3G TR 23.821 V1.0.1 (2000-07)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Architecture Principles for Release 2000
(Release 2000)

Keywords

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 Specification (TS) 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.

1 Scope

The scope of this Technical Report is to list architectural requirements, features, functions and solutions of UMTS inside the scope of UMTS Release 00. These are working assumptions agreed by TSG SA WG2. The TR focuses on

- new/modified functionality as compared to Release 99
- technical description of the features, functions and solutions of R00.

It is expected that this TR will act as a basis for the detailed Stage 2 specification work.

This TR has been created to ease the development of R00 work prior to the finalization of the R99 specifications. In conjunction with when R99 is finalized, work on the TR will cease and the relevant CRs will be produced to incorporate the contents of this TR within the R00 version of the specifications."

2 References

[Editor's note: Chapter to be completed]

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.

[1] J. Rosenberg, J. Lennox, H. Schulzrinne: "Programming Internet Telephony Services" , IEEE Network Magazine, 13(3):42-49, May/June 1999

[2] G.P. Gerhard: SIP and Parlay- "Design for Applications", Presentation at SIP 2000

[3] L. Slutsman, G. Ash, F. Haerens, V, Gurbani: "Framework and Requirements for the Internet Intelligent Networks (IIN)", Internet Draft, March 2000, <draft-lslutman-sip-iin-framework-00.txt>

[4] A. Kristensen, A. Byttner, R. Kurmanowytsch: "Programming SIP Services", iptel2000 Proceedings, 19-21

[5] 3GPP TR 21.978 - Feasibility Technical Report – CAMEL Control of VoIP Services

[6] 3GPP TS 23.127 - Virtual Home Environment / Open Service Architecture

[7] 3GPP TR 29.998 - Open Services Architecture - API - Part 2

[8] S. Beddus, G. Bruce, S. Davis: "Opening Up Networks with JAIN Parlay", IEEE Communications Magazine, 136-143, April 2000

3 Definitions, symbols and abbreviations

[Editor's note: To be completed]

[Note: The following section is intended to be included in TS 23.002 (proposed chapter, if any):

- 3.1 (Chapter 3)]

3.1 Definitions

CS Services: Telecommunication services provided to "GSM/ISDN" clients via 24.008 CC.

PS Connectivity Services: IP connectivity service provided to IP clients via 24.008 SM.

IM Services: IP Multimedia Services that require support on the Call Control level carried on top of the PS connectivity services (this may include an equivalent set of services to the relevant subset of CS Services).

PS services: The superset of IM services and PS connectivity Services.

CS CN domain: comprises all core network elements for provision of CS services.

PS CN domain: comprises all core network elements for provision of PS connectivity services.

IM CN subsystem: (IP Multimedia CN subsystem) comprises all CN elements for provision of IM services

Service Subsystem: Comprises all elements providing capabilities to support operator specific services (e.g. IN and OSA)

External Applications: Applications on an external Host. Examples of such applications:

- PS connectivity external applications access the network via the PS connectivity services (e.g. Email server on a corporate LAN)
- Service Control External Applications access the network via the capabilities of the IM CN Subsystem (e.g text to speech conversion via web browsing) or the CS CN Domain (e.g CS speech freephone application).

User Equipment is a device allowing a user access to network services. For the purpose of 3GPP specifications the interface between the UE and the network is the radio interface. A User Equipment can be subdivided into a number of domains, the domains being separated by reference points. Currently defined domains are the USIM and ME Domains. The ME Domain can further be subdivided into several components showing the connectivity between multiple functional groups. These groups can be implemented in one or more hardware devices. An example of such a connectivity is the TE – MT interface.

The **Radio Access Network domain** consists of the physical entities, which manage the resources of the radio access network, and provides the user with a mechanism to access the core network. The Access Network Domain comprises roughly the functions specific to the access technology.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

4 Introduction

[Editor's Note: This chapter is an introduction to the TR. The text in this chapter is not intended to be included in any other 3GPP specification]

This technical report (TR) was created in order to collect agreed working assumptions for R00 (see the scope of the TR in Chapter 1). The intention is that the text included in this TR will eventually be included in other 3GPP R00 reports/specifications, either via a change request (CR) procedure to existing R99 documents, or as part of new R00 reports/specifications. For this purpose, each chapter begins by suggesting in which report/specification the text in the chapter eventually will be included.

This TR is not intended to be published by 3GPP.

4.1 General guidelines for the UE to network protocols

In order to achieve access independence and to maintain a smooth interoperation with wireline terminals across the Internet, it is important to be conformant to IETF "Internet standards". Therefore, R00 shall, as far as possible, conform to IETF "Internet standards" for the cases where an IETF protocol has been selected, e.g. SIP.

As VoIP is targeted also for mass volume low-end products, it is important that a minimum set of mandatory codecs and minimum set of mandatory protocol options is standardised for integration in the mobile. The 3GPP shall specify the mandatory codecs and protocol options towards the UE.

3GPP shall guarantee the stability and backward compatibility of the air interface protocols including multimedia towards Ues. These protocols shall also be part of the 3GPP test specifications. Other multimedia aspects such as the real-time radio bearers and which codecs to be mandated in a UE shall be standardised by 3GPP.

5 Reference Architecture

[Editor's note: this chapter discusses overall reference architecture issues which are not covered in other chapters]

[Note: The following sections are intended to be included in TS 23.002 (proposed chapter, if any):

- Section 5.2 (Chapter 5)
- Section 5.3 (Chapter 4)
- Section 5.4 (Chapter 6. Alternatively, a chapter on Description of Reference Points may be created.)]

[Note: In which document the following section should be included is ffs (TS 23.121 may be a candidate):

- Section 5.1]

5.1 Architecture Principles

The following principles apply to the GSM/UMTS Reference Architecture for Release 00 and future releases.

Transport Independence (to control heterogeneous bearer mechanisms): The GSM/UMTS CN reference architecture shall be independent of the underlying transport mechanism (e.g. STM, ATM or IP). Further more the operators shall have the freedom to utilise a single or any combination of transport technologies.

Standardised alternatives for transport mechanisms: The alternatives for the signalling transport (e.g. SS7, SIGTRAN) for the service control, call control and bearer control protocols as well as the alternatives for the user plane transport shall be standardised for the relevant transport mechanisms.

Decomposition of network functions: The GSM/UMTS reference architecture all-IP option shall be defined in terms of separate functions and clear interfaces such that it is possible to separate transport from signaling. [With the objective of the separation of call/session, mobility and service control. This topic needs further study.] Thus operators shall have the freedom to provision, dimension and upgrade these network functions in a modular fashion. This modularity shall give operators flexibility and scaleability of network implementations.

Flexible traffic processing function placement: The GSM/UMTS reference architecture shall allow operators to place the traffic processing function in the most practical, cost-effective part of the network

Use of internet protocols: The GSM/UMTS reference architecture shall use, as appropriate, existing/evolving internet protocols e.g. to support multi-media services, interoperability with other next generation fixed or mobile networks (NGNs), and media gateway controllers.

Support for a variety of mobile equipment: The GSM/UMTS reference architecture shall support a range of different terminal types (simple speech only terminals, multi-media terminals, PDAs, Laptop, etc.). One particular aspect is that not all terminals may be able to support end-to-end IP capabilities, e.g. CS voice only terminals.

Independence of access technology: The GSM/UMTS reference architecture shall be designed to ensure that a common core network can be used with multiple wireless and wireline access technologies (e.g. xDSL, Cable, Wireless LAN, Digital Broadcast, all IMT2000 radio access technologies).

Support for roaming onto other 2G and 3G mobile networks: The GSM/UMTS reference architecture shall be designed to facilitate roaming between different network types.

Support of Service Requirements: The GSM/UMTS reference architecture shall include mechanisms for operators and third-parties to rapidly develop and provide services and for users to customise their service profile.

Support of regulatory requirements: The GSM/UMTS reference architecture shall include features to support regulatory requirements such as legal intercept, number portability, other regional requirements. To all terminal types and communication type (CS and PS) as appropriate.

Insertion of a new IP multimedia CN Subsystem with standard interface(s) with the service environment at home that can also be used in roaming cases.

Separation between Bearer level, Call control level and Service level:

- **Use of different access technology to connect the "IP multimedia CN Subsystem"**: The IP multimedia domain is connected to the bearer network at a fixed reference point (anchor point) thus hiding the micro mobility of the UE (it does not hide roaming). This reference point shall be independent from the access technology that can be GPRS, UMTS PS or any relevant wireless, wired-line access technology as long as they provide transport of user packets up to this reference point and as they hide micro-mobility of the UE. As a consequence, the behaviour of the multimedia call control server (CSCF) can be the same whatever the access technology (radio or wired-line). Multimedia call control/mobility management shall not be aware of the access technology: the multimedia Call Control (CSCF) does not handle notions such as Hand-Over, RA, …

- **The access to the IP Multimedia CN Subsystem is supported by the PS domain at the Gi interface**: The PS domain provides bearers that are used by the UE for its signalling and provides user plane exchanges with multimedia (SIP) call control servers (CSCF) and gateways. These servers / gateways are located behind the GGSN acting as an anchor point for the mobility which means that when the terminal is moving, the call control server is not changed as long as the UE is registered on this server. The bearer network is made up of radio access (e.g. UTRAN, GERAN,…) and of a backbone (SGSN and GGSN).

The specifications need to support both circuit-mode and packet-mode domains

- Considering the traffic mix resulting from the set of 3G services and the need for flexible evolution paths, it is necessary to have separate circuit switched domain and packet switched domain.

- Each domain will handle its own signalling traffic, switching and routing.

Keep network functions separate from radio access functions

- The same network should support a variety of access choices, and access technologies may evolve further. Therefore network functions such as call control, service control, etc. should remain separate from access functions and ideally should be independent of choice of access. This implies that the same CN should be able to interface with a variety of RANs.

Separate functions that are likely to evolve independently. The following bullets in the list are examples of major functions that may need to evolve independently. Further discussions are needed to establish an agreed list.

- Bearer control in both access and network

- Multimedia control for multimedia sessions

- Switching and routing

- PS Mobility management, session control and access security functions

- CS Call Control, Mobility Management and access security functions

- Security functions

- Control for and the traffic processing e.g. voice
- location-based service functionality
- Service control:
  - service capabilities, VHE for roamers
  - Mail services control
  - location-based services
  - Service features and applications

Break down mobility management into a set of independent functions. Mobility management will be a complex function in R'00. By breaking it down into independent components it will become more manageable. The list below is a suggested breakdown:

- Inter-domain mobility: Location of the user in terms of the domain (CS)/sub-system (IP Multimedia) currently serving the user.
- CSCF roaming: Location of the user in terms of the CSCF currently serving the user. The user may be within any wireless or fixed network.
- Change of Network Point of Attachment: Location of the user in terms of the address at which the user can be fund, depending on the registred mode. The user may be within any wireless or fixed network.
- Radio Access Mobility : Location management and management of the terminal associated with changes in RA/LA within a system, or associated with changes in cell and RNC within RA/LA.

  Radio Access Mobility can referred to as "micro-mobility" as opposed to the other types of mobility which have an impact on the IP multimedia sub-system.

The PS CN domain provides the PS Connectivity services to IP terminals. The PS domain maintains the service while the terminal moves and hides these moves to the other subsystems (i.e. IP multimedia CN Subsystem) using its bearer level service.

Speech support in the CS CN domain: R00 features to enhance speech support (e.g. TrFO/OoBTC: speech quality, transmission efficiency) in CS CN should consider a common solution for both UTRAN-speech (Iu i/f with codec in core) and GSM-speech (A i/f with codec in RAN).

Resource Allocation Principles: Release 2000 architecture shall be based on the principle that all resources within a network operator's network be managed by network elements within that network operator's network.

For calls that terminate on a network operator's Media Gateway (MGW), ports are allocated exclusively by the Media Gateway Control Function (MGCF) within that network operator's network. When multiple MGCFs exist within the network operator's network, choice of the proper MGCF for handling a call shall be made by a function within that network operator's network.

Authorization for bearer resources in a network operator's network is performed by a CSCF within that network operator's network. When call control is performed by a CSCF in the subscriber's home network, this authorization function shall be performed by a CSCF in the same network as the bearer resources being reserved.

5.2 Reference Architecture Overview

The full view of Release 2000 architecture is provided in figure 5.1.

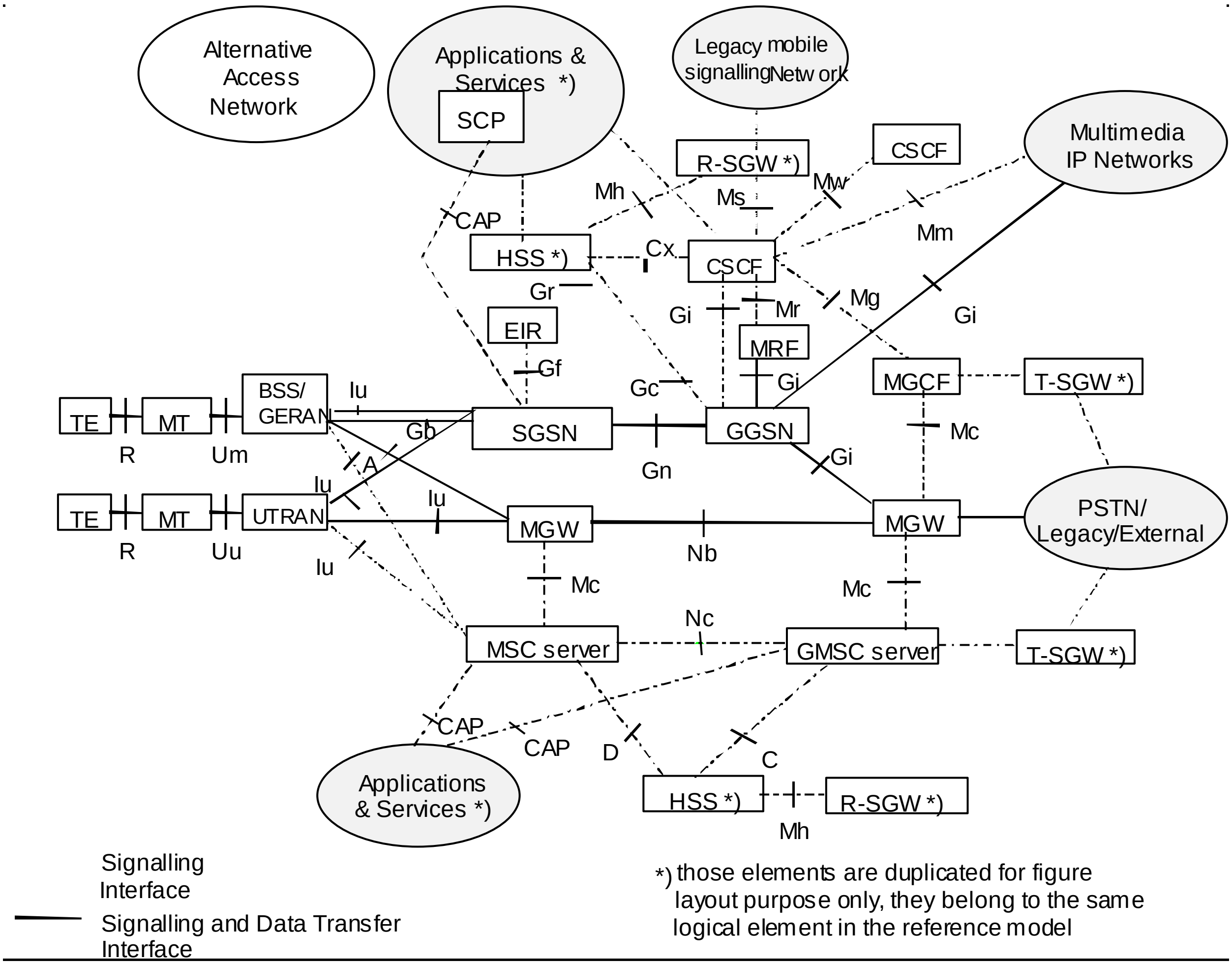

Figure 5.1: Reference Architecture for Release 2000

NOTE 1: A (G)MSC Server and associated MGW can be implemented as a single node as with the (G)MSC in R99.

