domicile and right of privacy;
- Freedom of speech and self expression, in particular two sub-categories of it:
    - The right to choose one's image;
    - The right to protect one's honour;
- Freedom of movement and to settle (granted only to fully aged people).

The personal identity is regulated at constitutional level, by the treaty of the European Union, by national private legislation, and protected by rules of the criminal law, against unduly unauthorised interference by third parties. Moreover administrative law regulates personal identity.

The Concept of Identity in the European Directive

The European Directive 95/46/CE about data protection is aimed at giving to the data subject (owner of data) the most control possible on its own identity and personal data, posing a series of requirements on recipients, controllers, processors and even third parties. Art. 2, letter a), giving a definition of "personal data", says: "identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

The main principles behind the Data Protection Directive are:

- Personal data must always be processed fairly and lawfully
- Personal data must be collected for explicit and legitimate purposes and used accordingly
- Personal data must be relevant and not excessive in relation to the purpose for which they are processed
- Data that identify individuals must not be kept longer than necessary.
- Data must be accurate and, where necessary, kept up to date
- Data controllers are required to provide reasonable measures for data subjects to rectify, erase or block incorrect data about them
- Appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data
- Personal data must not be transferred to a country or territory outside the European Economic Area unless that country ensures an "adequate level of protection" for data subjects.

Technologically, the terms "ID" or "identifier" play a big role rather than "identity" and denote "technological identities" of any possible object (or subject). An identifier could be a name, a serial number, or some other pointer or address to the entity being identified. Some identifiers allow unique mapping to a specific individual. Even if identifiers are not directly assigned to a user, but to, e.g., pieces of his/her hardware or programmes, the specific user may often be derived. Examples of identifiers are

- IDs for data sets, e.g., in relational databases where (unique) identifiers can be used to address data in a table or to join data of different tables (here e.g. MSISDN, IMSI);
- The MAC (Media Access Control) address which is a unique network card address and identifies the computer in a local area network, e.g., as an Ethernet address;
- The IP address which identifies the computer in the Internet;
- Globally unique identifiers (GUIDs), e.g.,IMSI;

Thus, those identifiers can be found in hardware, in software or in services.

For acting within an ICT (Information and Communications Technologies) system, the user has to be assigned an identifier. In many cases authentication, i.e., a verification of a claimed identity, of the user is necessary before any other action. In general there are three different methods for authentication:

- "Something you know" (e.g., a secret such as a password),
- "Something you have" (e.g., a token or a chipcard) and
- "Something you are" (biometrics).

The processes of authentication and identification are distinct. Identification, seen from the technological perspective, associates an identifier with an individual without the requirement of a claim on the part of the subject. The objective of identification is to determine which identifier refers to an individual. In contrast, authentication refers to the process of verifying the linkage between a (claimed) identifier and the individual.

From a legal point of view [46] the management of identities is not granted by legislation as such out of the following reasons:

- The category is relevant principally in technological environment, in particular in open networks (Internet).
- Identity is not regulated organically by legislation, as it would be required in order to have a legal management of identities.
- Identity from a legal perspective has a dual function. Identification of the subjects and reference point for rights and obligations.

Nonetheless legislation provides some (in most cases) constitutionally protected rights to individuals, that allow them to change some aspects of their identity, even if such changes are in conflict with the first function of the identity, which is to ensure uniqueness and identifiability of subjects. One of the topics is the right to pseudonymity, which can be defined as the right not to disclose that we don't want to disclose our identity. This is at least the case with pseudonyms which look like real names and don't reveal that they are pseudonyms.

So in order to identify a person in open networks, technically (and legally) speaking a name or an address does not need to be known any more. With the permission of the interested person one can connect the story of a relation to a reliable unique identifier (the pseudonym or the number of the signature certificate).

Technically and legally speaking, following the idea of the Directive on Electronic Signatures, which expressly declares the possibility of using pseudonyms, one can lawfully have different identities for on-line relations one establishes. Form this fact the authors of [46] deduce the need for an Identity Management System (IMS).

Another legal issue is the right to privacy. According to [46] it comprises the right not to disclose information and the obligation for data processing parties to provide technological and organisational measures to protect disclosed personal data. So the data gathering as such is not prohibited, but in order to collect personal data lawfully, there is the obligation to inform the interested person (and the data protection authority). Data minimisation is the key approach of legal systems recognising an individual right to data protection.

Note: The current problem is that data minimisation is an approach difficult to enforce: it is more difficult to select relevant data than to store everything that could be of interest. Storage capability is no more a limiting factor: huge databases and storage devices have become dramatically cheaper in the last 10 years.

The difficulty to enforce a proper gathering and handling of personal data is the reason why there is an increasing interest in Identity Management Systems. The problem of properly implementing on-line identity has been technically solved: There is the possibility to use the electronic signature for mutual identification and authentication. The problems related to the identification through a terminal or a random telecommunication link, can be solved through cryptographic tools, instead with IP addresses or other inappropriate substitutes.

Up to now pseudonymity or anonymity were the only viable options for on-line interaction. A reliable identification needed always at least some kind of direct or indirect personal contact. This is not anymore true: Many kinds of electronic signatures are available so that legally speaking there are the following options practicable:

- To be fully recognisable through qualified certificates, according to the Annex I of the Directive on Electronic Signatures 93/1999 EU;
- To be recognisable through a pseudonym displayed on the qualified certificate, according to the Annex I of the Directive on Electronic Signatures 93/1999 EU;
- To self declare one's identity;
- Not to declare one's identity.

[46] also deals with the technical aspects pertaining to the legal aspects just introduced for identities and Identity Management Systems.

As technical identities simply are numbers or strings, which can represent any object, they may identify directly or indirectly an individual, an organisation, or a machine. It is relevant from the privacy perspective that even if those identifiers do not directly represent an individual, but only a specific device, frequently there is a relation to a person so that many of these identities have to be regarded as at least potentially personal data. But as the existence and the disclosure of those IDs often goes unnoticed by the users, managing them is quite difficult: In many cases technology does not provide the functionality to influence assignment, storage and disclosure of those IDs. A possibility to regain control over these IDs is offered by some anonymising services which help the users in substituting or deleting those identifiers. In general it is not possible to successfully manage one's partial identities without knowing when and where they may be involuntarily disclosed. This is not only the case with data trails in digital networks, but also capturing

biometrics, e.g., by video surveillance, is often possible without knowledge and consent of the individual.103 Whereas the user can blur identifying data by anonymising services, there is no equivalent solution for preventing others to capture publicly noticeable biometrics such as the face, the shape of the body or the way of walking. Identity Management Systems as described in this study are acting as gateways and guardians for users in digital networks, but cannot prevent undesired data collection outside the network.

5.3.1.2.3.2 Identity Management in OMA

OMA developed an Identity management enabler in whose requirement document [86] it evaluates the benefits of a single Identity Management enabler for all OMA enablers to be:

- Management and use of Identity or personal information is easier for all stakeholders: End Users, mobile operators, enterprises and Service Providers;
- End Users do not have the burden of having to understand different service-specific Identity solutions;
- The same Identities and personal information can be utilised by multiple services;
- Privacy protection can be enabled more easily using a common Identity Management enabler;
- The OMA will not be seen to publish specifications with disparate, conflicting Identity Management solutions;
- Identity needs are the same (or very similar) for all enablers and so, by creating a single Identity Management enabler, duplication of work is kept to a minimum;
- New enablers with Identity requirements will be able to benefit from the existing Identity Management enabler;
- Greater interoperability between enablers;
- Improved time to market for those enablers that use the Identity Management enabler.

In [86] OMA also identified additional benefits if existing, standardised Authentication / Authorisation methods could be re-used in an Identity Management enabler. One such example is mobile operator subscription-based Identity:

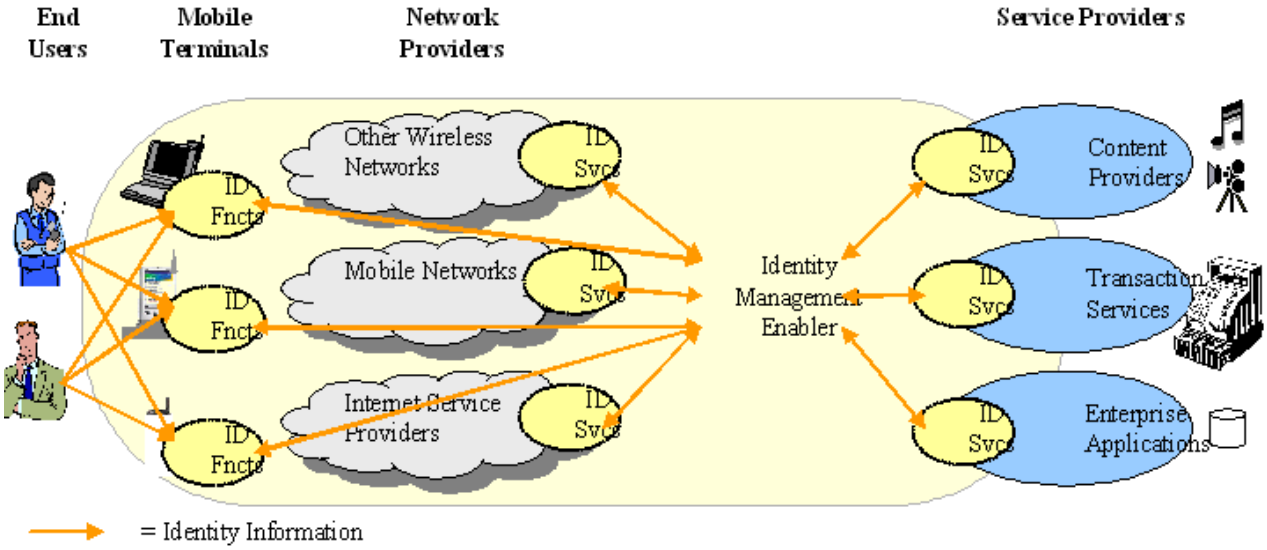
- Mobile operators already have an excellent trust relationship with millions of End Users due to their high level of security;
- Mobile operators can offer services of their own, or third party services, with improved Authentication and privacy protection by using IDP and Identity Broker models;
- Mobile operators can offer content Service Providers simple, event-based billing services suitable for low-value transactions.

OMA includes in its scope the following types of Identities:

- End User Identity: relating to the provisioning of and access to End User Identity information and related Attributes in
    - the mobile operator,
    - Service Provider,
    - enterprise infrastructures and in
    - the Device.

  This includes the management (e.g. conflict resolution) of several simultaneous Identities (for one End User) that enable multiple End User profiles, such as employee and a private customer profiles. Delegation and sharing of authority is also included in scope in order to enable the role of an intermediary Agent (e.g. for some enterprise situations).
- Provider Identity: for Authentication and to support delegation of authority.
- Device Identity: to enable topics such as digital rights management, for example.

- Application / Service Identity: to identify enterprise applications, for example, or enable the use of Identity Containers.



The following figure describes the Identity Management ecosystem as OMA sees it [86].

Figure 5.3.1.2.2.2.1: OMA's vision of an Identity Management eco system [86]

The following paragraphs describe a set of simplified Identity Management roles that the different actors in the ecosystem can implement and the interactions that would happen between them.

OMA defines the following mechanisms by which the actors in the IdM ecosystem can interact to exchange Identity information:

- The ability to discover Identity information;
- How Identity information can be transferred from one Entity to another;
- The ability to control the
  - availability,
  - visibility, and
  - use of Identity information.

The following roles - defined by OMA - can be used and implemented by the different actors of the Identity Management ecosystem:

- Principal Agent: A Principal is an Entity that has an Identity, and owns all Identity information about itself. Examples:
  - human beings (End Users),
  - a Group of End Users,
  - a corporation,
  - service enablers / applications,
  - system Entities and
  - other legal Entities.

A Principal Agent is an IdM role that represents 'real world domain' of a mobile operator or enterprise (can be thought of as a delegated source of Identity information i.e. delegated by the 'real world domain' Principal).

- Identity-based Service Consumer: IdM role that, in order to perform its functions, requires some Identity information about a Principal.

  Example: Provider that implements a weather forecast service. The Provider might wish to request location information (from an Identity-based Service Provider) about a certain End User in order to provide a local weather report to that End User.

- Identity-based Service Provider: IdM role that provides Identity information or Identity services for / about a Principal. The role of an Identity-based Service Provider includes acting upon some resource in order to

  - either retrieve information about an Identity,
  - update information about an Identity, or
  - perform some action for the benefit of some Identity.

  Attribute Provider: a special type of Identity-based Service Provider, whose function is to provide Identity Attributes about a specified Principal. Therefore an Attribute Provider would create, read, update, or delete Attributes of a Principal.

- Identity Provider (IDP): IdM role that offers key, core Identity functions that are required in order for other Identity services to be possible.

- Discovery Service Provider: IdM role that knows what Attributes are available for a particular Principal and how to gain access to those Attributes. Note that a Discovery Service Provider would not actually know the value of a particular Attribute, but just the Address of an appropriate Identity-based Service Provider.

In addition OMA describes the relationship between the Identity Management enabler and the OMA Policy enforcement infrastructure.

According to [86] the roles of the IdM ecosystem may need to make Authorisation decisions and evaluate other Policies (i.e. they may have to perform functions that belong to a Policy evaluation and enforcement enabler). If necessary, policy enforcement will be handled via delegation of certain PEEM functions to those other enablers that specialise in the particular functions.

Finally OMA sees the following use cases:

- Single Sign On (SSO) and Authentication Contexts:

  - Single Sign On improves the End User experience by reducing the number of username / password combinations that the End User must remember, and by reducing the number of keystrokes required on the Device.
  - Single Sign On can also improve security because it is more likely that an Identity Provider would use a more secure, 2 or 3-Factor Authentication solution than a Service Provider would (e.g. a SIM Smart Card in combination with an End User PIN)

- Federation, Single Log Out, and De-Federation: This use case describes some of the background processes that enable SSO. Specifically, this use case discusses:

  - Federation of an End User's Account at an IDP with her Account at an SP;
  - De-Federation of an existing Federation;
  - Single Log Out (SLO) of an End User.

- Delegation of Authority to Federate Identities, Bulk Federations and De-Federations: There are many cases where an End User may wish to delegate authority to federate her Identity Provider Account with her (new or existing) Accounts at other Service Providers to the Identity Provider itself, so that the IDP may federate her Accounts on her behalf. Using this delegated authority, the IDP can federate the End User's IDP Account with (new or existing) End User Accounts at SPs without the End User having to be logged in (i.e. authenticated) at the time.

- Seamless Attribute Transfer and Usage Directives:
    - Seamless Attribute Transfer: Typically, an End User has to enter her personal profile information (her Identity *Attributes*) many times when using on-line services. By offering seamless Attribute Transfer Identity Management can relieve the End User of this tiresome task.
    - Including *Usage Directives* when requesting End User Attributes from *Attribute Providers*: By Usage Directives OMA means a set of directives regarding how a particular Attribute would be used by the Service Provider once the Attribute has been released to it. By Attribute Provider OMA means a Service Provider whose service is to store and manage End Users' Attributes on their behalf.
- Anonymous Attribute Transfer: There are many scenarios where a Service Provider may wish to access certain Attributes associated with an End User without actually knowing the Identity of the End User.
- Transactions and Event Tokens: End User purchases goods and services using mobile Device enabled payment processes, where the merchant selling the goods and / or services could be a retail establishment or an online vendor.
- Authentication Domains, Identity Brokers and Circles of Trust: In a deployment scenario where several Identity Providers and Service Providers exist, it is highly likely that each Identity Provider will have business agreements with several Service Providers. Furthermore, a Service Provider may have to enter into a business agreement with many Identity Providers in order to cover a large customer base, which is not desirable from a Service Provider's point of view. In order to address these points the notion of Authentication Domains, Identity Brokers and Circles of Trust are introduced.
    - An Authentication Domain consists of one Identity Provider and all the Service Providers (and End Users) that have the necessary technical and business arrangements in place with the Identity Provider in order to be able to offer (or use) SSO services.
    - IDP1 and IDP2 might create a business agreement that allows them to act as *Identity Brokers* for each other. There still exist two Authentication Domains, but IDP1 and IDP2 can act as Identity Brokers in order to introduce Service Providers in one Authentication Domain to an Identity Provider (and hence End Users) in another Authentication Domain.
    - Circle of Trust means that there is a potential trusted link between every End User and every Service Provider in the Circle of Trust. A Circle of Trust could, itself, be a part of a bigger Circle of Trust, to the extent that if every IDP acts as an Identity Broker for at least one or two other IDPs then it would be easily possible to create an almost global Circle of Trust.
- Service Provider Alliances: There are many cases where several Service Providers decide to work together to form an Alliance so that, for certain functions, they appear as a single Entity to the End User. In other words, the different Entities or companies in the Alliance are no longer relevant to the End User, but the End User is merely interested in the services that the Alliance has to offer as a collective unit.

5.3.1.2.3.3 Identity Management using a common datamodel and the CPSF

The existence of one end-user model stored in a logically centralized common profile storage framework (for details see section 6) has soms business related aspects:

- The centralization of user administration tasks allows to
    - Reduce admin costs and
    - Improve accuracy and security of data store
- New applications can leverage the existing infrastructure which leads to a reduction of deployment time for new applications
- Improvement of end-user experience:
    - Quick access to applications for new users
    - Allows to modify attributes or preferences at one location only
    - Allows customized application experience (applications understand the user preferences and roles)

- Improvement of application security:
    - Password and security credentials managed centrally
    - Usability greatly improved

In addition some principles of fair information practices can be observed and proved more easily, when dealing with the identity of an end-user stured ina logically centralized CPSF within a common data model.

- Openess:
    - Means for establishing the existence and nature of personal data
    - Main purpose of the use of the data
- Collection Limitation:
    - Limits to collection of personal data
    - Acquisition by lawful and fair means (evtl. with knowledge and/or consent of data subject)
- Purpose specification:
    - Purpose, for which the data are collected, must be known latest at the moment of the beginn of the data collection
    - Use of the data shall be limited to the fullfillment of those purposes
- Limitation of data usage:
    - Non-disclosure of personal data
    - Use limited to purpose negotiated (subject to mutually agreed change requests)

5.3.1.4 The Relation between an End-User and a Subscriber

In clause 5.3.1.2 the relation of the end-user to his various key attributes has been discussed. This clause highlights the relationship between a contract holder and an end-user in more detail.

Figure 5.3.1.4.1 shows the general situation: An end-user can have n cards with the same or different services assigned. The end-user may also be a contract holder (subscriber), but does not need to be so. A contract holder can be assigned to one or more cards (for which he is billed) and to one or more end-users.

The following figure gives a simple example:

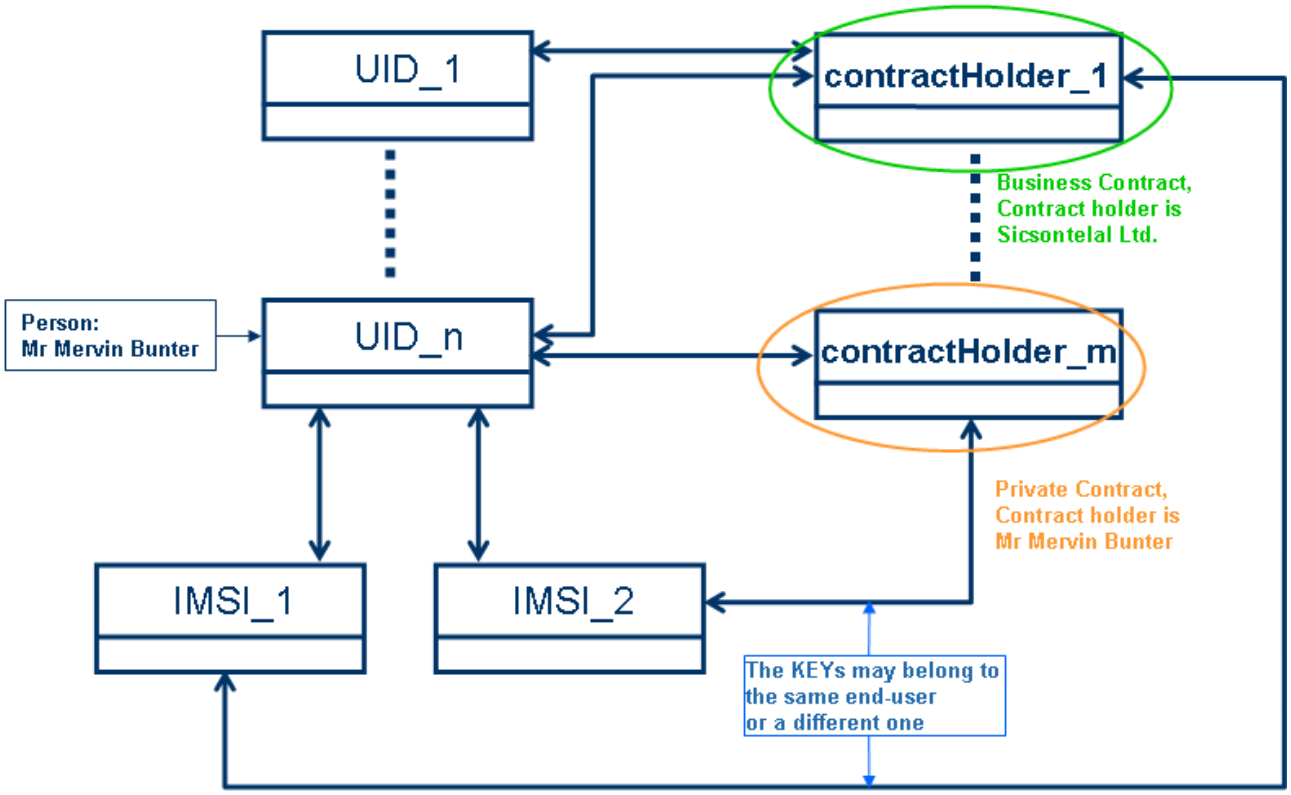


Figure 5.3.1.4.1: Specific example of the relationship between an end-user and a contract holder

Contract holder 1 is a company, which has n employees, with one mobile phone each (paid for by the company). Employee n (UID_n) is also a contract holder (contract holder m), because in addition to the company phone he has a pre-paid mobile for his private use. Thus UID_n is assigned two different keys (IMSI_1, IMSI_2).