NOTE 2: The following interfaces are also part of the R00 reference architecture, but are not shown for layout purposes only:

- between MSC's (including MSC server / MGW), E interface;
- between VLR's, G interface;
- between SGSN's, Gn interface;
- between CSCF and UE, Gm interface;
- between MSC (or MSC server) and SGSN, Gs interface (optional).

[Editor's note: The final approval of Figure 5.1 and related text is dependent on e.g.:

- *The specification of R00 requirements.*
- *The relationship between different call control models (H.323/H.324 etc.) needs to be clarified.*
- *Clarification of which interfaces/reference points that require standardization and which standardized protocols (from which standard body) to use, including those that 3GPP still has work on.*

- *Addition of potentially missing reference points, e.g. Gs and a reference point between the MGW and the multimedia related control nodes (e.g., CSCF, etc.) when multimedia is going to be operated in the CS Services domain. Also, further reference points should be considered, e.g. internal to the proposed HSS as well as components of the HSS to the other nodes.*
- *This reference architecture is subject to verification through the inclusion of flow charts showing signalling flows for MM, SM etc. in, e.g., an annex or other chapters in the TR.*
- *The inclusion of separate CBC node in the figure.*
- *Clarify the relationship with Mobile IP.*
- *Appropriate description on the GERAN will be added.]*

The architecture shown and the components of which are described in subsequent sections allow for flexible and scaleable mechanisms to support global roaming and interoperability with external networks such as PLMN, 2G Legacy networks, PDNs and other multimedia VoIP networks.

5.3 Functional Elements

5.3.1 Call State Control Function (CSCF)

The CSCF consists of two components: the Serving CSCF and the Interrogating CSCF.

The Serving CSCF is used for mobile originated communications and also to support mobile terminated communications, it provides the SPD and AH functionality defined below. The Serving CSCF supports the signalling interactions with the UE via the Gm interface. The HSS is updated with the Serving CSCF address and the HSS sends the subscriber data to the Serving CSCF for storage.

The Interrogating CSCF is used for mobile terminated communications and is used to determine how to route mobile terminated calls. The Interrogating CSCF interrogates the HSS for information to enable the call to be directed to the Serving CSCF. The Interrogating CSCF provides the ICGW and AH functionality defined below.

[Editor's note: The role of the CCF (see below) with the Interrogating and Serving CSCF is for further study.]

For mobile terminated communications both Serving CSCF and Interrogating CSCF functionality can be involved.

For mobile originated communications Interrogating CSCF functionality is not required.

Both Serving CSCF and Interrogating CSCF components can be provided in a single CSCF if required.

CSCF functionality:

ICGW (Incoming call gateway)

- Acts as a first entry point and performs routing of incoming calls,
- Incoming call service triggering(e.g. call screening/call forwarding unconditional) may need to reside for optimisation purposes,
- Query Address Handling (implies administrative dependency with other entities)
- Communicates with HSS

CCF (Call Control Function)

- Call set-up/termination and state/event management
- Interact with MRF in order to support multi-party and other services
- Reports call events for billing, auditing, intercept or other purpose
- Receives and process application level registration

- Query Address Handling (implies administrative dependency)
- May provide service trigger mechanisms (service capabilities features) towards Application & services network (VHE/OSA)
- May invoke location based services relevant to the serving network
- May check whether the requested outgoing communication is allowed given the current subscription.

SPD (Serving Profile Database)

- Interacts with HSS in the home domain to receive profile information for the R00 all-IP network user and may store them depending on the SLA with the home domain
- Notifies the home domain of initial user's access (includes e.g. CSCF signalling transport address, user ID etc. needs further study)
- May cache access related information (e.g. terminal IP address(es) where the user may be reached etc.)

AH (Address Handling)

- Analysis, translation, modification if required, address portability, mapping of alias addresses
- May do temporary address handling for inter-network routing.

5.3.2 Home Subscriber Server (HSS)

The Home Subscriber Server (HSS) 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.

As an example, HSS could provide support to the call control servers in order to complete the routing/roaming procedures by solving authentication, authorization, naming/addressing resolution, location dependencies, etc…

HSS is responsible for holding 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; HSS handles the user registration, and stores inter-system location information, etc.
- The User profile (services, service specific information…)

Based on this information, the HSS is also responsible of supporting the CC/SM entities of the different control systems (CS Domain control, PS Domain control, IP Multimedia control…) offered by the operator.

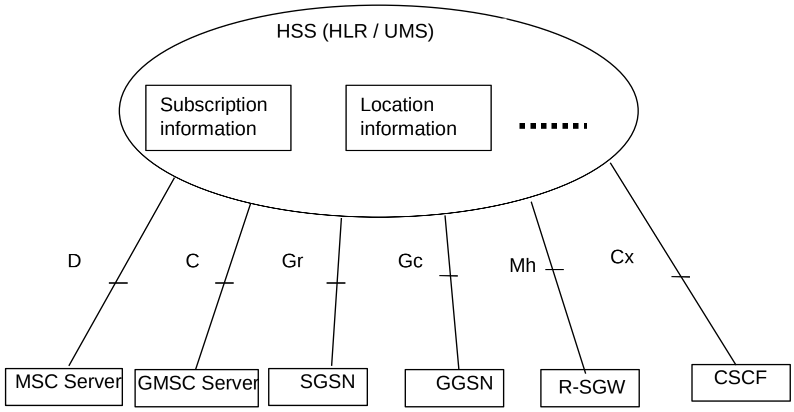

Figure 5.2: Example of a Generic HSS structure and basic interfaces

HSS may integrate heterogeneous information, and enable enhanced features in the core network to be offered to the application & services domain, at the same time hiding the heterogeneity.

The HSS consists of the following functionalities:

- User control functions required by the IM CN subsystem.
- The subset of the HLR functionality required by the PS-Domain.
- And the CS part of the HLR, if it is desired to enable subscriber access to the CS-Domain or to support roaming to legacy GSM/UMTS CS-Domain networks

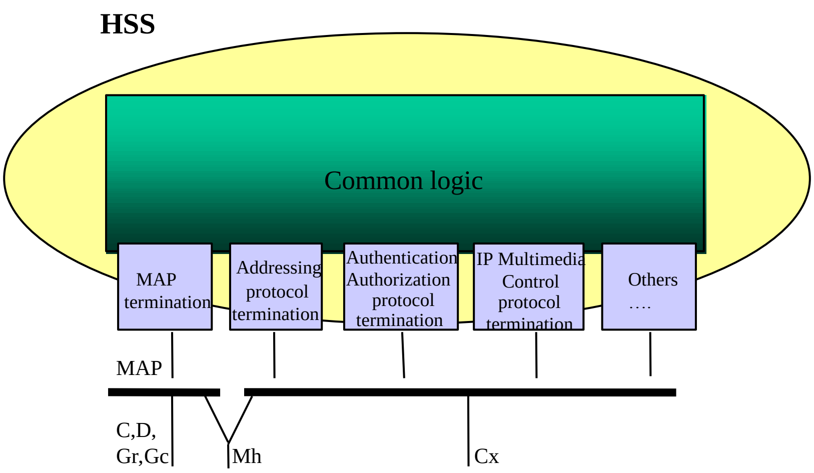

Figure 5.3: Example of a generic HSS structure with further breakdown into protocols over the basic interfaces

The HSS structure is as follows (see also figure 5.3):

MAP termination:

HSS terminates the MAP protocol as described in MAP specifications:

- User Location Management procedures
- User Authentication Management procedures
- Subscriber profile Management procedures,
- Call handling support procedures (Routing information handling)
- SS related procedures, etc…

Addressing protocol termination:

HSS terminates a protocol to solve addressing according to appropriate standards:

- Procedures for user names/numbers/addresses resolution
- As an example, DNS+ protocol could be a suitable candidate, as it is being defined within the ENUM group in IETF (currently looking into URL/E.164 naming translation, etc…).

Authentication, Authorization protocol termination:

HSS terminates authentication and authorization protocols according to appropriate standards:

- User authentication and authorisation procedures for IP based Multimedia services
- As an example, Diameter protocol could be a suitable candidate, as it is being defined within IETF [1].

IP MM Control termination:

HSS terminates the IP based MM call control protocol, according to appropriate standards:

- User Location Management procedures for IP based Multimedia services
- IP based Multimedia Call handling support procedures (Routing information handling)

As an example, the SIP protocol (or some parts of it, related with location procedures) could be a suitable candidate.

5.3.3 Transport Signalling Gateway Function (T-SGW)

This is component in the R00 network is PSTN/PLMN termination point for a defined network. The functionality defined within T-SGW should be consistent with existing/ongoing industry protocols/interfaces that will satisfy the requirements.

- Maps call related signalling from/to PSTN/PLMN on an IP bearer and sends it to/from the MGCF.
- Needs to provide PSTN/PLMN <-> IP transport level address mapping.

5.3.4 Roaming Signalling Gateway Function (R-SGW)

The role of the R-SGW described in the following bullets is related only to roaming to/from 2G/R99 CS and GPRS domain to/from R00 UMTS Teleservices domain and UMTS GPRS domain and is not involving the Multimedia domain.

- In order to ensure proper roaming, the R-SGW performs the signaling conversion at transport level (conversion: Sigtran SCTP/IP versus SS7 MTP) between the legacy SS7 based transport of signaling and the IP based transport of signaling. The R-SGW does not interpret the MAP / CAP messages but may have to interpret the underlying SCCP layer to ensure proper routing of the signaling.
- (For the support of 2G / R99 CS terminals): The services of the R_SGW are used to ensure transport interworking between the SS7 and the IP transport of MAP_E and MAP_G signalling interfaces with a 2G / R99 MSC/VLR

[1] Work/early discussions on IETF are still ongoing

5.3.5 Media Gateway Control Function (MGCF)

This component is PSTN/PLMN termination point for a defined network. The functionality defined within MGCF should be consistent with existing/ongoing industry protocols/interfaces that will satisfy the requirements.

- Controls the parts of the call state that pertain to connection control for media channels in a MGW.
- Communicates with CSCF.
- MGCF selects the CSCF depending on the routing number for incoming calls from legacy networks.
- Performs protocol conversion between the Legacy (e.g. ISUP, R1/R2 etc.) and the R00 network call control protocols.
- Out of band information assumed to be received in MGCF and may be forwarded to CSCF/MGW.

5.3.6 Media Gateway Function (MGW)

This component is PSTN/PLMN transport termination point for a defined network and interfaces UTRAN with the core network over Iu.

The functionality defined within MGW should be consistent with existing/ongoing industry protocols/interfaces that will satisfy the requirements.

A MGW may terminate bearer channels from a switched circuit network (i.e., DSOs) and media streams from a packet network (e.g., RTP streams in an IP network). Over Iu MGW may support media conversion, bearer control and payload processing (e.g. codec, echo canceller, conference bridge) for support of different Iu options for CS services: AAL2/ATM based as well as RTP/UDP/IP based.

- Interacts with MGCF, MSC server and GMSC server for resource control.
- Owns and handles resources such as echo cancellers etc.
- May need to have codecs.

The MGW will be provisioned with the necessary resources for supporting UMTS/GSM transport media. Further tailoring (i.e packages) of the H.248 may be required to support additional codecs and framing protocols, etc.

The MGW bearer control and payload processing capabilities will also need to support mobile specific functions such as SRNS relocation/handover and anchoring It is expected that current H.248 standard mechanisms can be applied to enable this.

5.3.6.1 General Principles for Use of CS-MGW Resources

The following principles for use of CS-MGW resources apply:

1. it shall not be necessary to have the CS-MGW co-located with the MSC Server;
2. the CS-MGW resources need not be associated with any particular MSC Server (see note 1);
3. it shall be possible for any MSC Server to request resources of any CS-MGW in the network (see note 1);
4. it shall be possible for an RNC to connect to the CS-MGW indicated by the MSC server;

NOTE 1: For points 2 and 3 above, issues related to O&M procedures such as where notification of restart of a CS-MGW should be sent to, need to be considered. Extensions to H.248 may be required.

5.3.7 Multimedia Resource Function (MRF)

This component:

- performs multiparty call and multi media conferencing functions. MRF would have the same functions of an MCU in an H.323 network.
- Is responsible for bearer control (with GGSN and MGW) in case of multi party/multi media conference
- may communicate with CSCF for service validation for multiparty/multimedia sessions.

5.3.8 MSC Server

MSC server mainly comprises the call control and mobility control parts of a GSM/UMTS MSC.

The MSC Server is responsible for the control of mobile originated and mobile terminated 04.08CC CS Domain calls. It terminates the user-network signalling (04.08+ CC+MM) and translates it into the relevant network – network signalling. The MSC Server also contains a VLR to hold the mobile subscriber's service data and CAMEL related data.

MSC server controls the parts of the call state that pertain to connection control for media channels in a MGW.

5.3.9 Gateway MSC Server

The GMSC server mainly comprises the call control and mobility control parts of a GSM/UMTS GMSC.

5.3.10 MSC

A MSC server and a MGW make up the full functionality of a MSC as defined in 23.002 Gateway MSC

5.3.11 Gateway MSC

A GMSC server and a MGW make up the full functionality of a GMSC as defined in 23.002

[Editor's note: There is a need to consider possibilities that call incoming to the PLMN may be routed to entities other than the GMSC, e.g., for networks that do not deploy CS domain.]

5.4 Description of Reference Points

5.4.1 Cx Reference Point (HSS – CSCF)

The Cx reference point supports information transfer between CSCF and HSS.

The main procedures that require information transfer between CSCF and HSS are

1) Procedures related to Serving CSCF assignment
2) Procedures related to routing information retrieval from HSS to CSCF
3) Procedures related to UE-HSS infromation tunneling via CSCF

5.4.1.1 Procedures related to Serving CSCF assignment

Assigning a Serving CSCF for a subscriber

When a mobile subscriber becomes active (e.g. when terminal is powered on) and possibly when the subscriber moves, a CSCF shall be assigned to serve the subscriber.

The CSCF selection mechanism is outside of the scope of this section. The selection could be made either by the subscriber or by the HSS, but in any case it shall be authorised by the HSS by allowing the assignment procedure to complete successfully.

It is outside of the scope of this section whether the assignment procedure is initiated by the CSCF or by the HSS, in which order the related information is transferred, and whether the procedures include negotiation of parameters. In any case, **it is required that the following types of information can be transferred between CSCF and HSS:**

REQ 1: The Cx reference point shall support the transfer of *CSCF-UE security parameters* from HSS to CSCF, unless SA3 defines a different method to support a secure association between UE and CSCF.

- This allows the CSCF and the subscriber to communicate in a trusted and secure way (there is no à priori trust relationship between a subscriber and a CSCF)
- The security parameters can be for example pre-calculated challenge-response pairs, or keys for an authentication algorithm, etc.

REQ 2: The Cx reference point shall support the transfer of *service parameters of the subscriber* from HSS to CSCF.

- This may include e.g. supplementary service parameters, application server address, triggers etc

Note: it has to be determined what parameters should be stored where depending on the service control model. It has also to be made clear what are the functionality of the application level and service level.

REQ 3: The Cx reference point shall support the transfer of *CSCF capability information* from CSCF to HSS.

- This may include e.g. supported service set, protocol version numbers etc.

Note: The requirement has to be revisited in view of the choice of the service control model.

REQ 4: The Cx reference point shall support the transfer of *call signalling transport parameters* from CSCF to HSS. The requirement has to be revisited in view of the choice of the service control model.

- The HSS stores the signalling transport parameters and they are used for routing mobile terminated calls to the Serving CSCF.
- The parameters may include e.g. IP-address and port number of CSCF, transport protocol etc.