5.3.2 Semantic Identity of Data Entities

One idea of a common data model is to avoid redundant definition and storage of data model entities. So all data, which are used by more than one network function in the same way ("semantic identity") shall only be defined once.

This requirement has to be analysed under the following conditions:

- Different applications might need differing forms of representation of the semantically identical data entities in question.

  The representation of a numerical value might be a number (Roman or Arabic, which already creates a problem) or a string (“fifteen”). In addition, if this value is needed in string form, it might be needed in English by one application and in French by another application.

  In case of object oriented databases the objects might contain the same attributes, but might be called differently (e.g. different standardization bodies defining the same entities).

- Different applications might need the semantically identical data differently organized out of functional reasons

  A set of attributes might be put into n object classes for one application, the reason being that for a fast read there should not be too many data to be analyzed. For another application it might be essential to read as many data as possible with one read, so the set of attributes is put into one object class only.

- Different applications might need the semantically identical data differently organized out of backwards compatibility reasons

Out of historical reasons, applications using the same data entities in a directory type of organization (e.g. X.500) might still have different organizations of their tree.

- In general, an application should not need to know of the existence of another application

  This bullet has implications both for the physical architecture of the data storage (certain properties of distributed systems have to be met) and on the way, in which the data model itself has to be designed. Here only the last point is of interest and can be summarized by the requirement that the addition of a new network function or management application onto the central profile store should not affect the data access layer of the network functions or management applications already working with the central profile store.

  At this point the notion "semantically identical" comes to its full importance: If two CPS applications have write access to the same data entity, it must be clear that

  - the same understanding about the consequences of a data manipulation must exist within the two applications, that
  - the necessity to change the data entity must be experienced by both applications in the same situations and that
  - there needs to be a mechanism via which all interested applications of the CPS can be informed of the change of the data entity (for a suggestion see the subsection about triggers).

- Only the applications, which need access to a data entity, should be granted this access.

  Once the common data model would – theoretically – be accessible to all database users, one has to take care that only authenticated and authorized users manipulate certain data entities.

5.3.3 Adapting Entities

In order to be able to comply with the bullets above, adapting entities shall be defined, which

- Provide a certain view of the complete or data model or a part of it,
- Are able to provide different value representations for the same value,
- Are able to provide the proper access rights,
- Hide the fact that they ARE adapting entities and
- Are able to inform subscribed applications of a value change of a data entity.

5.3.4 Content of Post Update Triggers

In any of the cases described in 4.3.2, in which two or more network functions use the same data entity as described in 4.3.3, it must be possible for all of these network functions to be informed about any change happening to the data entity in question.

As soon as the creation, deletion or modification of a data model item common to two or more network functions has been carried out by the end-user database, a triggering mechanism should be able to inform any interested network function about it.

Content: Name of the data entity, old value, new value

5.3.5 Adaptation Layer

In the relational world, views as defined in SQL cover part of the requirements, in the object oriented world implementation of the functionality required for adapting entities would most probably be proprietary.

The capabilities, which need to be implemented into the CPS so that adapting entities can be defined, have been summarized under the notion Adaptation Layer Functions (ALF).

The data model part containing the adapting entities is called Adaptation Layer.

Note: The adaptation Layer is not a layer in the sense of X.200.

5.3.6 Different Levels of Data Consolidation

This clause discusses two completely different approaches to the design of a complete data model of an end-user:

- Approach 1: The complete model is exposed to all network functions and only in the cases, where there are semantically identical data entities handled by different network functions, Adaptation Layer Functionality is used to guarantee the integrity of these entities for all involved network functions.
- Approach 2: The complete model is hidden from the network functions (perhaps, because it reflects the business processes of a provider) and Adaptation Layer Functionality has to be provided for a high percentage of the entities of the data model in order to satisfy the network functions.
- Approach 3: Mixed scenarios, which allow to expose real data to network functions or enterprise applications, if out of some reason this seems desirable.

5.3.6.1 Adaptation Layer for partial Data Consolidation (Approach 1)

The complete structure of the end-user data model is, in principle, exposed to any network function. A specific network function is

- either able to ignore data, which are not relevant for its function,
- or the data base requests are tailored so that only data relevant for this network function are manipulated.

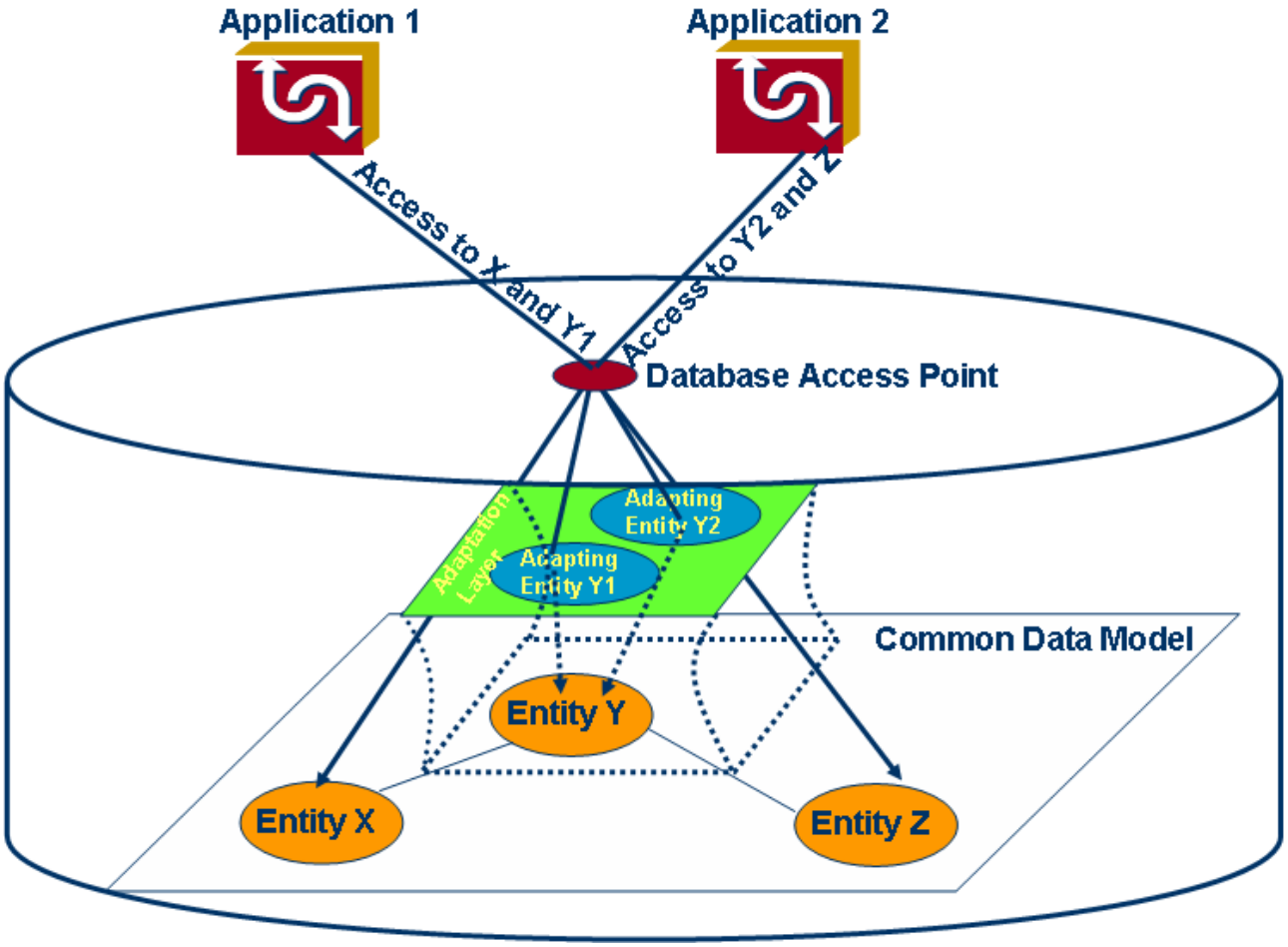


Figure 5.3.2.1.1: Overview over a common object model in case of a partial data consolidation

In case two network functions share a common data entity (Entity Y in Figure 5.3.2.1.1) then it may be necessary to define Adapting Entities Y1 and Y2 under the conditions described in section 4.3.3.

5.3.6.2 Adaptation Layer for full data consolidation (Approach 2)

The structure of the common data model is completely hidden from the network functions for reasons discussed in more detail in section 6.

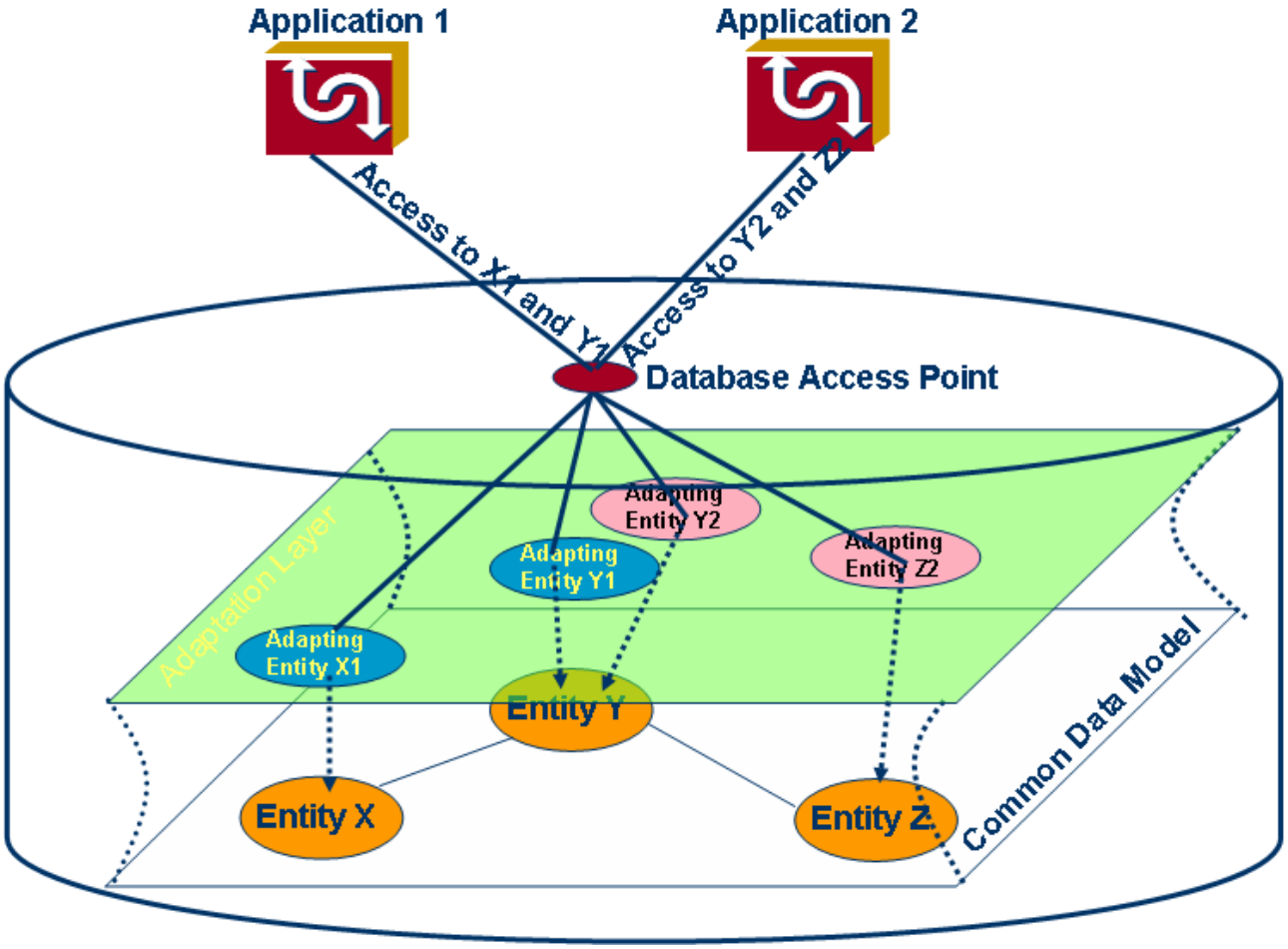


Figure 5.3.2.2.1: Overview over a common object model with a fat Adaptation Layer

5.3.6.3 Mixed Scenarios (Approach 3)

Depending on the criteria for the definition of the word "common" in common data model, the common part might, semantically seen, contain only a subset of data needed by one of the network functions.

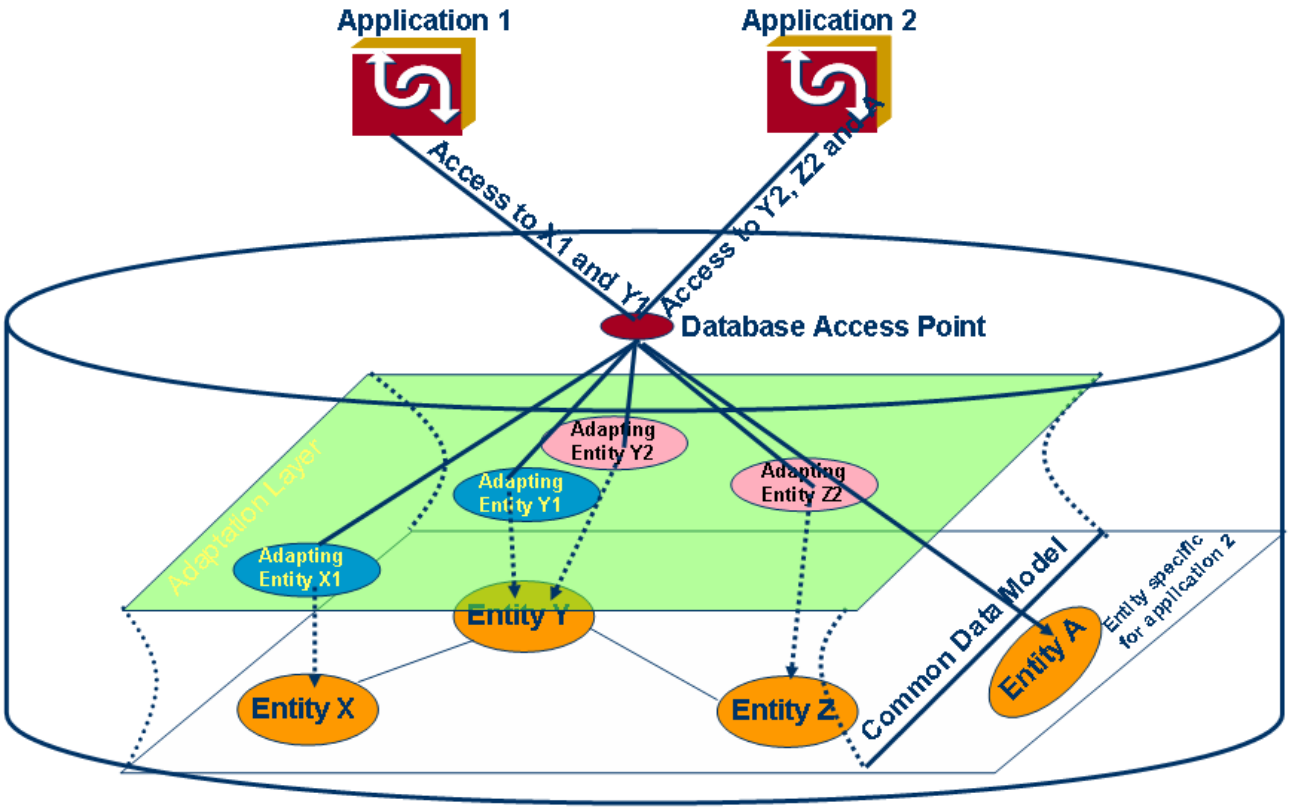


Figure 5.3.2.3.1: Overview over a mixed architecture

6 Basic Structure of the Common Profile Storage Framework (CPSF)

Clause 6.1 just gives the general properties such a storage framework should have independent of any variant of implementation.

Clause 6.2 describes possible ways to realize a centralized data base.

Clause 6.3 describes ways in which a CPSF could be realized.

Clause 6.4 is devoted to the question, what kind of tooling would be needed to make the CPSF work in reality.

6.1 Logical View

This clause deals with the functions the CPSF has to support. Figure 6.1.1 depicts a typical three-tier architecture consisting of a:

- Database subsystem, which is concerned with data management and resource management; and
- Application subsystem containing network functions (e.g. HSS, HLR, etc.) as well as enterprise applications (e.g. CRM, Marketing applications, etc.); and
- A client subsystem providing e.g. a GUI.

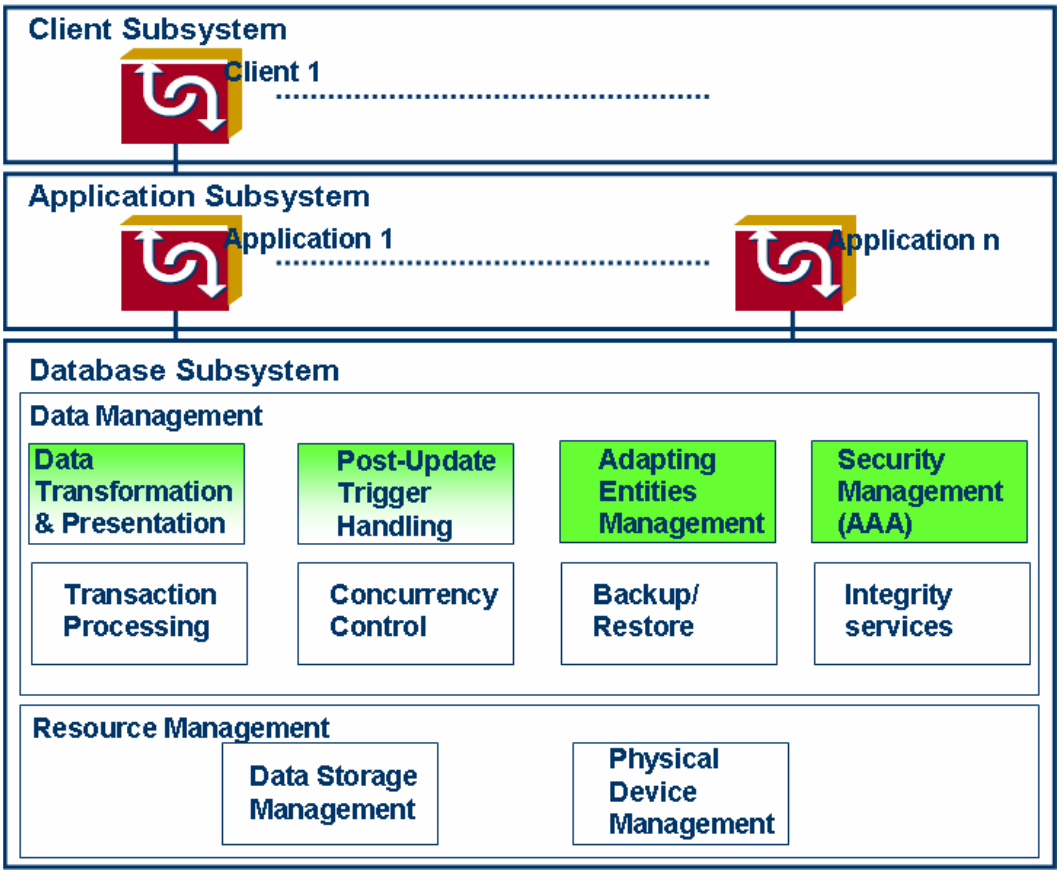


Figure 6.1.1: Logical view of the Common Profile Storage Framework as a 3-tier architecture

6.1.1 Actual End-User Data Storage Framework

This clause deals with the part of the framework, which takes care of the real data handling.

Resource Management:

- *Data Storage Management:* This function hides the storage complexity from the application orchestrating the execution of queries, including I/O generation and caching.
- *Physical Device Management:* This function has the task of ensuring optimal query execution in database management systems using a variety of metrics, cost estimators, and run-time statistics to devise a query plan with the lowest cost.