The information mentioned in REQ 1 – 4 shall be transferred before the CSCF is able to serve the mobile subscriber. It shall also be possible to **update** this information while the CSCF is serving the subscriber, for example if new supplementary services are activated for the subscriber.

Cancelling the Serving CSCF assignment

When the subscriber deactivates the terminal or possibly when he moves, the Serving CSCF assignment shall be cancelled.

REQ 5: The Cx reference point shall support the indication of cancelling the CSCF assignment.

- It shall be possible to initiate cancelling by both the CSCF and the HSS

5.4.1.2 Procedures related to routing information interrogation

The mobile terminated calls for a subscriber shall be routed either to a Serving CSCF or to a MGCF (if the subscriber is roaming in a legacy network). When a mobile terminated call set-up arrives at a CSCF that is authorised to route calls, the CSCF interrogates the HSS for routing information.

REQ 6: The Cx reference point shall support retrieval of routing information from HSS to CSCF

- The resulting routing information can be either Serving CSCF signalling transport parameters (e.g. IP-address).

Note: The requirement has to be revisited in view of the choice of the service control model.

5.4.1.3 Procedures related to UE-HSS information tunneling over Cx

The UE and HSS may need to exchange information that is transparent to CSCF, for example activation or modification of supplementary services. The CSCF may forward this information between UE and HSS, and the Cx reference point shall support tunneling of this information between CSCF and HSS.

REQ 7: The Cx reference point shall support tunneling of information that is exchanged between UE and HSS and forwarded transparently by the CSCF.

5.4.2 Gf Reference Point (SGSN – EIR)

Refer to TS 23.060 for a description of this reference point.

5.4.3 Gi (GGSN – Multimedia IP Network)

Refer to TS 23.060 for a description of this reference point.

5.4.4 Gm Reference Point (CSCF – UE)

This interface is to allow UE to communicate with the CSCF e.g.

- register with a CSCF,
- Call origination and termination
- Supplementary services control.

The Gm reference point supports information transfer between UE and serving CSCF. The main procedures that require information transfer between UE and serving CSCF are

- Procedures related to Serving CSCF registration,
- Procedures related to User service requests to the serving CSCF,
- Procedures related to the Authentication of the Application/Service,
- Procedures related to the CSCF's request for Core Network resources in the Visited Network.

5.4.5 Gn Reference Point (GGSN – SGSN)

Refer to TS 23.060 for a description of this reference point.

5.4.6 Mc Reference Point (MGCF – MGW)

The Mc reference point describes the interfaces between the MGCF and MGW, between the MSC Server and MGW, and between the GMSC Server and MGW. It has the following properties:

- full compliance with the H.248 standard, baseline work of which is currently carried out in ITU-T Study Group 16, in conjunction with IETF MEGACO WG.
- flexible connection handling which allows support of different call models and different media processing purposes not restricted to H.323 usage.
- open architecture where extensions/Packages definition work on the interface may be carried out.
- dynamic sharing of MGW physical node resources. A physical MGW can be partitioned into logically separate virtual MGWs/domains consisting of a set of statically allocated Terminations.
- dynamic sharing of transmission resources between the domains as the MGW controls bearers and manage resources according to the H.248 protocols.

The functionality across the Mc reference point will need to support mobile specific functions such as SRNS relocation/handover and anchoring. It is expected that current H.248/IETF Megaco standard mechanisms can be applied to enable this.

5.4.7 Mg Reference Point (MGCF – CSCF)

The Mg reference point is based on external specifications, e.g. SIP

5.4.8 Mh Reference Point (HSS – R-SGW)

This interface supports the exchange of mobility management and subscription data information between HSS and R99 and 2G networks. This is required to support Release 2000 network users who are roaming in R99 and 2G networks.

5.4.9 Mm Reference Point (CSCF – Multimedia IP networks)

This is an IP interface between CSCF and IP networks. This interface is used, for example, to receive a call request from another VoIP call control server or terminal.

5.4.10 Mr Reference Point (CSCF - MRF)

Allows the CSCF to control the resources within the MRF.

5.4.11 Ms Reference Point (CSCF – R-SGW)

This is an interface between the CSCF and R-SGW.

5.4.12 Mw Reference Point (CSCF – CSCF)

The interface allows the Interrogating CSCF to direct mobile terminated calls to the Serving CSCF.

5.4.13 Nc Reference Point (MSC Server – GMSC Server)

Over the Nc reference point the Network-Network based call control is performed. Examples of this are ISUP or an evolvement of ISUP for bearer independent call control (BICC). In the R'00 architecture different options for signalling transport on Nc shall be possible including IP.

5.4.14 Nb Reference Point (MGW-MGW)

Over the Nb reference point the bearer control and transport are performed. The transport may be RTP/UDP/IP or AAL2 for transport of user data. In the R00 architecture different options for user data transport and bearer control shall be possible on Nb, for example: AAL2/Q.AAL2, STM/none, RTP/H.245.

5.4.15 Reference Points towards SCP (CAP based interfaces)

This includes the interfaces from the SGSN to the SCP, from the Serving CSCF (and possibly the Interrogating CSCF) to the SCP, from the MSC Server to the SCP, and the GMSC Server to the SCP.

The interface from the SGSN to the SCP in the Applications and services domain is the interface defined for UMTS GPRS to support Charging Application Interworking. The interface from the CSCF to the SCP is required to allow the support of existing CAMEL based services.

The interface from the MSC Server to the SCP, and the GMSC Server to the SCP is the standard interface defined for CAMEL feature, which provides the mechanisms to support services of operators which are not covered by standardized UMTS/GSM services even when roaming outside the home PLMN.

The CAP based interfaces may be implemented using CAP over IP, or CAP over SS7 as shown in figure 5.4.

CAP		
TCAP		
SCCP		
M3UA	MTP-3B	Narrow-band SS7
SCTP (1)	SAAL	
IP (2)	ATM(2)	STM (2)

Figure 5.4: Protocol Stack for CAP

Note:

1) In IETF work is ongoing (e.g., SCTP/UDP/IP or directly SCTP/IP). The finally selected protocol stack is meant here.

2) The protocols do not correspond to the same OSI layer. They are drawn on the same height as they are "transport alternatives".

5.4.16 Gc, Gr, C, D Reference Points MAP based interfaces)

This includes the interfaces from the GGSN to the HSS (Gc reference point), from the SGSN to the HSS (Gr reference point), from the GMSC Server to the HSS (C reference point), and the MSC Server to the HSS (D reference point).

The MAP based interfaces may be implemented using MAP transported over IP, or MAP over SS7.

MAP can be transported on the same protocol stacks as CAP (refer to protocol stack in figure 5.4)

5.4.17 Iu Reference Point

This is the reference point between UTRAN and the R00 core network. This reference point is realized by one or more interfaces:

- Between UTRAN and SGSN, transport of user data is IP based.
- Between UTRAN and SGSN, transport of signalling is based on IP or SS#7.
- Between UTRAN and MGW, transport of user data is based on different technologies (e.g., IP, AAL2), and includes the relevant bearer control protocol in the interface.
- Between UTRAN and MSC server, transport of signalling is based on IP or SS#7.

When the Iu_cs is ATM based, then the protocols used can be based on R99 protocols or an evolved version.

When Iu_cs is IP based, new IP transport related protocols need to be added as part of the Iu protocols. It shall be possible to have R99 Iu interface with MSCs compliant to R99 specifications in the network.

It shall be possible to have a R99 CS domain with R99 Iu_cs reference point coexisting with a R00 Iu reference point.

6 Mobility Management

[Note: The following sections are intended to be included potentially in a new R00 specification on IP multimedia (proposed chapter, if any):

- 6.1]

[Note: The following sections are intended to be included in 23.121 (proposed chapter, if any):

- 6.2.1

- 6.3]

6.1 Address Management

6.1.1 Overview

The UMTS network may be implemented as a number logically separate IP networks which contain different parts of the overall system. In this discussion each of these elements is referred to as an "IP Addressing Domain". Within an "IP Addressing Domain" it is required that the nodes within the domain are part of a consistent non-overlapping IP-address space. It is also required that IP packets may be routed from any node in the domain to any other node in the domain using conventional IP routing. In a real implementation an IP Addressing Domain may be a physically separate IP network or an IP VPN.

IP Addressing Domains may be interconnected at various points. At these points of interconnect gateways, firewalls or NATs may be present. It is not guaranteed that IP packets from one IP Addressing Domain can be directly routed to any interconnected IP Addressing Domain. Rather inter-Domain traffic will be handled via firewalls or tunnels. This implies that different IP Addressing Domains can have different (and possibly overlapping) address spaces.

Figure 6.1 below shows the IP Addressing Domains involved in PS-domain and IP-subsystem services.

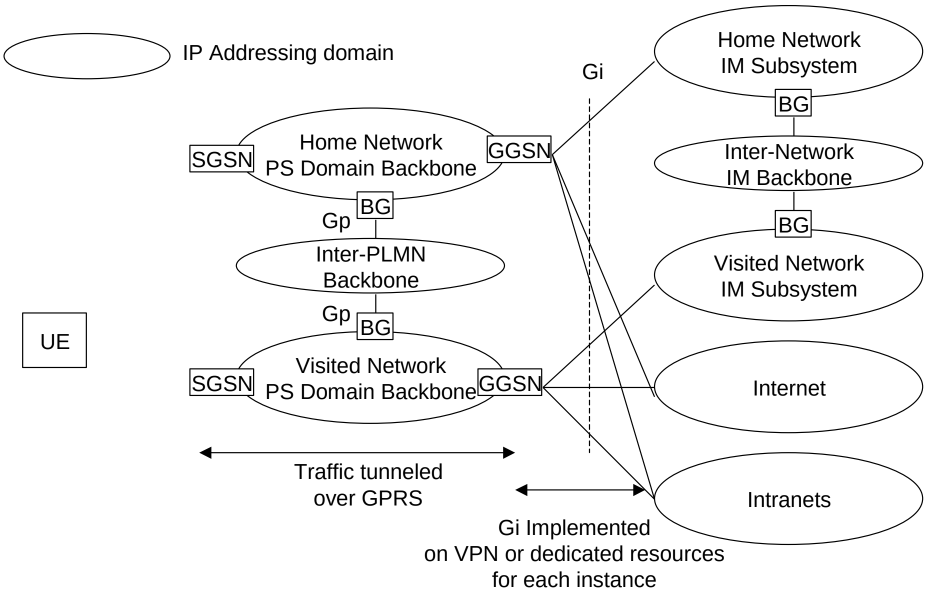

Figure 6.1: IP Addressing Domains Involved In PS-Domain and IM Services

Though UMTS permits the possibility of using different IP Addressing Domains as shown above it is possible that several different IP Addressing Domains fall under a common cooperative management regime. In this case the different IP Addressing Domains may be physically implemented as a single domain at the operator's discursion.

6.1.2 Addressing and Routing for Access to IM-Subsystem Services

NOTE: This section deals with a UE making access to IM-subsystem services only and via UMTS. How a UE can access IM subsystem services via other access types, or make simultaneous access to services in other IP networks is FFS.

A UE accessing IM-Subsystem services requires an IP address which is logically part of the Visited Network IM Subsystem IP Addressing Domain. This is established using an appropriate PDP-context. For routing efficiency this context should be connected though an GGSN in the visited network. The connection between the UE and the Visited Network IM Subsystem is shown below:

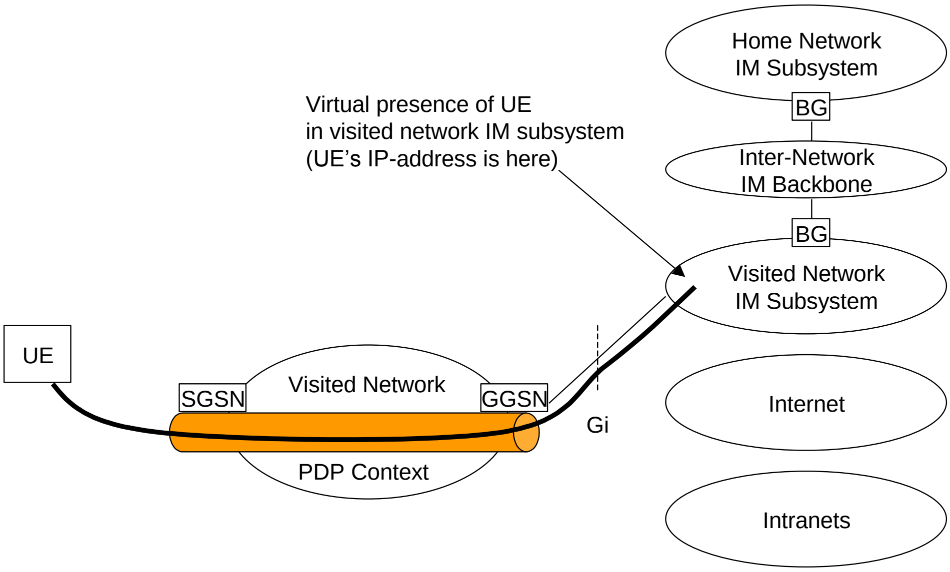

Figure 6.2: UE Accessing IM Subsystem Services in the visited network

6.2 Context Activation and registration

The IP address is allocated to UE either by GPRS or some other means e.g. by DHCP The UE shall use IP addresses assigned to it for, but not limited to, the following:

- the exchange application level signaling (e.g., registration, CC) with the serving CSCF from the acces s network currently used,
- application level registration to IP MM CN subsystem as an address used to reach the UE

  [Editor's Note: The use of DNS names, NAI (Network Access Identifier RFC2486) and SIP URL instead of IP address for application level registration is FFS],
- an address used to reach the UE for multimedia calls.

In GPRS, the terminal is associated with an IP address when the primary PDP context is activated. The IP address used for the purpose described above can be:

- the IP address obtained by the UE during the activation of a primary PDP context (e.g. if the UE does not have any existing PDP context active or desires to use a different IP address)
- the IP address of one of the already active PDP contexts.

In the following, a description of the order in which the registration procedure is executed need and how the IP address is allocated is shown. Figure 6.3 shows what procedures and in which order they are performed during the registration.

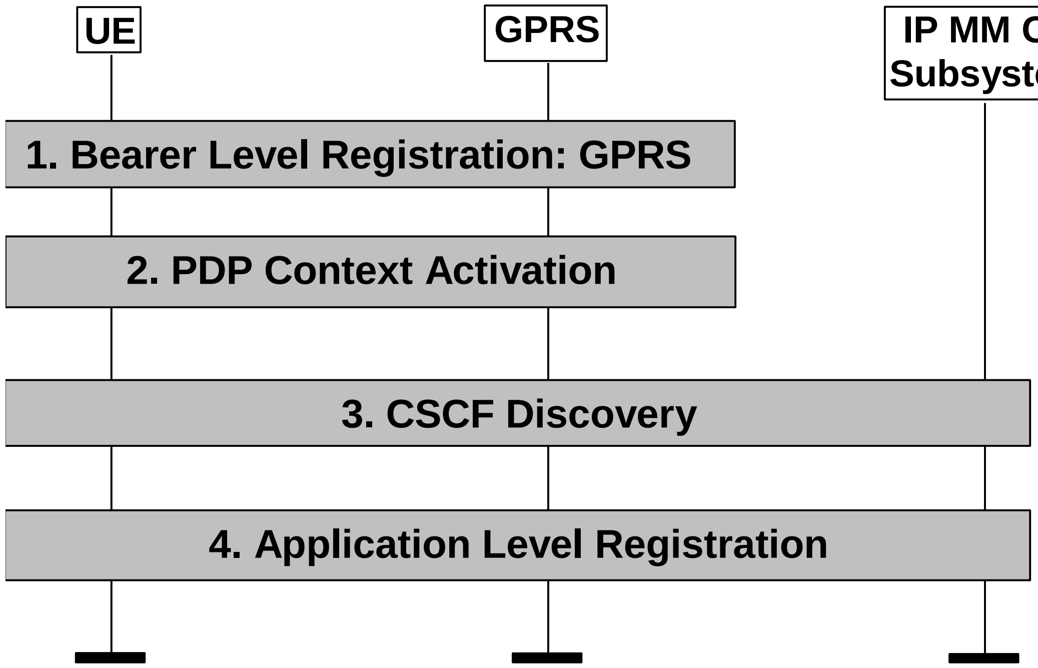

Figure 6.3: Registration

The following steps are performed:

1. the bearer level registration is performed (e.g. when the terminal is switched on or upon explicit indication from the user).