Data Management:

- *Data transformation and presentation:* This function has two properties:
  - Maintenance of data independence.
  - Removal of the distinction between logical and physical data.
- *Concurrency Control:* This function prevents clashes between user operations:
  - Allows high database performance by admitting concurrent data accesses from multiple network functions and enterprise applications at the same time.
  - Ensures that interleaved action coming from multiple network functions and enterprise applications do not lead to inconsistencies in the database.
  - Ensures that each network function and enterprise application is unaware of all other concurrent database users.
- *Backup and Restore:* This function block provides backup and restore mechanisms and strategies.
- *Integrity Services:* This function enforces referential integrity rules.
- *Transaction Processing:* This function enforces the ACID (Atomicity, Consistency, Isolation, Durability) properties on a set of database operations, which have been collected into one transaction:
  - Atomicity: If a set of database operation has been collected into one transaction this transaction will only be committed, if all operations have been carried out successfully.
  - Consistency: At the Begin and at the Commit of a transaction (or after the roll back) the data within the database have to be consistent.
  - Isolation:
    - network functions and enterprise applications seemingly run one at a time; and
    - are protected by either locking mechanisms or database versioning.
  - Durability: A committed transaction has to survive failures:
    - Put the logs of committed transactions into a durable place (e.g. duplicated disk);
    - Redo transactions from the log in case of:
      - System failure: lost in-memory updates.
      - Media failure (e.g. lost disk).
    - Undo non-committed transactions.
- *Post Update Trigger Handling:* This function allows:
  - The subscription to a post update trigger.

- The sending of post update triggers to the subscribed users of the CPSF.

- *Adapting Entities Management:* This function decouples the network functions and enterprise applications from the database in two ways:
  - Logical decoupling: Provides all functions using the database with protection from changes in the logical structure of the data (i.e. provides tailored views for network functions and enterprise applications, which use the database).
  - Physical decoupling: Provides all functions using the database with protection from changes in the physical structure of the data.
- *Security Management:* This function provides:
  - Authentication and authorization.
  - Object access control.
  - Accountability via auditing.
- Additional functions not shown in the figure:
  - Database access languages and application programming interfaces.
  - Database communications interfaces.

6.1.2 Adaptation Layer Functionality

This clause deals with the basic functionality, which a CPSF has to provide in order to make data consolidation work. The sum of properties realizing this functionality will be called Adaptation Layer for the rest of the present document. The data model building blocks of the Adaptation Layer were already introduced in clauses 5.3.2 and 5.3.4.

NOTE: The notion "Layer" is only logical. There are no well defined interfaces on the north and south. Instead the "Adaptation Layer" consists of a list of functions, which allow a complete decoupling of the Application Subsystem whenever this is necessary.

6.1.2.1 Adapting Entities

In accordance with the scenarios introduced in clause 5 adapting entities shall be able to cover the following situations:

- More than one application uses the same data entity, each needing a different representation.

EXAMPLE: Language sensitive representation of values (e.g. red, rouge, rot), different representation of values (1, one, I).

- The real data model is used to support the business processes of a provider and the application needs a specific "view" on its data.
  One advantage of a CPSF containing a common model is the fact that it can contain all relevant business data for an end user as has been shown in clause 5. Thus it is capable of supporting both network functions and enterprise applications alike. There will obviously be many ways to organize the data as long as the principal structures described in clause 5.1 for the network functions and in clause 5.3 for identification of an end user can be retrieved. In which ever way a provider intends to structure his data (best suited to his business), he will have to provide specific adapting entities for some or all of his functions using the CPSF.

- Support of legacy applications: Here two situations need to be distinguished:
  - Mandatory: The legacy application uses the same standardized data modelling language and database access protocol, but its legacy data model does not fit into the general data modelling strategy. Then respective "views" have to be provided for the application.
  - Optional: The legacy application uses a different standardized data modelling language and database access protocol, which cannot be adapted to the current conditions. Then an according interface and an automatic conversion into the current model entities allows the legacy application to remain mainly unchanged.

6.1.2.2 Access Control

Control of access to information:

- prevention of unauthorized detection;
- disclosure; or
- modification of that information.

At minimum the Basic Access Control Model [44] from ITU-T has to be supported, whose decisions entail actions on the following entities:

- the entity of the data model being accessed - protected item;
  a protected item is an element of the data model to which access can be separately controlled
  Basic Access Control also provides the means to define collections of related items (e.g. attributes in an entry, all attribute values of a given attribute) in order to specify a common protection for them.
- the user requesting the operation - requestor;
- a particular right necessary to complete part of the operation - permission;
- one or more operational attributes that collectively contain the security policy governing access to that item - ACIs (Access Control Items).

6.1.2.3 Post-Update Trigger Mechanism

In clause 5 the possibility of semantically identical attributes for different network functions and enterprise application end-user models has been discussed. In the case that one common end-user model is used, this attribute will then be visible and accessible to all concerned functions and applications.

6.1.2.4 Preserving the Real-Time Capability of the CPSF

In clause 5 the proponents of the Application Layer were introduced. Especially the applications listed under the network supporting services have stringent real-time constraints. Thus any Adaptation Layer has to guarantee their support.

6.2 Physical View

In this clause different possibilities of a physical realization of the CPSF as a database are analyzed.

Clause 6.2.1 is a special case of clause 6.2.2. It just describes what a CPSF should be able to do in case it could be realized via one NE only. The clause is only very brief, as there is an abundant amount of literature describing the basics of relational and object oriented databases.

Clause 6.2.2 treats the case, in which the database is distributed. Obviously, some of the requirements discussed in clauses 6.1.1 and 6.1.2 are not easy to realize in a distributed database, so some of its key features are reviewed.

6.2.1 Centralized Data Base

In a centralized database data are stored at one physical location (database server) only, which might e.g. be a mainframe.

The network element should

- Provide the properties described in clauses 6.1.1 and 6.1.2;
- Be highly available; and
- Allow geographical redundancy.

The last bullet actually needs some discussion. From a theoretical point of view the database would then already be distributed and is treated as the case of complete replicas (see clause 6.2.2).

6.2.2 Distributed Data Base

Again the network element should

- Provide the properties described in clauses 6.1.1 and 6.1.2;
- Be highly available; and
- Allow geographical redundancy.

As a common denominator this TR will regard a distributed database as one where data are stored at several physically different locations.

There are two different types of distributed databases:

- Homogeneous databases: Every site runs the same type of DBMS.
- Heterogeneous databases: Different sites run different DBMS (even both RDBMS and ODBMS at the same time).

Distributed databases can have the following architectures:

- Client-Servers Architecture:
  - The client sends a query to each database server in the system.
  - The client caches and accumulates all answers.
- Collaborating Server Architecture:
  - The client sends the query to the nearest server.
  - The server either executes the query locally or sends it on to other servers as required.
  - The server sends the response to the client.

Distributed data can be stored as follows:

- In fragments at each site:
  - The data has to be split up.
  - Each site stores one or more fragments. This can have some advantages:
    - One can put the data near the function using it.
    - The network traffic can be reduced.
    - Response times can be optimized.
    - Availability of the data can be optimized .
- In complete replicas at each site:
  - Each site stores a replica of the complete data. This can yield the following advantages:
    - Improvement of data availability.
    - Allows disconnected operation.
    - Allows load distribution.
    - Read operations are much cheaper.

- Replication can be done:
  - Synchronously: All data, which have been changed, must be propagated before the transaction commits. Thus during the time, the changes are made and propagated, the transaction gas to obtain a lock on all modified copies.
  - Asynchronously: Updates are sent periodically, which has two consequences:
    - Updates can go out of sync.
    - Functions using the database need to be aware of the fact that updates can go out of sync.
  - Types of replication:
    - Primary site replication:
      - One copy is designated as a master.
      - All other copies are published to other, "secondary", sites.
    - Peer-To-Peer replication:
      - More than one copy can be master.
      - Conflicting changes must be resolved.

- A mixture of fragments and replicas:
  - Each site stores a replica and/or one or more fragments of the complete data.

6.3 Analysis of alternative solutions

In this clause different possibilities of realization of the CPSF within the network are analyzed. The difference in the approaches concerns the questions:

- whether one employs a separate, eventually distributed database for all end-user data, which is logically seen as one network element by all network functions and enterprise applications; or
- whether the CPSF is logically seen as one network element.

6.3.1 Logically Centralized Approach

This clause deals with possible architectures of the CPSF, which can, logically, be summarized as shown in figure 6.3.1.1.

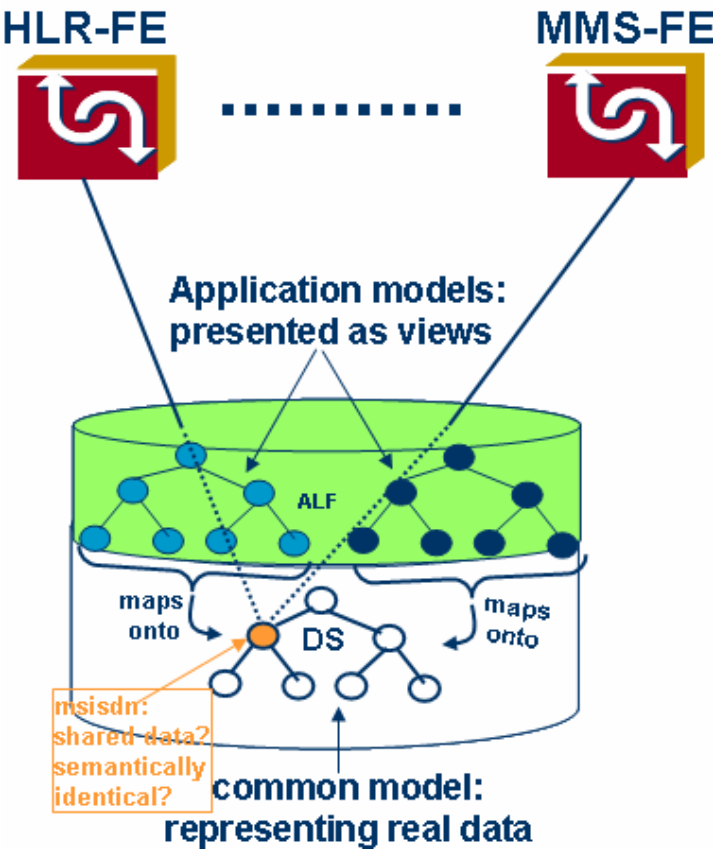


Figure 6.3.1.1: Logical view of the Centralized Approach to the Common Profile Storage Framework

Figure 6.3.1.1 shows that all applications (i.e. network functions and enterprise applications) of the CPSF access one logical network element, which provides them their specific data structure.

In case the scenario of clause 6.2.1 applies, figure 6.3.1.1 can be an example of a physical realization. In case the physical realization of a CPSF is in the form of a distributed system (one of the variants described in clause 6.2.2) figure 6.3.1.2 represents a valid example.

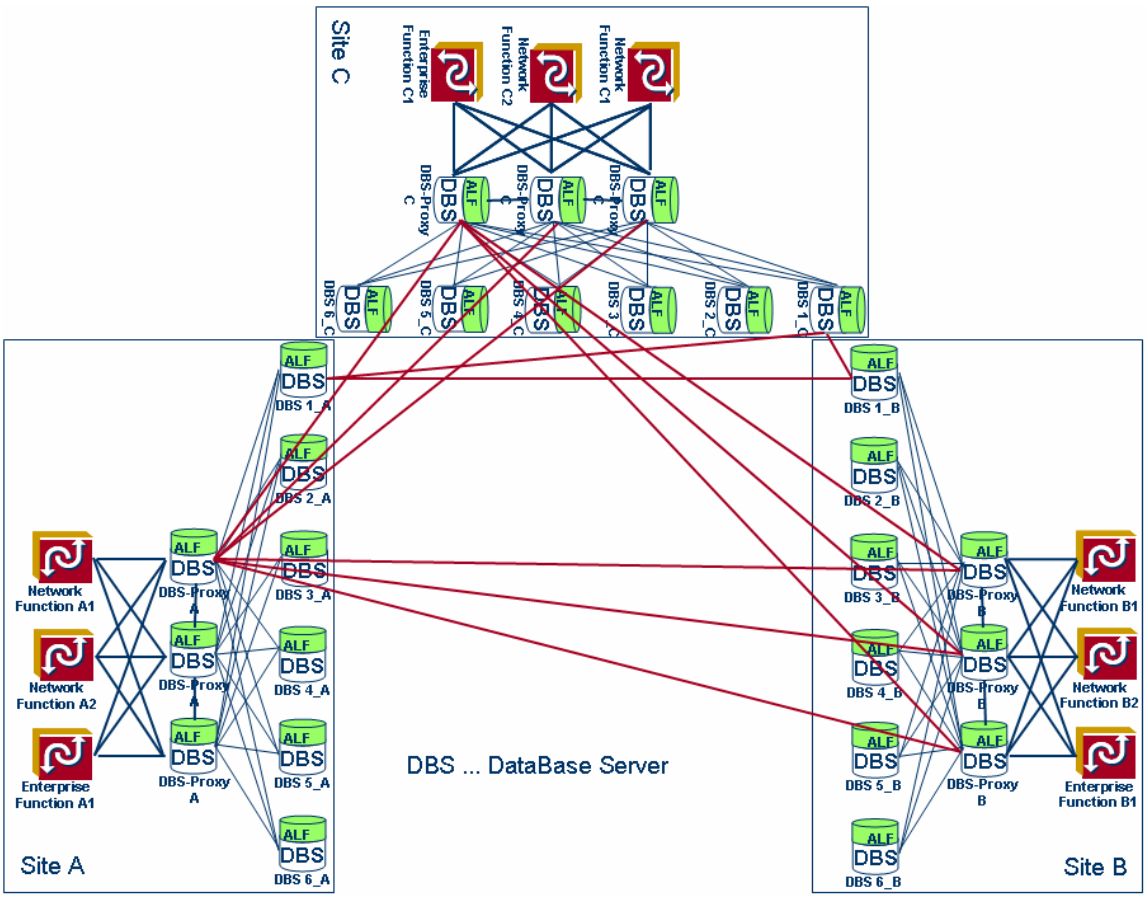


Figure 6.3.1.2: Physical view of the Centralized Approach to the Common Profile Storage Framework Using a Distributed Database

Figure 6.3.1.2 gives an example of a possible CPSF deployment using a distributed database.

Remarks:

- Sites A, B and C are geographically redundant.
- The DBS-Proxies are one possibility to provide uniform access for the network/enterprise functions. In the example in figure 6.3.1.2 there are nine such proxies, three per site for load balancing and three geographically redundant copies for high availability.
- The database servers contain the actual end-user data:
  - In the example there are 18 servers, six at each site. These six each contain a fragment of the complete set of data and each site has a complete replica for reasons of high availability.
  - The example also shows the possibility of connecting three specific DBSs (1_A, 1_B, 1_C), which contain identical replicas of a data fragment (either by peer to peer or by primary site replication).
- The full mesh shown between the network / enterprise functions and the DBS-Proxies, as well as between the DBS-Proxies and the database servers is only shown in a logical sense. These connections will most probably be switched.

6.3.2 Logically Distributed Approach

In clause 6.3.1 the fact that the database is distributed is hidden from all network functions and management applications. This clause deals with a distributed system, in which knowledge about its components may be necessary.

An example of a logically distributed approach is 3GPP's Generic User Profile (GUP), which is described in more detail in clause 5.1.4.

A data consumer (network function or enterprise application) can request a copy of a GUP component, which is the designated master instance of the component and which - according to 3GPP - is held by the data supplier.

This copy may be of one of two types:

- Working copy: the GUP component instance corresponds to a copy (or snapshot) of the master instance at a given point in time. The working copy is held within the data consumer's local store. Future changes to the master instance (e.g. update, deletion, etc.) are NOT propagated to the working copy. The working copy remains unaffected by changes of the master instance of the GUP component.

- Synchronized copy: the GUP component instance is kept synchronized with the master instance and is held within the data consumer's local store.

If a GUP component is no longer applicable for a given user, the master instance for this GUP component is deleted and all data stores holding synchronized copies are notified about this deletion.

If the access rights of the component are changed, a proper notification is sent to the owner of the synchronized copy.

6.4 Tooling

The intention of clause 6.4 is to point out the necessity that a fairly comprehensive tooling landscape is necessary to allow a network/service provider to:

- be capable of defining a common data model and its adaptation layer (i.e. adapt the data to the specific needs of this operator);

- remain vendor independent in choosing both the CPSF and the network functions / management applications;

- be able to manipulate his data structures as well as the content in a running system (the addition or modification of network functions / management applications should not affect other functions already running as users of the CPSF).

Areas in which the CPSF needs tooling are:

- data migration support;

- meta data manipulation and repository;

- a tool management system; and

- a report/documentation system.

7 Gap-Analysis

This section lists gaps between the current 3GPP concepts and concepts introduced in this TR.

7.1 Concept of the End-User

According to [1] the following distinction between a subscriber and a user is made:

Subscriber: A Subscriber is an entity (associated with one or more users) that is engaged in a Subscription with a service provider. The subscriber is allowed to subscribe and unsubscribe services, to register a user or a list of users authorised to enjoy these services, and also to set the limits relative to the use that associated users make of these services.

User: An entity, not part of the 3GPP System , which uses 3GPP System services. Example: a person using a 3GPP System mobile station as a portable telephone

While in the past these concepts/definitions have been sufficient to describe the relevant roles in 3GPP the new concept of an "End-User", as described in section 5.3.1, needs to be introduced in 3GPP.

To introduce the concept of an end-user in 3GPP the following gaps would need to be closed:

- The definition of an "End-User" in [1] and its relation to the terms "user" and "subscriber". An "end-user" exists independently of a particular service at first, but may be granted access to different services by a subscriber.
- An (optional) requirement to be able to uniquely identify an End-User needs to be specified.
- The definition of a UID identifying an End-User is missing in [2].
- A decription of the UID and its relations to other identities (IMSI, IMPI, IMPU, …) as well as relevant numbers (e.g. MSISDN) is missing in [3].

7.2 Concept of a Model Entity for a Contract Holder/Subscriber

In order to introduce a contractHolder as described in section 5.3.1, the following gaps would have to be closed:

- The definition of a subscriber as given in [1], or – equivalently of a contractHolder as described in 5.3.1 of this TR – is missing in [2].
- The relations to subscription information (IMSI, subscriptionId for HSS, …) are missing

7.3 Concept of a Contract

In order to understand the type of contract a contract holder is representing, relevant contract information has to be present:

- Pointers to subscription information are missing in [2]
- Contract Information (Contract identification, Contract Version, …) are missing in [2]
- Pointers to the services to be delivered according to the contract are missing in [2]
- Pointers to policies, where they exist are missing in [2]

7.4 Introduction of a network function “Common Profile Store (CPS)”

In order to introduce a Common Profile Storage Framework according to section 6 of the TR the following gaps have to be closed:

- The definition of such a logical network element in TS 23.002 [13] and/or TS 23.228 [22] is missing
- The definition of additional interfaces between the new NE and the network elements that depend on end-user-related data is missing
- The description of impacts on the existing 3GPP NEs and network architecture is missing

8 Conclusions

This section lists proposed standardization actions based on the gaps between the current 3GPP concepts and concepts introduced in this TR in section 7.

8.1 Introduce the Concept of an End-User

The scope of the end-user concept should be

- that it is supported by all vendors providing a common end-user model to providers and
- It exists independent of a particular service, but may assume the "user" role in services under a particular subscription. An end-user may also act as a "subscriber" in a particular subscription.
- that it supports data federation among different providers.

The introduction of the concept of an End-User inside 3GPP as described in section 5.3.1should be started in SA1:

- Analysis of the general concepts.
- Analysis of potential requirements regarding an End-User.
- Description of the relationships between subscriber, user and end-user.

8.2 Introduce the Concept of a Contract

The scope of the concept of a contract should be

- that it is supported by all vendors providing a common contract model to providers and
- that it supports data federation among different providers.

In order to understand the type of contract a contract holder is representing, analysis should be started in SA1:

- Analyse, which information needs to come into a common object model
- Analyse, whether TMF's concepts [95] – [98] could be used

8.3 Introduce a network function "Common Profile Store (CPS)"

The scope of the concept of a CPS should be

- That it provides a logically centralized, physically possibly distributed, service-independent storage of data related to end-users.
- That it provides network elements that implement services, as well as enterprise applications concerned with end-user data, with access to the relevant parts of that end-user-related data.
- that it is supported by all vendors providing a common contract model to providers and
- that it supports data federation among different providers.

In order to introduce a Common Profile Storage Framework according to section 6 of the TR analysis should be started in SA2:

- The definition of such a logical network element
- The definition of additional interfaces between the CPSF NE and the network functions

- The description of impacts on the existing 3GPP NEs and network architecture

Annex A:
Example for the realization of an end-user database according to the Common Profile Storage Framework

This annex shows the realization of an end-user database according to clauses 5 and 6 of this TR using ITU-T's Recommendation X.500 [89] as a basis.

Clause A.1 will introduce the rough structure of two network applications, how they might form a common model and some notions about the requirements for an adaptation layer. The example intentionally chooses a hypothetical deployment of a scenario, which has a mixture of 3GPP-R4 and 3GPP-R6 components, in order to demonstrate the capability to be backwards compatible.