2. the PDP context activation is done. The UE has two options:

   - activate a primary PDP context and obtain a new IP address (e.g. if the UE does not have any existing PDP context active or desires to use a different IP address)

   - activate a secondary PDP context and re-use the IP address of one of the already active PDP contexts.

3. UE performs the CSCF discovery procedure, where the UE performs a CSCF discovery to select the CSCF to register with. *[Editor's note: Details regarding the CSCF discovery procedure are FFS]* .

There can be time gaps between these procedures and the following one. For instance, the UE may perform PDP context activation and the CSCF discovery, but not the application level registration. The UE may use the activated PDP context for other types of signalling, e.g. for CSCF discovery.

4. UE performs application level registration by providing the IP address obtained at step 2 to the CSCF selected at step 3. The IP address used for signalling purposes is allocated in association with PDP context activation and not on an incoming call basis. *[Editor's note: When and how often the UE should update application level registration is FFS]* The selected CSCF becomes the serving-CSCF. Note that the S-CSCF can be either in the home or visited network. *[Editor's note: Where the association of the IP address used by the UE and application level identifier is held in the network is FFS.]* From the S-CSCF point of view, the IP address provided by the UE is the address where the UE is reachable for mobile-terminated call control signalling and any other type of mobile terminated signaling.

Whether the procedures are activated individually by the UE or some of them are performed automatically depends on implementation of the terminal and on the UE's configuration. For instance, the multimedia application in the UE could start the application level registration and steps 2-4 would have to be executed in response to support the operation initiated by the application. Interaction with the UE may happen during these steps.

6.3 Location Management

6.3.1 Registration concepts for a R00 Subscriber Roaming Into a Circuit-Switched Network Domain

Figure 6.4 shows the registration concept for a R00 subscriber roaming into a UMTS/GSM CN domain.

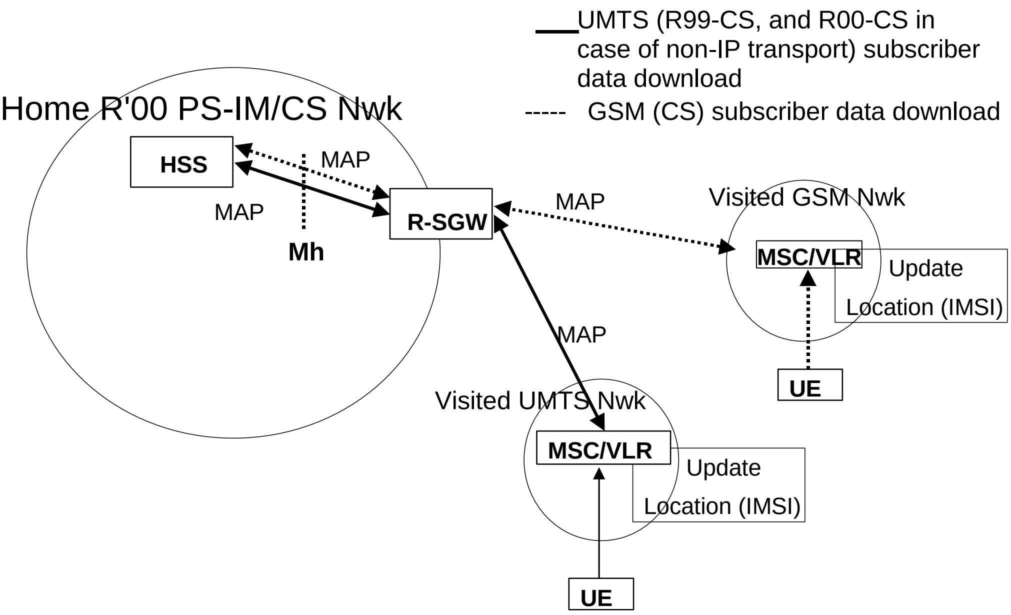

Figure 6.4: A roaming model for registration in a CN domain

The detailed message sequence chart for a UMTS R00 subscriber roaming into a CN domain is shown in figure 6.5.

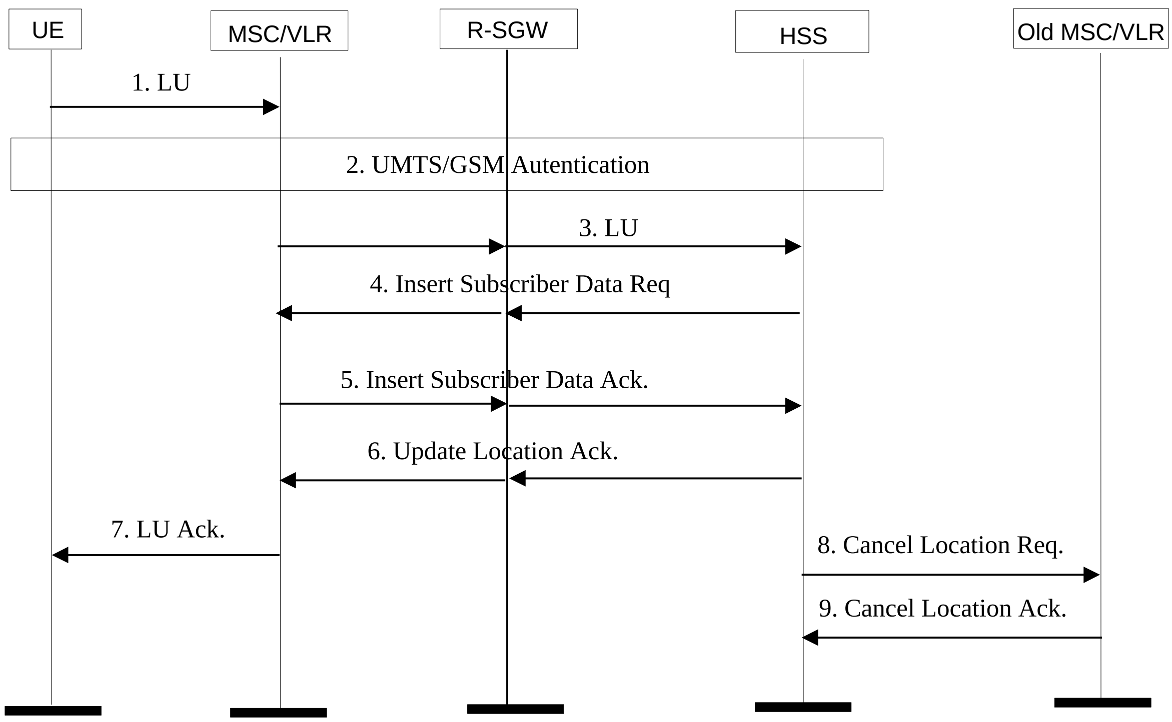

Figure 6.5: Message sequence for roaming into a CN domain

1. The UE initiates the UMTS R99/GSM Location Update procedure with the MSC/VLR of the visited network. The LU message contains the IMSI of the subscriber.

2. The UMTS/GSM authentication is performed as per the existing UMTS R99/GSM specifications.

3. The MSC/VLR initiates the MAP Location Update procedure towards the HSS of the user via R-SGW. The HSS stores the VLR address etc. The message contains IMSI and other parameters as defined in UMTS R99/GSM specifications. The message is passed through the R-SGW transparently while the SS7 to/from IP conversion is performed in R-SGW.

4. The HSS provides the subscriber data for the roaming user to VLR by sending MAP Insert Subscriber Data message via R-SGW. The message contains IMSI and other necessary parameters as defined in the UMTS/GSM specification. The message is passed through the R-SGW transparently while the SS7 to/from IP conversion is performed in R-SGW.

5. The serving VLR then acknowledges the receipt of the subscriber data to the HSS via R-SGW.

6. The HSS acknowledges the completion of location updating procedure to the MSC/VLR via R-SGW.

7. The MSC/VLR acknowledges the completion of location updating procedure to the UE.

8. The HSS sends the MAP Cancel Location message to the old MSC/VLR (optional procedure).

9. Location cancellation is acknowledged to the HSS by the old MSC/VLR.

NOTE 1: The steps 8 and 9 above assume that the UE was previously registered to a CN domain .

NOTE 2: The MAP messages between the MSC/VLR and HSS are passed transparently via R-SGW. The R-SGW does not interpret the MAP messages in anyway, but performs only the lower level conversion between SS7 and IP. This is in accordance with the 3GPP definition for R-SGW.

6.4 Handover

For handover of circuit-switched services involving the change of CN equipment (only CS-MGW or CS-MGW and MSC-server) the anchor principle shall be applied.

- The first MSC Server involved in a call will become the Anchor MSC Server for this call during and after handover , and will remain in the call until the call is released. Every subsequent handover (Intra and Inter) will be controlled by this MSC Server.

- The first CS-MGW involved in a call will become the Anchor CS-MGW for this call during and after handover , and will remain in the call until the call is released. The Nc interface is anchored in the CS-MGW, the correlation between MGW to PSTN and the MGW to UTRAN remain fixed until the call is released.

6.5 Mobility across networks

[Editor's note: this section with deal with e.g. Mobile IP related issues]

7 Application Level Registration

7.1 Requirements considered for Registration

The following points are considered as requirements for the purpose of the registration procedures.

1. The architecture shall allow for the serving CSCFs to have different capabilities or access to different capabilities. E.g. a VPN CSCF or CSCFs in different stages of network upgrade.

2. The network operator shall not be required to reveal the internal network structure to another network. Association of the node names of the same type of entity and their capabilities and the number of nodes will be kept within an operator's network. However disclosure of the internal architecture shall not be prevented on a per agreement basis.

3. A network shall not to expose the explicit IP addresses of the nodes within the network (excluding firewalls and border gateways).

4. It is desirable that the UE will use the same registration procedure(s) within its home and visited networks.

5. It is desirable that the procedures within the network(s) are transparent to the UE, when it register with the IM CN subsystem with either its home or visited CSCF.

6. The serving CSCF understands a service profile and the address of the functionality of the proxy CSCF.

7.2 Registration flows

Annex B presents the detailed application level registration flows and requirements used to define the registration process. This informative Annex is to be used as the basis for further work within SA2.

8 Service Platforms

[Editor's note: this chapter deals withVHE/OSA, SAT, CAMEL etc.]

[Note: The following sections are intended to be included potentially in a new R00 specification on IP multimedia (proposed chapter, if any):

- 7.2]

8.1 Location Services

8.2 VHE

In order to allow the support of existing CAMEL based services, and to allow the development of new services independent of network domain, the home CSCF should support a CAP interface. In this case operators could then choose for their subscribers to register to the vCSCF in networks that also support CAMEL. This situation is similar to that in GSM today.

NOTE: The exact implementation is dependent upon the agreed service architecture

However in the case where the visited network does not support CAMEL or the capabilities to support a given service then it shall be possible to provide call control in the hCSCF. This would mean that either the user is registered with the hCSCF directly, or if the user is registered in the vCSCF, then the vCSCF shall be able to forward the call set up request to the hCSCF. This case shall also be supported for operators that choose to have all of their subscribers (including roamers) supported by the hCSCF.

9 Multimedia

[Editor's note: this chapter deals with multimedia related issues such asSIP, H.324, their impact on the reference architecture etc.]

[Note: The following sections are intended to be included potentially in a new R00 specification on IP multimedia (proposed chapter, if any):

- 8.1
- 8.2]

9.1 Signalling

A Single call control between the UE and CSCF. For MultiMedia type services delivered via the PS Domain within the R00 architecture, a single call control protocol shall be used between the user equipment UE and the CSCF (over the Gm reference point).

Protocols over the Gm reference point. The single protocol applied between the UE and CSCF (over the Gm reference point) within the R00 architecture will be based on SIP (as defined by RFC 2543, other relevant RFC's, and additional enhancements required to support 3GPP's needs).

A Single call control on the Mw, Mm, Mg. A single call control protocol shall be used on the call control interfaces between MGCF and CSCF, between CSCFs within one operator's network and between CSCFs in different operators' networks.

Protocols for the Mw, Mm, Mg. The single call control protocol applied to the interfaces between MGCF and CSCF, between CSCFs within one operator's network and between CSCFs in different operator's networks will be based on SIP (as defined by RFC 2543, other relevant RFC's, and additional enhancements required to support 3GPP´s needs).

UNI vs. NNI call control. The SIP based signalling interactions between CN elements may be different then SIP based signalling between the UE and the CSCF.

9.2 Support of Roaming Subscribers

The Release 2000 architecture shall be based on the principle that the service control for a roaming subscriber is designated by the Home network.

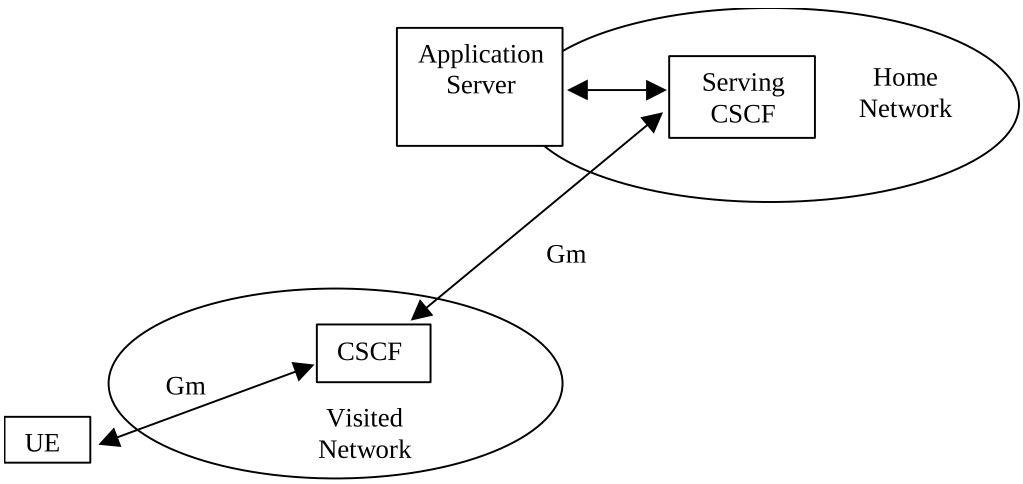

Figure 9.1: Support of a UE via Serving CSCF in Home Network

The serving CSCF can be located either in the Home network (see figure 9.1) or in the visited network (see figure 9.2). This assignment of the serving CSCF is designated by the Home network during the registration of the UE at the visited network.

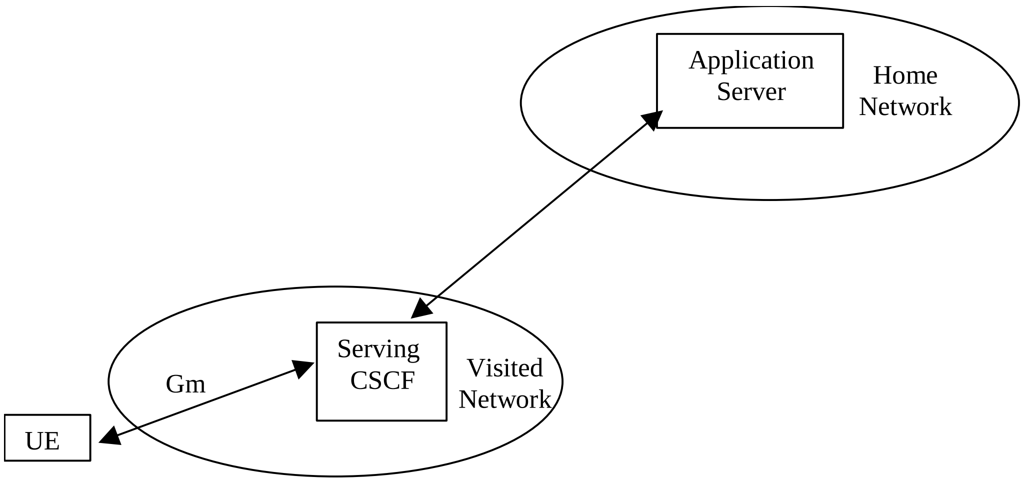

Figure 9.2: Support of the UE via Serving CSCF in the Visited Network

The R00 standards shall support roaming for IM users between operators. To achieve roaming a serving CSCF is required.The serving CSCF can be located in the visited network or in the home network. The decision as to whether the UE is served by a serving CSCF in the home network or a serving CSCF in the visited network is made by the home network.