Clause A.2 will introduce the corresponding network architecture showing one possibility to realize a distributed central database using the X.500 network structure and LDAP v3 as access protocol [88].

A.1 The Model Structure

The basic scenario selected for the model example is the existence of an HLR according to 3GPP-R4 and an HSS according to 3GPP-R6, which contains the functionality required for R6 which is not already realized within the HLR.

X.500 [89] defines - from a model point of view - the basics for a directory like information base. The following figure shows some of the crucial elements, for details please refer to [89].

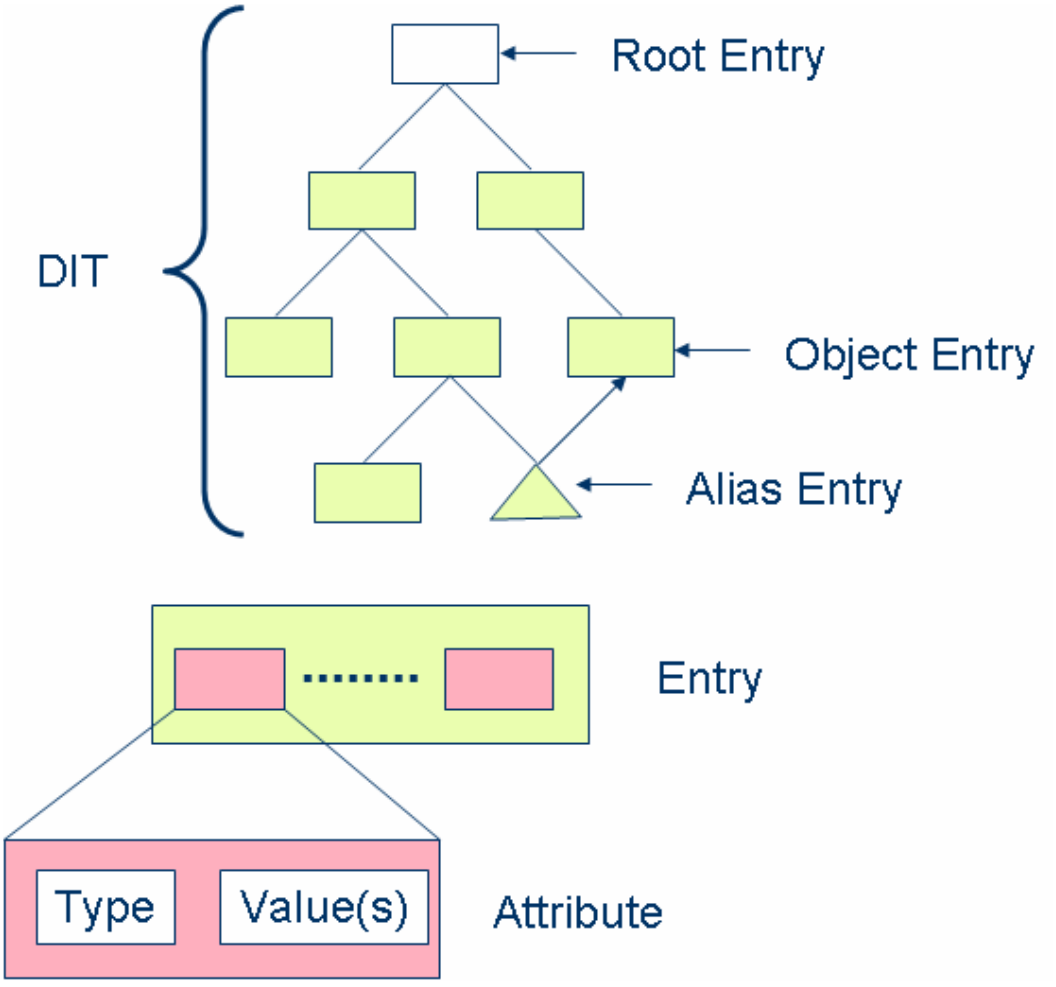


Figure A.1.1: X.500 Directory Information Tree - DIT

Figure A.1.1 shows the structure and the contents of an instantiated X.500 schema. Data are collected into entries (which are instantiated object classes) and these entries are organized in a tree like fashion into the Directory Information Tree (DIT). The building blocks of the object classes in the schema definition are attributes, whose types and values for the basis of the entries in the DIT.

One specific type of entry, which can be seen in figure A.1.1 is the "Alias" entry, which performs a redirect to another entry within the tree.

The following figure shows the rough structure of a possible instantiation of an X.500 based HLR schema.

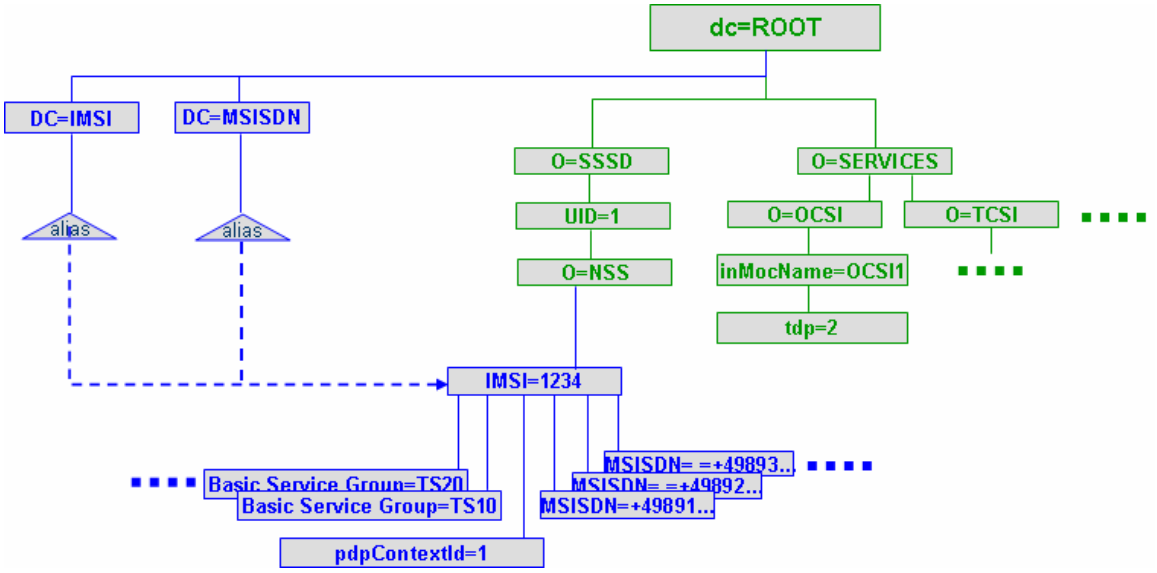


Figure A.1.2: X.500 based HLR DIT for a multi-numbering subscriber

The model in figure A.1.2 shows three parts (only the entry names, no attribute values):

- Common part:
  - Root: Common to the whole DIT.
  - SSSD: Subscriber Specific Service Data, is root of the part of the DIT, which is concerned with individual subscriber/end-user data.
  - UID: End-user identity, containing data specific for this end-user.
  - NSS: Network Supporting Services, is the root node for all Network Supporting Services (see clause 5).
  - Services: is the root node for the end-user data, which are transmitted (e.g. in the course of a Location Update), but which are common to many end-users (and maybe also to more than one network function or enterprise application).
  - OCSI: CAMEL Subscription Information for a Mobile Originated Call (with respective instances below).
- Direct Access part:
  - The Aliases have been described as possibilities to define a redirect. This fact can be used to model fast accesses. In the above example aliases for MISISDNs and IMSIs lead to the respective end-user instance, exactly to the service needed.
- HLR specific part: The entries represent a part of a multi-number and GPRS enabled post-paid mobile end-user.
  - IMSI: represents the root of the 2G/2.5G end-user information, with the respective properties below it.

The next figure represents the delta-HSS model as discussed at the beginning of this clause.

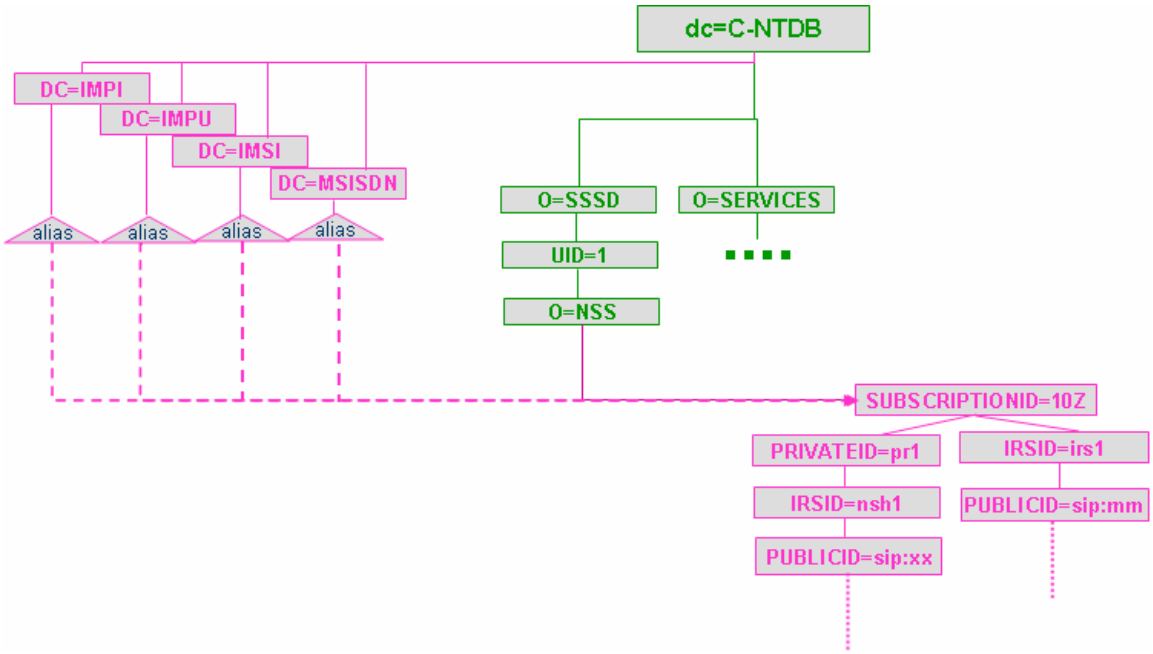


Figure A.1.3: X.500 based HSS DIT

The grouping is the same as in the HLR case in figure A.1.2.

- Common part: see explanations to figure A.1.2.
- Direct Access part:
  - Additional Aliases for the private and public userid have been added.
- HSS specific part: The entries represent a part of an end-user subscribing e.g. to a presence service:
  - SubscriptionId: represents the root of the HSS end-user information, with the respective properties below it.

The next figure shows a combined HLR-HSS DIT.