- When subscribers roam to networks where serving CSCF is not offered, the roamed to (visited) network must support a proxy CSCF. The proxy CSCF will enable the call control to be passed to the home network based serving CSCF which will provide service control.
- When subscribers roam to networks where a serving CSCF is offered but the home network decides to use a home network based serving CSCF, the roamed to (visited) network must support a proxy CSCF. The proxy CSCF will enable the call control to be passed to the home network based serving CSCF which will provide service control.
- When subscribers roam to networks where a serving CSCF is offered and the home network decides to use the visited network based serving CSCF solution, the visited network serving CSCF may be used to provide service control to the roamed subscriber.

The visited network may support serving CSCF for inbound roamers.

The visited network shall support proxy CSCF for inbound roamers.

If a visited network decides not to offer serving CSCF capability for inbound roamers, then the home network shall provide a serving CSCF to support IM Roaming.

The home network may provide a serving CSCF for outbound roamers even when a visited network offers the support of a serving CSCF (in this case the visited network provides proxy CSCF).

When users are within their home network, a home network based serving CSCF provides service control. If the home operator wishes to use home service control for outbound roamers, then a home network based serving CSCF shall be used for outbound roamers' service control.

9.2.1 Assignment of Serving CSCF

The home network shall designate the serving CSCF in the home network or with the help of the visited network, request a serving CSCF in the visited network. This selection is done on a per subscriber basis at registration time based on consideration of at least the following factors:

a) The service capabilities and toolkits supported by the visited network and the home network

b) The subscription profile of the subscriber.

9.3 Transcoder

10 QoS

[Note: The following sections are intended to be included in TS 23.107 (proposed chapter, if any):

- 9.1.1 (new Chapter 4.4)
- 9.1.2 (new Chapter 4.5)
- 9.2 (Chapter 6.2)
- 9.3 (Chapter 6.4.3.1)]

10.1 QoS Requirements

10.1.1 End-to-End QoS Negotiation Requirements

- The UMTS QoS negotiation mechanisms used for providing end-to-end QoS in UMTS Release 2000 shall be backward compatible with UMTS Release 99.
- The UMTS QoS negotiation mechanisms used for providing end-to-end QoS shall not make any assumptions about the situation in external networks which are not within the scope of 3GPP specifications.
- The UMTS QoS negotiation mechanisms used for providing end-to-end QoS shall not make any assumptions about application layer signalling protocols.
- No changes to non-UMTS specific QoS negotiation mechanisms.
- The UMTS QoS negotiation mechanisms used for providing end-to-end QoS shall not make any assumptions about applications which may be used on terminal equipment attached to mobile terminals.
- Unnecessary signalling complexity and processing complexity in the network elements as well as the mobile terminal shall be avoided.
- Unnecessary signalling traffic due to end-to-end QoS negotiation shall be avoided.
- Methods for user authentication as well as billing and charging mechanisms related to the end-to-end QoS negotiation shall be kept as simple as possible.
- Minimum changes to network architecture and mechanisms due to introduction of end-to-end QoS negotiation.
- The UMTS network shall be able to negotiate end-to-end QoS also for mobile terminals and applications which are not able to use QoS negotiation mechanisms other than the ones provided by UMTS.

10.1.2 QoS Policy Requirements

- The UMTS policy mechanisms described in TS 23.060 shall be used for control of the UMTS bearers.
- Interaction between UMTS bearer services and IP bearer services shall only occur at the translation function in the UE and GGSN.

NOTE: The following general guidelines shall apply [Editor's note: these notes will not be included in the normative portion of the specifications]:

- The IP policy framework employed in UMTS shall, as far as possible, conform to IETF "Internet Standards". The IETF policy framework may be used for policy decision, authorization, and control of the IP level functionality, at both user and network level.
- There shall be separation between the scope and roles of the UMTS policy mechanisms and the IP policy framework. This is to facilitate separate evolution of these functions.

10.2 QoS End-to-End Functional Architecture

To provide QoS end-to-end, it is necessary to manage the QoS within each domain. An IP BS Manager is used to control the external IP bearer service. Due to the different techniques used within the IP network, this communicates to the UMTS BS manager through the Translation function.

To enable coordination between events in the application layer and resource management in the IP bearer layer, an element called IP Policy Control is used as a logical policy decision element. It is also possible to implement a policy decision element internal to the IP BS Manager in the GGSN. The IP policy architecture does not mandate the policy decision point to be external to the GGSN.

Whenever resources not owned or controlled by the UMTS network are required to provide QoS, it is necessary to interwork with an external resource manager that controls those resources.

IP BS Manager

The IP BS Manager uses standard IP mechanisms to manage the IP bearer service. These mechanisms may be different from mechanisms used within the UMTS, and may have different parameters controlling the service. The translation/mapping function provides the interworking between the mechanisms and parameters used within th e UMTS and the external IP bearer service, and interacts with the IP BS Manager.

If an IP BS Manager exists both in the UE and the Gateway node, it is possible that these IP BS Managers communicate directly with each other by using relevant signalling protocols.

The required options in the table define the minimum functionality that shall be supported by the equipment in order to allow multiple network operators to provide interworking between their networks for end-to-end QoS. Use of the optional functions listed below, other mechanisms which are not listed (eg over-provisioning), or combinations of these mechanisms are not precluded from use between operators.

The IP BS Managers in the UE and GGSN provide the set of capabilities for the IP bearer level as shown in Table 9-1. Provision of the IP BS Manager is optional in the UE, and required in the GGSN.

Table 9.1: IP BS Manager capability in the UE and GGSN

Capability	UE	GGSN
DiffServ Edge Function	Optional	Required
RSVP/IntServ	Optional	Optional
IP Policy Enforcement Point	Optional	Required (*)

(*) Although the capability of IP policy enforcement is required within the GGSN, the control of IP policy through the GGSN is a network operator choice. Where the APN is not located at the GGSN, the location of policy enforcement point is for further investigation.

IP Policy Control

The IP Policy Control is a logical policy decision element which uses standard IP mechanisms to implement policy in the IP bearer layer. These mechanisms may be conformant to, for example, the framework defined in IETF [RFC2573] "A Framework for Policy-based Admission Control" where the IP Policy Control is effectively a Policy Decision Point (PDP). The IP Policy Control makes decisions in regard to network based IP policy using policy rules, and communicates these decisions to the IP BS Manager in the GGSN, which is the IP Policy Enforcement Point (PEP).

A protocol interface between the IP Policy Control and application servers/proxies (e.g. local SIP proxy) supports the transfer of policy related information from the application layer to the policy decision point. *[Editor's note: The exact mechanisms, protocols whether proprietary or standardized, and how they are used are for further study.]*

A protocol interface between the IP Policy Control and GGSN supports the transfer of information and policy decisions between the policy decision point and the IP BS Manager in the GGSN. *[Editor's note: The exact mechanisms, protocols whether proprietary or standardized, and how they are used are for further study. One possible candidate is the COPS protocol [RFC2748] which describes a simple query and response protocol that can be used to exchange policy information between a policy server (PDP) and its client (PEP). Where RSVP is used as the signalling protocol in the IP bearer level, a COPS protocol variant carrying embedded RSVP information, i.e., COPS-RSVP, defined in [RFC2749] may be used.]*

The IP Policy Control bases policy decisions only on information obtained from nodes / elements within its domain or from nodes with which it has a trust relationship. The IP Policy Control needs to be in the same domain as the GGSN or have a trust relationship with the GGSN.

NOTE 1: Currently in IETF, inter-domain policy interactions are not defined.

NOTE 2: The security issues regarding the trust relationship between the nodes / elements is outside the scope of this chapter.

[Editor's note: Additionally, the IP Policy Control may have protocol interfaces to other devices (e.g., AAA, bandwidth broker) which support transfer of information (e.g., authentication, availability of resources, etc.) for use in policy decisions. These are for further study.]

[Editor's note: Where the access point of the APN is not located at the GGSN, the location of policy enforcement point is for further investigation. The IP policy architecture for cases where the access point of the APN is located in a third party network, e.g., a corporate network, is for further study.]

Resource Manager

Within the UMTS network, there is resource management performed by various nodes in the admission control decision. The resources considered here are under the direct control of the UMTS network.

In IP Networks, it is also necessary to perform resource management to ensure that resources required for a service are available. Where the resources for the IP Bearer Service to be managed are not owned by the UMTS network, the resource management of those resources would be performed through an external resource management function for the IP network.

In addition, where the UMTS network is also using external IP network resources as part of the UMTS bearer service (for example for the backbone bearer service), it may also be necessary to interwork with an external IP resource manager.

[Editorial Note: The following needs further clarification: (1) the functional split between the IP BS Manager and Resource Manager, and between the IP Policy Control and Resource Manager, (2) the exact location and control scope of the Resource Manager, (3) the interface between the IP BS Manager and the Resource Manager, the exact mechanisms, protocols whether proprietary or standardized, and how it is used.]

Figure 10.1 shows the scenario for control of an IP service using IP BS Managers in both possible locations in the UE and Gateway node and an external Resource Manager. The figure also indicates the optional communication path between the IP BS Managers in the UE and the Gateway node.

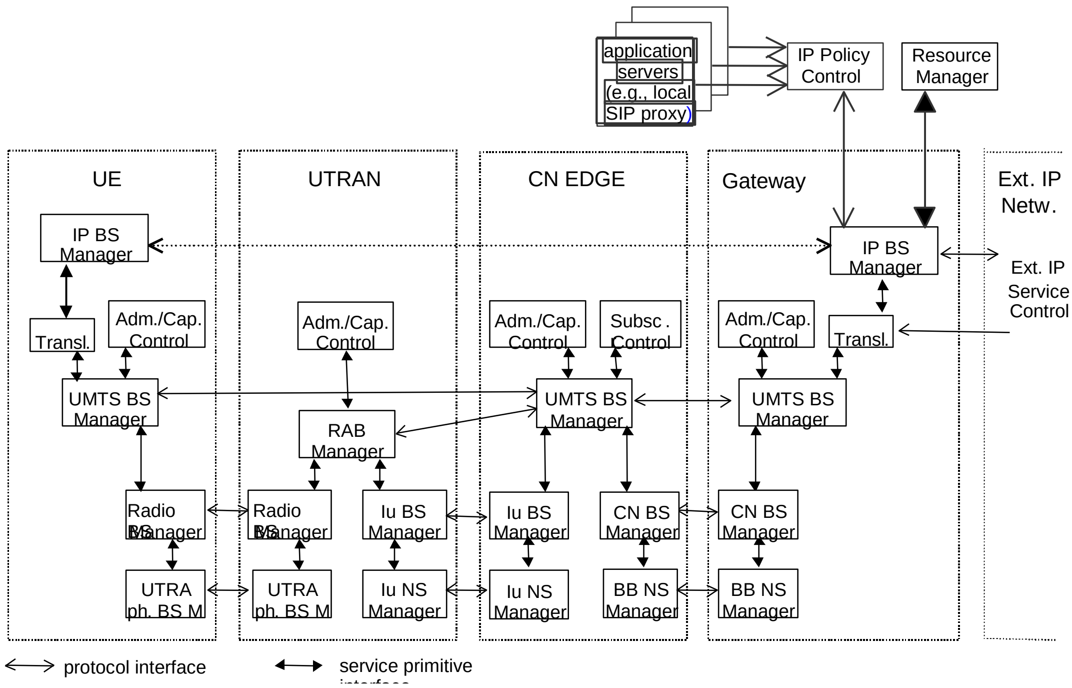

Figure 10.1: QoS management functions for UMTS bearer service in the control plane for an external IP Service

NOTE: This does not cover the cases of a circuit switched service, or an IP service interworking with an ATM service at the gateway node.

[Editor's note: The actual split of the UE into separate elements (as described in TS 23.002 and TS 24.002) as well as the terminology regarding the UE elements and the distribution of functionalities between the UE elements is for further study. The modeling of the UE in TS 23.107 is not in line with TS 23.002 and TS 24.002, which makes this clarification necessary.]

[Editor's note: Elements external to the nodes are used to highlight and explain possible solutions to requirements that have been identified. If elements or interfaces are specified or mandated within 3GPP, they shall be included in the Reference Architecture.]

10.3 UMTS Bearer Service Parameters

One additional QoS parameter has been defined for the R00 UMTS bearer service:

Source statistics descriptor ('speech'/'unknown')

Definition: specifies characteristics of the source of submitted SDUs.

[Purpose: Conversational speech has a well-known statistical behaviour (or the discontinuous transmission (DTX) factor). By being informed that the SDUs for a UMTS bearer are generated by a speech source, UTRAN, the SGSN and the GGSN may, based on experience, calculate a statistical multiplex gain for use in admission control on the relevant interfaces.]

[Editor's note: The number of different source statistics descriptors that should be allowed is FFS.]

11 Transport

[Editor's note: this chapter deals with user and control plane transport issues for relevant interfaces]

[NOTE: The following sections are intended to be included in 23.121 (proposed chapter, if any):

- 10.1]

11.1 IP Version Issues

The R00 architecture will be designed to support Ipv4 / Ipv6 based on the statements below.

- IP transport between network elements of the IP Connectivity services (between RNC, SGSN and GGSN) and IP transport for the CS Domain.
  - Both Ipv4 / Ipv6 are already options within R99 for IP connectivity. No change moving to R00
- IP Multimedia CN subsystem elements (UE to CSCF and the other elements e.g. MRF):
  - The architecture shall make optimum use of Ipv6.
  - The R00 IM CN subsystem shall exclusively support Ipv6.
  - The R00 UE shall exclusively support Ipv6 for the connection to R00 IM services.

    [Editor's note: The exact set of the functionality available in the whole Ipv6 protocol suite (such as IPSec, IP multicast etc.) that will be mandated in R00 standards is FFS.]
- Access to existing data services (Intranet, Internet,…):
  - The UE shall be able to access Ipv4 and Ipv6 based services.

12 Point-to-Multipoint

13 Security

14 Charging

15 UTRAN Aspects

[Editor's note: requirements on UTRAN from a system perspective]

16 BSS Aspects

17 Alternative Access Networks

[Editor's note: this chapter deals with system aspects relating to other access tehnologies than UTRAN, e.g. EDGE and Hiperlan2]

18 Multi-mode

[Editor's note: this chapter deals with issues in relation to the handling of multimode terminals]

19 Compatibility

[Editor's note: this chapter deals with compatibility issues between different releases, and between different options]

20 Work Plan

[Editor's note: an overall workplan is specified here]

An overall work plan for R00 may be found in TR 30.801 v.1.1.0.

Annex A (Informative): QoS Conceptual Models

A.1 Introduction

There are many different end-to-end scenarios that may occur from a UE connected to a UTMS network. The following examples depict how end-to-end QoS will be delivered for a number of scenarios that are considered to be significant.

In all the scenarios presented below, the network architecture is as shown in figure A.1 below.

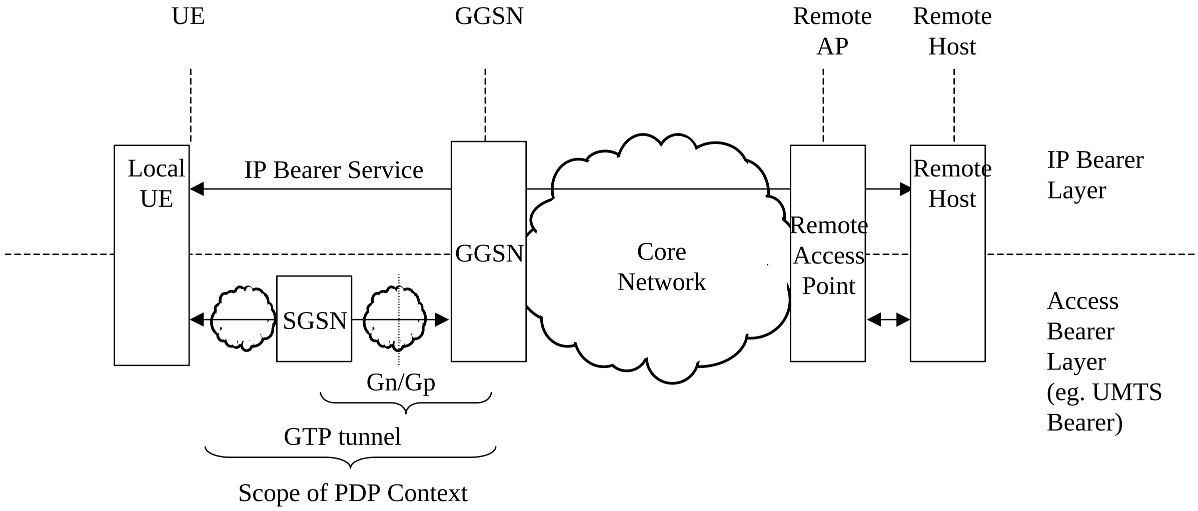

Figure A.1: Network Architecture

Notes:

- Although the core network is shown as a single domain, it may consist of a number of separate domains.
- The structure of the Local UE is not specified. It includes cases from a simple host, to a gateway to a network such as a LAN. If the UE is acting as a gateway, it is responsible for providing the IP BS Management towards the extended network.
- The remote side is shown as a simple host. Other more complex cases on the remote side such as a private LAN with over-provisioning, or possibly LAN priority marking, and DiffServ and/or RSVP capable routing elements is not depicted. It is envisaged however that interworking between the QoS mechanisms in a more complex remote user side could also be performed with some similarities to the mechanisms shown at the local side.
- The GGSN and the APN are co-located in these scenarios.

The reference point shown at the UE is at the interface to the UE. Within the UE, the QoS control could be derived from any of the mechanisms that occur across that reference point, or it could use a different mechanism internally.

Although the scenarios currently identified are mainly using DiffServ in the core network (RSVP is indicated as an alternative in scenario 4), it is not mandated that DiffServ must be used in the core network. Other mechanisms, for example, over-provisioning and aggregated RSVP may be used.

A.2 Scenarios

[Editorial Note: the precedence and sequence of the different phases of session / bearer establishment need further study.]

[Editorial Note: note that the notion of "core network" is according to figure A.1 which is not fully in line with the main body of this TR.]

NOTE: Scenario 5 and 6 is reserved for the Release 2000 IP multimedia services involving, e.g., SIP signalling , IP policy control, and subscription checking.

A.2.1 Scenario 1

The UE does not provide an IP BS Manager. The end-to-end IP QoS bearer service towards the remote terminal is controlled from the GGSN.

The scenario assumes that the GGSN supports DiffServ edge functions, and the core network is DiffServ enabled.

In this scenario, the control of the QoS over the UMTS access network (from the UE to the GGSN) may be performed either from the terminal using the PDP context signalling, or from the SGSN by subscription data.

The IP QoS for the downlink direction is controlled by the remote terminal up to the GGSN. The GGSN will apply receiver control DiffServ edge functions and can reclassify the data (remarking the DiffServ Code Point (DSCP)). This may affect the QoS applied to the data over the UMTS access (the TFT may use the DSCP to identify the data to be allocated to the PDP context).

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the core network, and DiffServ in the remote access network in the scenario shown in the figure below. The GGSN provides the interworking between the PDP context and the DiffServ function. However, the interworking may use information about the PDP context which is established, or be controlled from static profiles, or dynamically through other means such as proprietary HTTP based mechanisms. The UE is expected to be responsible for the control of the PDP context, but this may instead be controlled from the SGSN by subscription.

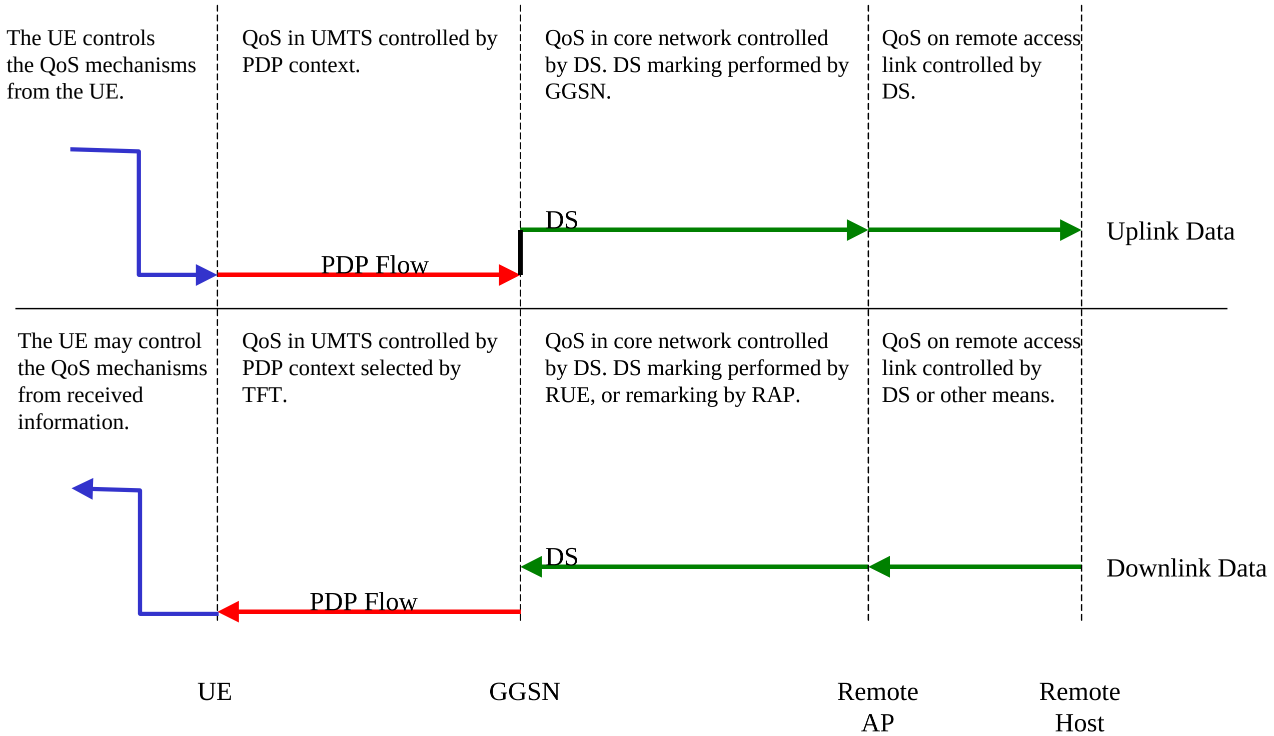

Figure A.2: Local UE does not provide IP BS Manager

Notes:

- The solid horizontal lines indicate the mechanism that is providing QoS for the flow of data in the direction indicated.
- The dashed horizontal lines indicate where QoS control information is passed that is not directly controlling the QoS in that link/domain.
- The arrows on the horizontal lines indicate nodes that receive information about QoS from that mechanism, even if that mechanism is not used to control the QoS over that link/domain.
- The solid vertical lines indicate interworking between the different mechanisms.

No solid vertical line is shown from DiffServ to PDP flow on the downlink at the GGSN. The TFT determines the QoS applicable over the UMTS access. However, the configuration of the TFT may use the DiffServ to select the PDP context to be applied, so there may be interworking between DiffServ and the PDP Flow via the TFT filters.

A.2.2 Scenario 2

The UE performs an IP BS function which enables end-to-end QoS without IP layer signalling towards the IP BS function in the GGSN, or the remote terminal.

The scenario assumes that the UE and GGSN support DiffServ edge functions, and that the core network is DiffServ enabled.

In this scenario, the control of the QoS over the UMTS access network (from the UE to the GGSN) may be performed either from the terminal using the PDP context signalling. Alternatively, subscription data accessed by the SGSN may override the QoS requested via signalling from the UE.

In this scenario, the terminal supports DiffServ to control the IP QoS through the core network.

The IP QoS for the downlink direction is controlled by the remote terminal up to the GGSN. The PDP context controls the QoS between the GGSN and the UE. The UE may apply DiffServ edge functions to provide the DiffServ receiver control. Otherwise, the DiffServ marking from the GGSN will determine the IP QoS applicable at the UE.

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the core network, and DiffServ in the remote access network in the scenario shown in figure A.3 below. The UE provides control of the DiffServ, and therefore determines the appropriate interworking between the PDP context and DiffServ.

The GGSN DiffServ edge function may overwrite the DSCP received from the UE, possibly using information regarding the PDP context which is signalled between the UMTS BS managers and provided through the translation/mapping function to the IP BS Manager.

Note that DiffServ control at the Remote Host is shown in this example. However, other mechanisms may be used at the remote end, as demonstrated in the other scenarios.

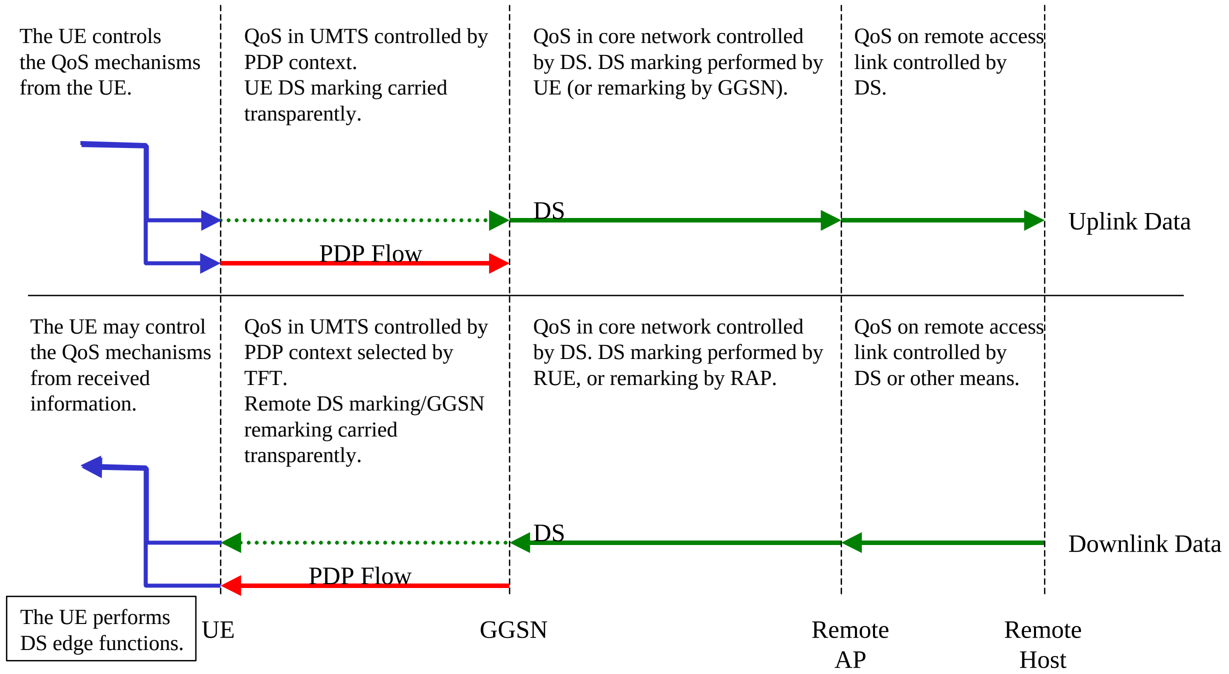

Figure A.3: Local UE supports DiffServ

A.2.3 Scenario 3

The UE performs an IP BS function which enables end-to-end QoS using IP layer signalling towards the remote end. There is no IP layer signalling between the IP BS Managers in the UE and the GGSN. However, the GGSN may make use of information regarding the PDP context which is signalled between the UMTS BS managers and provided through the translation/mapping function.

This scenario assumes that the UE and GGSN support DiffServ edge functions, and that the core network is DiffServ enabled. In addition, the UE supports RSVP signalling which interworks within the UE to control the DiffServ.

In this scenario, the control of the QoS over the UMTS access network (from the UE to the GGSN) may be performed either from the terminal using the PDP context signalling. Alternatively, subscription data accessed by the SGSN may override the QoS requested via signalling from the UE.

In this scenario, the terminal supports signalling via the RSVP protocol to control the QoS at the local and remote accesses, and DiffServ to control the IP QoS through the core network. The RSVP signalling protocol may be used for different services. It is only expected that RSVP using the Integrated Services (IntServ) semantics will be supported. It is only expected that only RSVP using the Integrated Services (IntServ) semantics would be supported, although in the future, new service definitions and semantics may be introduced. The entities that are supporting the RSVP signalling may fully support the specifications for IntServ and IntServ/DiffServ interwork. If not, they are expected to set the break bit.

The QoS for the wireless access is provided by the PDP context. The UE may control the wireless QoS through signalling for the PDP context. The characteristics for the PDP context may be derived from the RSVP signalling information, or may use other information.

QoS for the IP layer is performed at two levels. The end-to-end QoS is controlled by the RSVP signalling. Although RSVP signalling can be used end-to-end in the QoS model, it is not necessarily supported by all intermediate nodes. Instead, DiffServ is used to provide the QoS throughout the core network.

At the UE, the data is also classified for DiffServ. Intermediate QoS domains may apply QoS according to either the RSVP signalling information or DiffServ mechanisms. In this scenario, the UE is providing interworking between the RSVP and DiffServ domains. The GGSN may override the DiffServ setting from the UE. This GGSN may use information regarding the PDP context in order to select the appropriate DiffServ setting to apply, as shown in the figure below.

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the core network, and DiffServ in the remote access network in the scenario shown in figure A.4 below. The RSVP signalling may control the QoS at both the local and remote accesses. This function may be used to determine the characteristics for the PDP context, so the UE may perform the interwork between the RSVP signalling and PDP context.

The UE provides control of the DiffServ (although this may be overwritten by the GGSN), and in effect, determines the appropriate interworking between the PDP context and DiffServ.