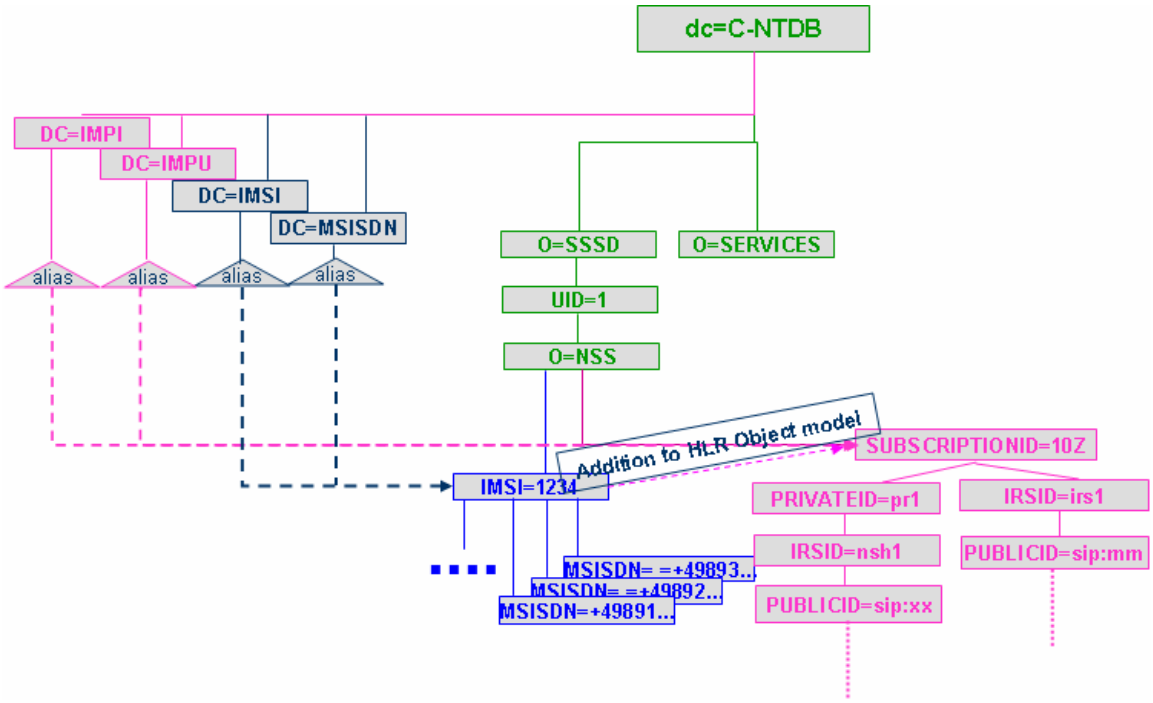


Figure A.1.4: X.500 based combined HLR and HSS DIT

When combining the two models, a few points become obvious:

- The wish to keep data redundancy at a minimum leads to the fact that both network functions (HLR and HSS) use the same fast access for IMSI and MSISDN. As these pointers are unique they can only point either to SUBSCRIPTIONID or to IMSI.
- If one of the network functions has been there before the other, its data model will change with the introduction of the next one (figure A.1.4. shows that for the HSS a different handling of the fast access for IMSI and MSISDN would be necessary, for HLR an additional attribute in one of "its" entries is present).
- In general, every addition of an object model for a new network function or enterprise application could yield similar problems and provoke changes both in the fragments of the end-user model pertaining to the respective function as well as in the function itself.

The three bullets above arising from a rather simplified example show the necessity of an Adaptation Layer:

- If data can be shared between network functions or enterprise applications as discussed in clause 5, then they should only exist once in the database.
- Already running network functions or enterprise applications should not be affected by the addition of new ones. So the data structure, as far the function sees it, should not change.

So the Adaptation Layer has to posses mechanisms to:

- Provide specific Adaptive Entities in order to simulate certain data structures.
- Ensure data integrity for all functions involved.
- Provide standard access (in this case LDAP v3), which hides the fact that an Adaptation Layer exists.

NOTE: In case of LDAP v3 any implementation of an Adaptation Layer would be proprietary, whereas e.g. in case of SQL the Adaptation Layer would be standardized for a greater part, as SQL99 officially supports view technology.

A.2 The Network Architecture

In clause 6 properties of distributed databases were discussed in detail. This clause will see a specific instance of one, namely an X.500 based database.

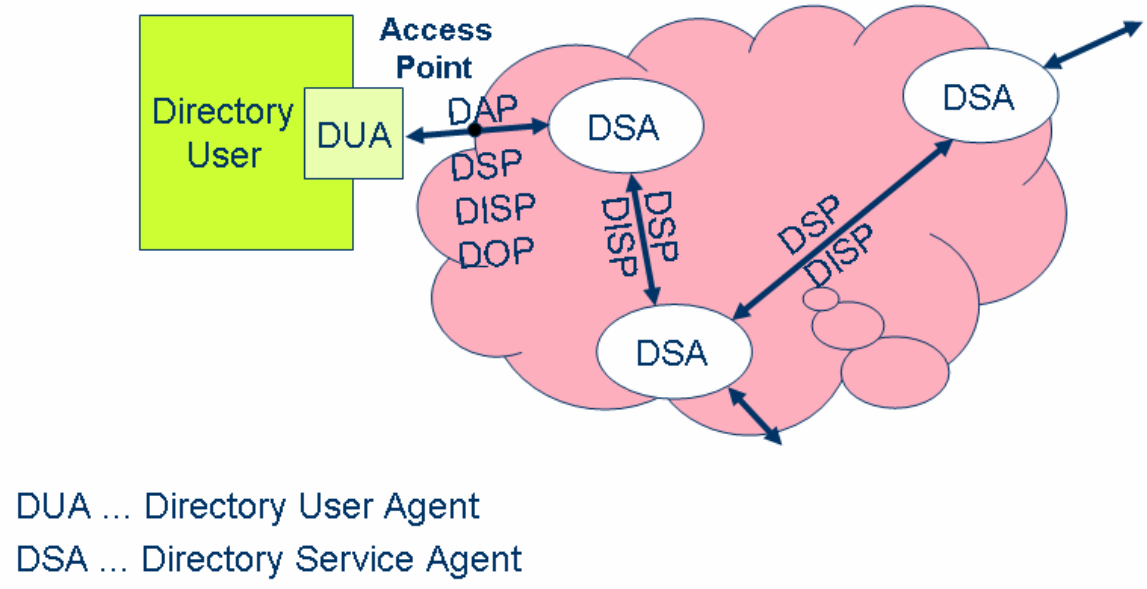


Figure A.2.1: X.500 based distributed database

Figure A.2.1 shows a distributed database as it is defined in X.500. It supports the following communication protocols:

- Directory Access Protocol (DAP): defines the exchange of requests and outcomes between a DUA and a DSA (ITU-T).
- Directory System Protocol (DSP): defines the exchange of requests and outcomes between two DSAs (ITU-T).
- Directory Information Shadowing Protocol (DISP): defines the exchange of replication information between two DSAs that have established shadowing agreements (ITU-T).
- Directory Operational Binding Management Protocol (DOP): which defines the exchange of administrative information between two DSAs to administer operational bindings between them (ITU-T).

The DUA in figure A.2.1 is equivalent to the network functions and enterprise applications discussed in this TR. The inter-DSA network provides:

- One logical database, as the DUA only needs one access point (requests are passed on internally using DSP).
- The possibility to provide local "shadow copies" for fast read access (using DISP).
- The possibility to define data fragments for different DSAs.

As DAP is a fairly complex protocol, IETF developed a lightweight form of DAP, which is easier to handle. The drawback was that originally it was only intended as a client server application without any distribution. One of the more frequent ways round this problem was to define a protocol mapping from LDAP to DAP, which would allow the client a simple data handling and still provide the distribution necessary (see figure A.2.2).

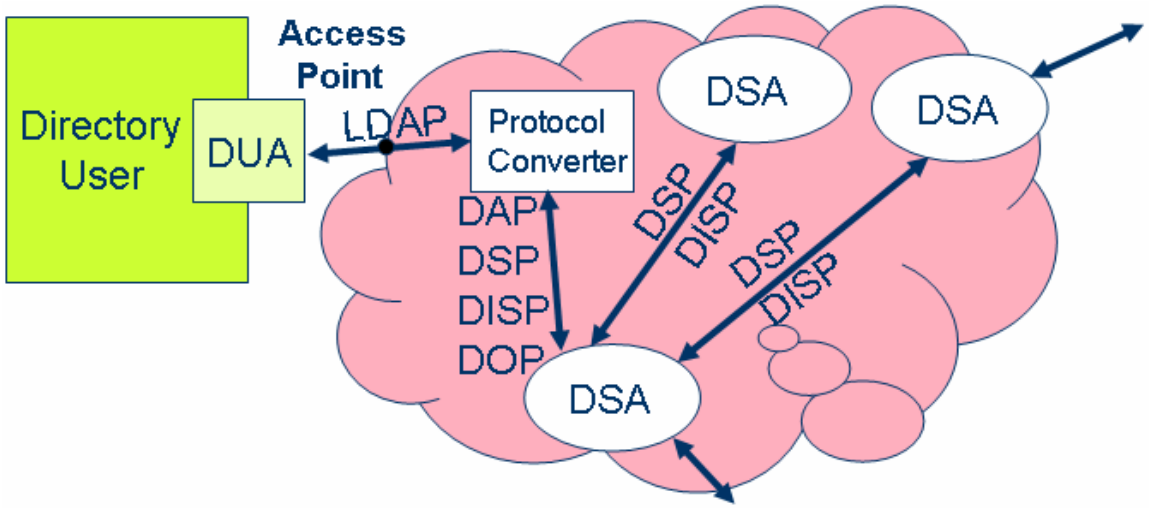


Figure A.2.2: LDAP in conjunction with an X.500 based distributed database

Lightweight DAP (LDAP): defines the exchange of requests and outcomes between a DUA and a DSA (IETF).

NOTE: The directory definitions from ITU-T were originally not intended for real-time and update intensive applications, so for the purposes of the functions discussed in clause A.1 some observations are appropriate:

- In order to minimize the number of redirects within the distributed data base, all of the data requested by the DUA in one operation (read or update)should be found on one DSA.
- All information about the fast accesses as defined in clause A.1 should be placed on the entry DSA of the DUA (which then gets a kind of proxy function similar to the one described in clause 6, figure 6.3.1.2).

Annex B:
Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Cat**	**Old**	**New**
Dec 2006	SA_34	SP-060840	--	--	Submitted to TSG SA#34 for Information	--	1.0.0	
May 2007	SA_36	SP-070302	--	--	Submitted to TSG SA#36 for Approval		2.0.0	8.0.0