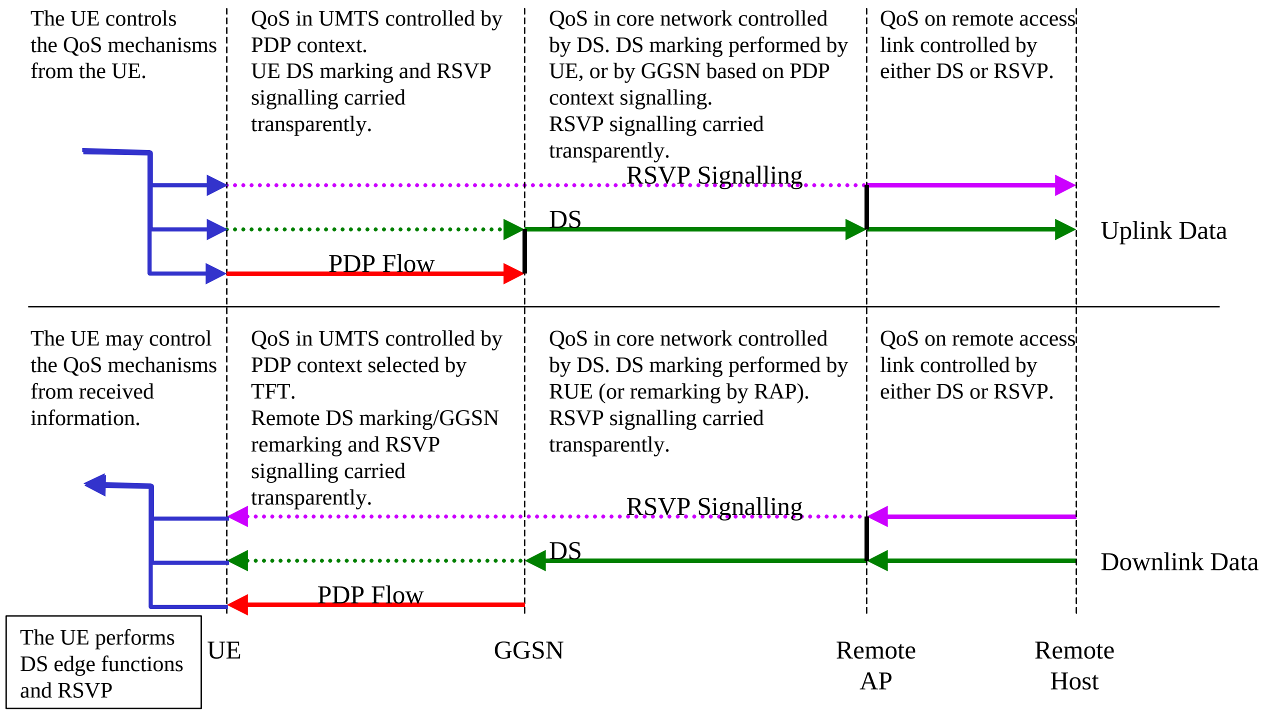

Figure A.4: Local UE supports RSVP signalling with IntServ semantics, and DiffServ

A.2.4 Scenario 4

The UE performs an IP BS function which enables end-to-end QoS using IP layer signalling towards the remote end. However, the UE relies on this end-to-end communication being utilised by at least the access point (GGSN) in order to provide the end-to-end QoS.

This scenario assumes that the UE and GGSN support RSVP signalling which may control the QoS directly, or interwork with DiffServ. The core network is RSVP and/or DiffServ enabled.

In this scenario, the terminal supports signalling via the RSVP protocol to control the QoS across the end-to-end path. The GGSN also supports the RSVP signalling, and uses this information rather than the PDP context to control the QoS through the core network. The control of the QoS through the core is expected to be supported through interworking with DiffServ at the GGSN, althopugh it may optionally be supported by per flow resource reservation. The RSVP signalling protocol may be used for different services. It is only expected that only RSVP using the Integrated Services (IntServ) semantics would be supported, although in the future, new service definitions and semantics may be introduced. The entities that are supporting the RSVP signalling may fully support the specifications for IntServ and IntServ/DiffServ interwork. If not, they are expected to set the break bit.

In this scenario, the control of the QoS over the UMTS access network (from the UE to the GGSN) may be performed either from the terminal using the PDP context signalling. Alternatively, subscription data accessed by the SGSN may override the QoS requested via signalling from the UE.

QoS for the IP layer is performed at two levels. The end-to-end QoS is controlled by the RSVP signalling. Although RSVP signalling occurs end-to-end in the QoS model, it is not necessarily supported by all intermediate nodes. DiffServ is used to provide the QoS throughout the core network, although optionally each node may support RSVP signalling and allocation of resources per flow.

The GGSN supports the RSVP signalling and acts as the interworking point between RSVP and DiffServ. Intermediate QoS domains may apply QoS according to either the RSVP or DiffServ mechanisms.

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the core network, and RSVP in the remote access network in the scenario shown in figure A.5 below. The RSVP signalling may control the QoS at the local access. This function may be used to determine the characteristics for the PDP context, so the UE may perform the interwork between RSVP and the PDP context.

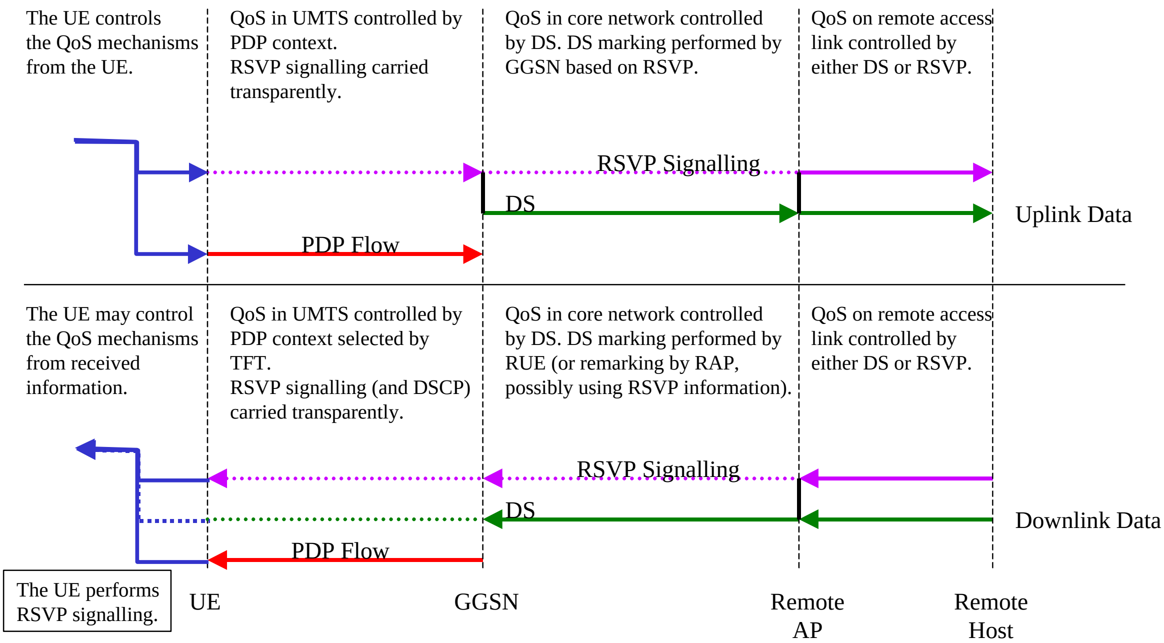

Figure A.5: Local UE supports RSVP signalling using IntServ Semantics

A.2.5 Scenario 5

The UE performs an IP BS function which enables end-to-end QoS without IP layer signalling and negotiation towards the IP BS function in the GGSN, or the remote host. The UE provides IP specific information to the GGSN, using IP specific elements of the PDP context activation/modification message, to enhance the interworking options to the DiffServ edge function of the GGSN.

The scenario assumes that the GGSN support DiffServ edge functions, and that the core network is DiffServ enabled.

The GGSN DiffServ edge function may use the IP specific information for the DiffServ classifier functionality, e.g., 5-tuple combination of source and destination IP address, source and destination port number, and the protocol identifier. The information can also be used for DiffServ class admission control, e.g., the requested end-to-end bandwidth from the UE for a particular flow may be informed to the GGSN beforehand for the GGSN DiffServ edge to determine if the flow can be allowed to a certain DiffServ class or an egress point. As a result, the GGSN may select the appropriate DiffServ setting to apply. This is shown in the figure below.

There exist IP specific elements of PDP context activation/modification message that are transferred from the UE to the GGSN. The elements are discussed in Appendix D.

In this scenario, the control of the QoS over the UMTS access network (from the UE to the GGSN) may be performed from the terminal using the PDP context signalling. Alternatively, subscription data accessed by the SGSN may override the QoS requested via signalling from the UE.

TheQoS for the downlink direction is controlled by the remote host from the remote network to the GGSN. The PDP context controls the UMTS level QoS between the GGSN and the UE. The QoS in the uplink direction is controlled by the PDP context up to the GGSN. The GGSN uses the IP specific elements of UMTS signalling to interwork with DiffServ in the core network and controlling the IP QoS bearer service towards the remote -host.

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the core network, and DiffServ in the remote access network. Note that DiffServ control at the Remote Host is shown in this example. However, other mechanisms may be used at the remote end, as demonstrated in the other scenarios.

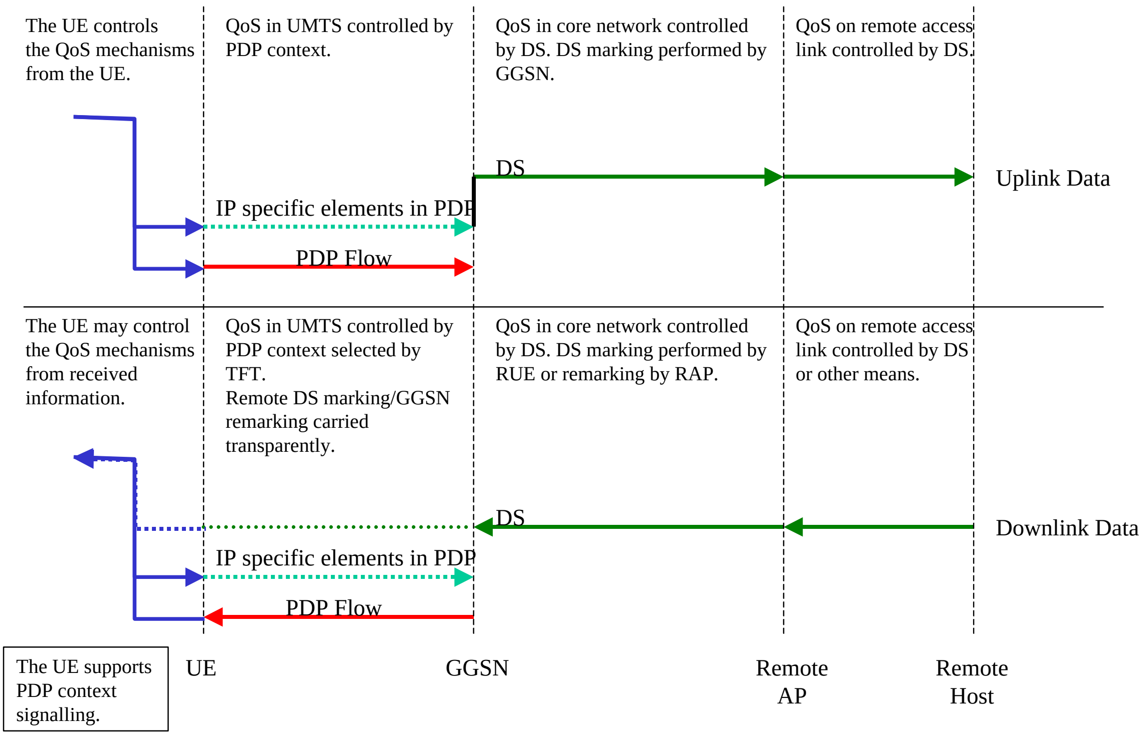

Figure A.6: Local UE supports IP specific elements in PDP context activation/modification message and GGSN provides interworking with DiffServ

A.2.6 Scenario 6

The UE performs an IP BS function which enables end-to-end QoS without IP layer signalling and negotiation towards the IP BS function in the GGSN, or the remote host. The UE provides IP level end-to-end QoS information to the GGSN, using IP specific elements of the context activation/modification message , to enhance the interworking options to an RSVP function in the GGSN. The end-to-end IP QoS bearer service towards the remote host is controlled from the GGSN.

The scenario assumes that the GGSN supports DiffServ edge functions, and the core network is DiffServ enabled. This scenario does not preclude the core network from having RSVP non-transparent routers.

The GGSN may use the IP specific elements in PDP context activation/modification messageto invoke RSVP messages to setup the uplink as well as the downlink flows in the core network up to the remote host. For example, in the uplink direction, the GGSN may use the IP specific elements in PDP context activation/modification message to generate the RSVP Path messages, with the desired QoS / traffic specification, to the specified destination IP address. Also, the GGSN DiffServ edge function may use the IP specific elements in PDP context activation/modification messageto select the appropriate DiffServ setting to apply. This is shown in the figure below.

There exist IP specific elements of PDP context activation/modification message that is transferred from the UE to the GGSN. The elements are discussed in Appendix D.

In this scenario, the control of the QoS over the UMTS access network (from the UE to the GGSN) may be performed either from the terminal using the PDP context signalling. Alternatively, subscription data accessed by the SGSN may override the QoS requested via signalling from the UE.

The QoS for the downlink direction is controlled by the PDP context between the UE and the GGSN. The GGSN terminates the RSVP signalling received from the remote host, and may use the information in theIP specific elements in PDP context activation/modification message when processing RSVP. The QoS in the uplink direction is controlled by the PDP context up to the GGSN. The GGSN may use the IP specific elements in PDP context activation/modification message to provide the interworking with RSVP towards the remote host. The IP specific elements in PDP context activation/modification message may allow for the establishment of the RSVP session..

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the core network, and RSVP in the remote access network.

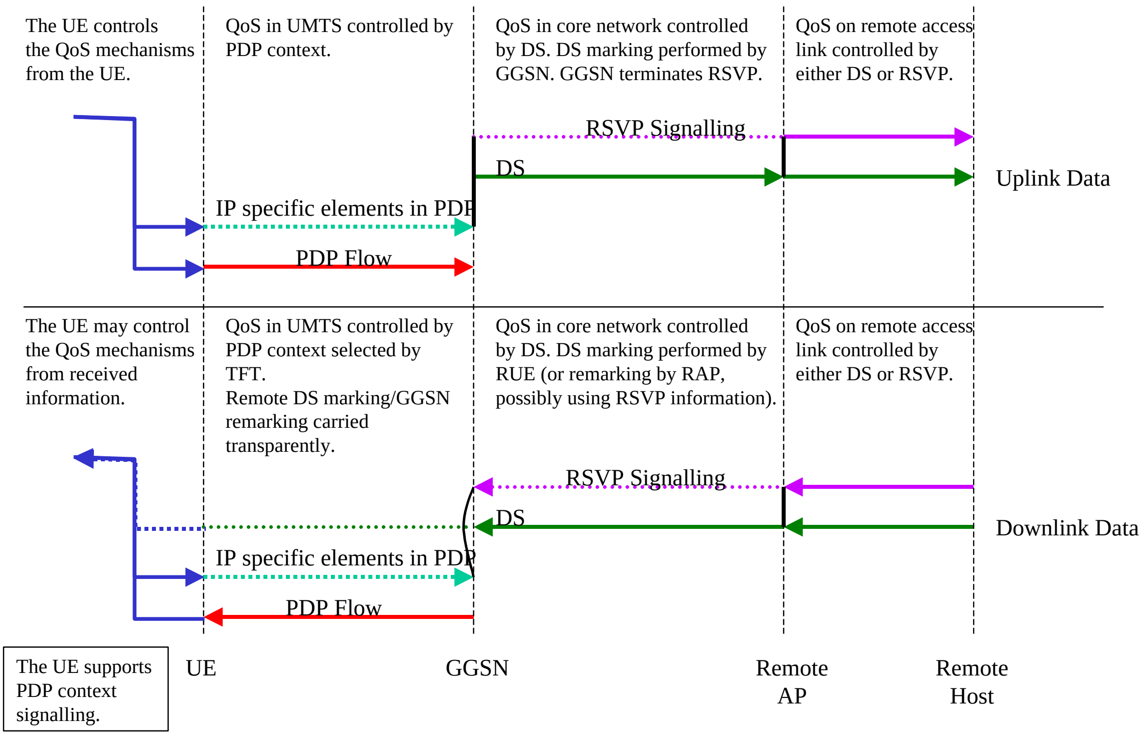

Figure A.7: Local UE supports IP specific elements in PDP context activation/modification message and GGSN provides interworking with RSVP

A.3 RSVP Usage for End-to-End QoS in UMTS

This section contains typical RSVP usage for end-to-end QoS which is applicable to UMTS networks. It aims to convey the general cases when RSVP is used as IP layer signalling protocol from the UMTS network to the remote end terminal to enable end-to-end QoS.

Clarification of terminology:

RSVP transparent – describes the case where GGSN is transparently relaying the RSVP messages, i.e., the GGSN does not process any RSVP message.

RSVP non transparent – describes the case where the GGSN processes RSVP message. (For example the GGSN may maintain RSVP soft states, and/or may use QoS information derived to interwork with other QoS mechanisms (e.g., DiffServ, PDP context), and may forward RSVP messages onwards.)

NOTE: It is assumed that there is an existing PDP context that carries signalling (e.g., SIP or RSVP) between the UE and GGSN.

A.3.1 RSVP in Scenarios 3 and 4

In Scenarios 3 and 4, the UE is supporting RSVP enabled applications. In order to provide QoS over the UMTS segment in an appropriate manner for the end-to-end IP QoS requested through RSVP, the UE shall examine the RSVP signalling and use this information to control the activation/modification of the PDP context as shown in figures A.8 and A.9 below. The UE must not reply with RSVP RESV before the PDP context resources is setup.

Figures A.8 and A.9 do not preclude the case where the GGSN is RSVP transparent as shown in Scenario 3.

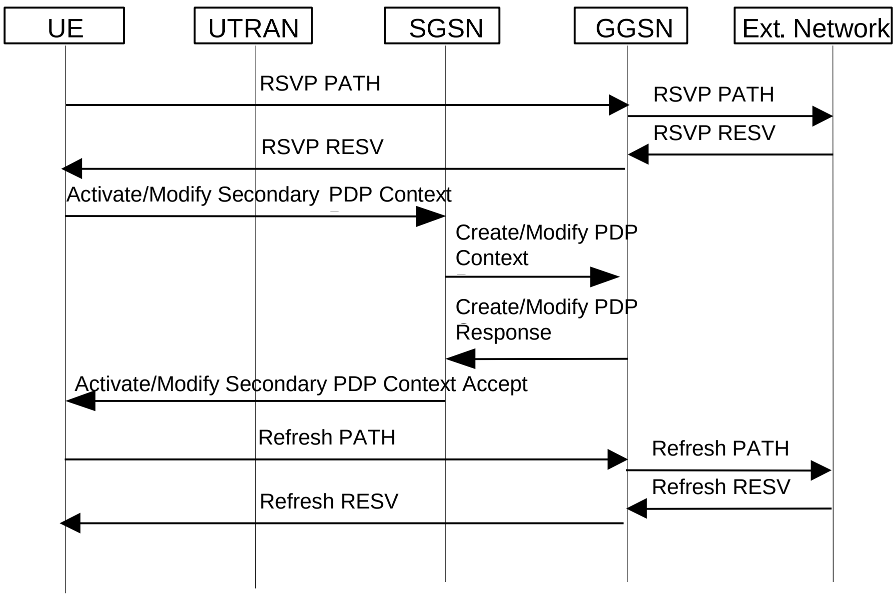

Figure A.8: UE supports RSVP signalling for the uplink flow

NOTE The above diagram depicts only one possible signalling sequence, depending on UE implementation decision, other alternative signalling sequences are:

- to trigger the Activate/Modify Secondary PDP Context when the PATH message is generated by the UE (either directly or after some timeout) without waiting for the arrival of the RESV message.
- to trigger the Activate/Modify Secondary PDP Context before the PATH message is forwarded by the UE.

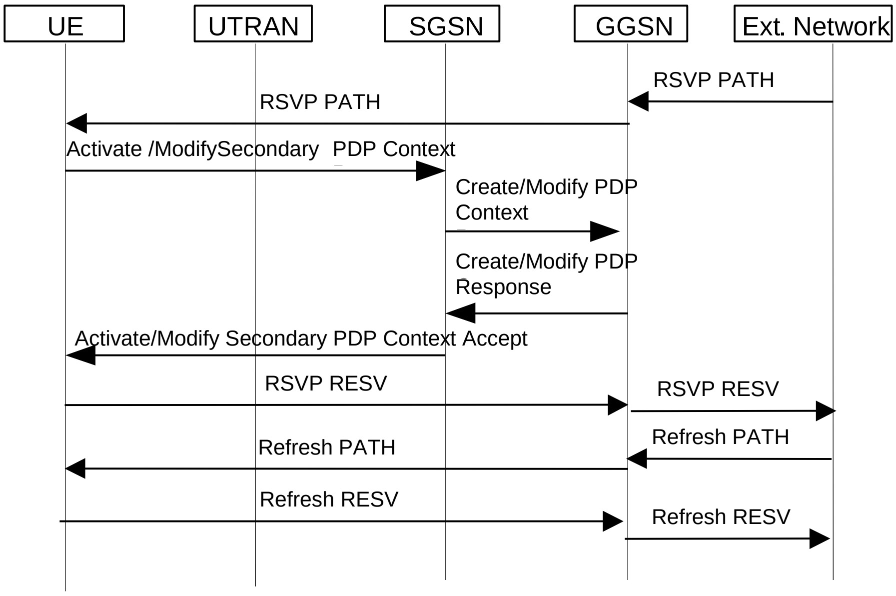

Figure A.9: UE supports RSVP signalling for the downlink flow

A.3.2 RSVP in Scenario 6

In Scenario 6, the UE provides IP level end-to-end QoS information to the GGSN using IP specific elements in PDP activation/modification message, and the GGSN uses this information to invoke RSVP messages to setup the uplink as well as the downlink flows. RSVP signalling is generated and terminated by the GGSN as shown in figures A.10 and A.11 below.

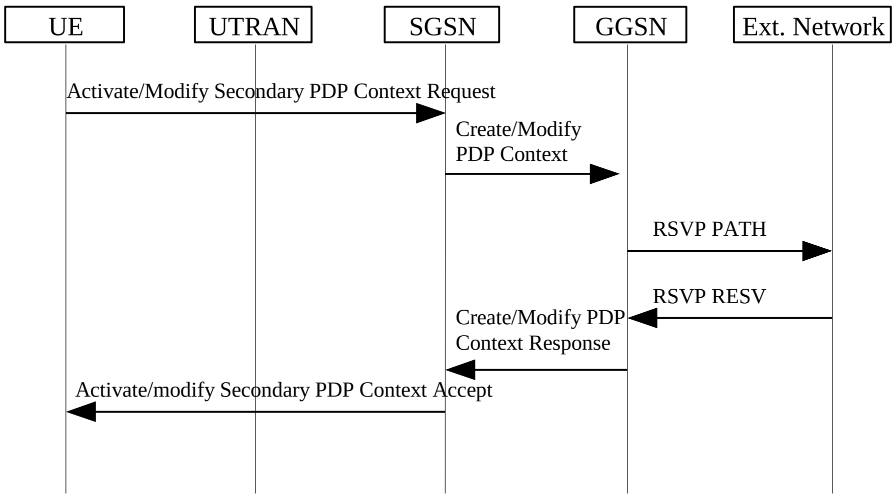

Figure A.10: UE provides IP specific elements in PDP activation/modification message, and GGSN invokes RSVP messages for uplink flow

[Editorial Note: the above diagram depicts a signalling sequence, however, the alternative signalling sequences below are possible and are for further study:

- *to trigger the Create PDP Context Response message on the PATH or after a timeout without waiting for the RESV message.*

- *to trigger the Create PDP Context Response message before the PATH.]*

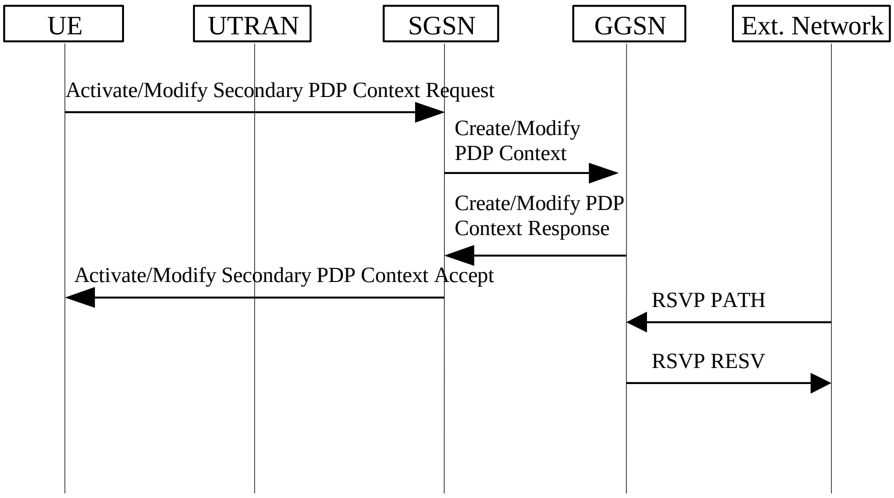

Figure A.11: UE provides IP specific elements in PDP activation/modification message, and GGSN terminates and invokes RSVP messages for downlink flow

In the above figure, the association between the RSVP PATH message and the PDP context is carried out in the GGSN.

[Editorial Note: the above diagram depicts a signalling sequence, however, the alternative signalling sequence below is possible and is for further study:

- *the RSVP PATH message arrives in the GGSN before the Activate/Modify Secondary PDP Context Request from the UE is received in the GGSN.]*

Annex B (Informative): Application Level Registration

B.1 Requirements to Consider for Registration

The additional requirement for the registration information flow for annex B is:

1. A serving CSCF is assigned at registration, this does not preclude additional serving CSCFs or change or CSCF at a later date. The additional CSCFs are for FFS.

B.2 Assumptions

The following is considered as assumptions for the registration procedures as described in Annex B:

1. Radio bearers are already established for signaling and a mechanism exists for the first REGISTER message to be forwarded to the proxy.
2. The I-CSCF will use the same mechanism in visited and home networks for determining the serving CSCF address based on the required capabilities. Resource Broker, RB performs (for figure B.1 and figure B.3 (as a note in figure B.3)) the determination and allocation of the serving CSCF during registration.

B.3 Registration Procedures

For the assumptions included in section B.1 above, the registration procedures are separated into three information flows. Information flow A is the common initiation of the registration information flows; information flow B is in the case that the serving CSCF is selected to be in the home network; and information flow C is in the case that the serving CSCF is selected to be in the visited network.

It should be noted that the requirements in section B.1 are for the case where there is a single serving CSCF selected, and the case where there are a number of serving CSCFs which are possible in the session is FFS. The following information flows are not intended to preclude this case.

In the case where the functional element is prefixed by a "h" it indicates that the functional element is located in the home network. In the case where the functional element is prefixed by a "v" it indicates that the functional element is located in the visited network. In the case where there isn't a prefix to the functional element the functional element could be in either the visited network, the home network.

In the following information flows, further work is required to identify the information elements related to credentials and possible additional processes require for authentication of the user and the messages.

In the following flows a "resource broker" exists and is used to select a serving CSCF. The exact interaction with the resource broker is for further study.

In the following information flows, there is a mechanism for to resolve a name and address. The text in the information flows indicates when the name-address resolution mechanism is utilised.

B.3.1 Registration Information Flow A : Start of registration

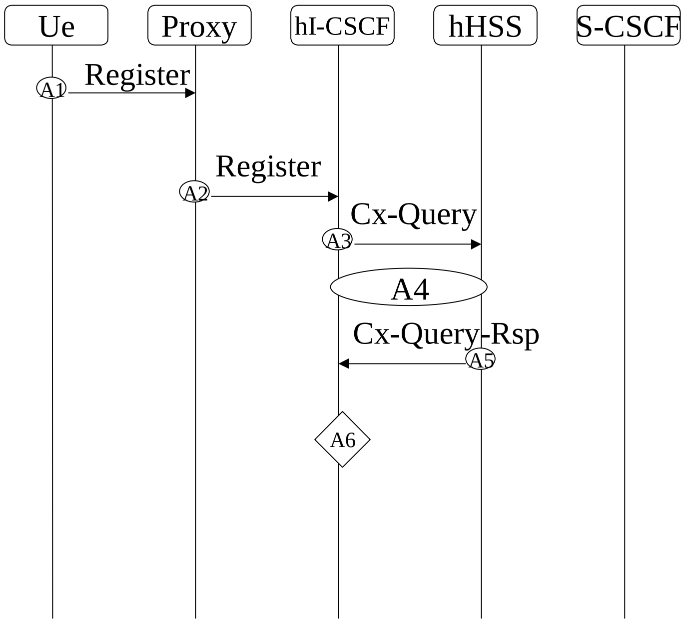

Figure B.1: Start of Registration

____

A1 Register Ue to Proxy

Control information
Ue address
Subscriber Identity
home domain name

Initiation of information flow: Ue securing a signalling channel in the "PS" domain, and deciding to initiate the IPMM subsystem registration.

Processing upon receipt: When the proxy receives the registration request, it examines the "home domain name" to discover the entry point to the home network. The proxy will insert its own "name" in the contact header, and insert the local network capabilities, the local network entry point into the Register information flow. The information flow (A2) is initiated. A name-address resolution mechanism is utilised in order to determine the destination of information flow (A2), with the home domain name as the input.

____

A2 Register Proxy to hInterrogating CSCF

Control information
proxy name
Subscriber Identity
home domain name
Local Network contact name
(the name that the registration
would be returned to in the case
of visited serving CSCF)
Local Network capabilities

Initiation of information flow: Receipt of information flow (A1).

Processing upon receipt: When the Interrogating CSCF receives the register information flow (1), it queries the HSS with information flow (A3). It is FFS whether the terminal name, or proxy name, or both is included within this and subsequent Register messages.

____

A3 Cx-Query hInterrogating CSCF to hHSS

Control information
proxy name
Subscriber Identity
Local Network contact name
Local Network capabilities

Initiation of information flow: Receipt of information flow (A2).

Processing upon receipt: Information flows (A3) (A4) and (A5) are treated together.

____

A4 - between hInterrogating CSCF and hHSS

Control information
Subscriber Identity
Local Network capabilities
Other information

Initiation of information flow: Receipt of information flow (A2) and (A3).

Processing upon receipt: The hHSS and the hInterrogating CSCF determined whether the serving CSCF is in the home network or the local network (when the local network is not the home network). In the case that the serving CSCF is in the home network, the name of the serving CSCF is determined, otherwise it is agreed that the Register information flow should be forwarded to the local network to select the serving CSCF. The mechanism for the determination and whether this is done by the hInterrogating CSCF and the hHSS is FFS, and may make use of some form of a "resource broker" to select an appropriate serving CSCF in the home network, in the case that the serving CSCF is determined to be in the home network.

____
_

A5 Cx-Query-Response hHSS to hInterrogating CSCF

Control information
Required Capabilities
Other FFS

Initiation of information flow: Receipt of information flow (A3) and procedure (A4).

Processing upon receipt: After processing information flow (A5) it is assumed that the authentication of the user has been completed and is successful (although it may have occurred at an earlier point in the message flows). The hInterrogating CSCF and the hHSS have determined the serving CSCF, or that the serving CSCF is located in the "local" network. The behaviour of the hInterrogating CSCF is dependant upon whether the serving CSCF is the home network or in the visiting network. In the case where the serving CSCF is in the home network, information flow B is followed; otherwise information flow C is followed. This decision is represented by the decision (A6) in figure x-1. The hInterrogating CSCF has received the name of the HSS and will forward this to serving CSCF for the purpose of downloading the subscriber profile.

____
_

A6 - hI-CSCF to hS-CSCF or vI-CSCF

Control information
-

Initiation of information flow: Receipt of information flow (A5).

Processing upon receipt: The behaviour of the hInterrogating CSCF is dependant upon whether the serving CSCF is determined to be in the home network of the visited network. In the case where the serving CSCF is determined to be in the home network, then the hInterrogating CSCF has the name of the Serving CSCF, and information flow (H1) is initiated. In the case where the serving CSCF is determined to be in the visited network, the hInterrogating CSCF has the name of the vInterrogating CSCF, which was provided to the home network in information flow (A2), and information flow (V1) is initiated. A name-address resolution mechanism is utilised in order to determine the destination of information flow (H1) or (V1), with the serving CSCF name or vInterrogating CSCF name as the input.

B.3.2 Registration Information Flow B : Continuation of Registration – serving CSCF in home network

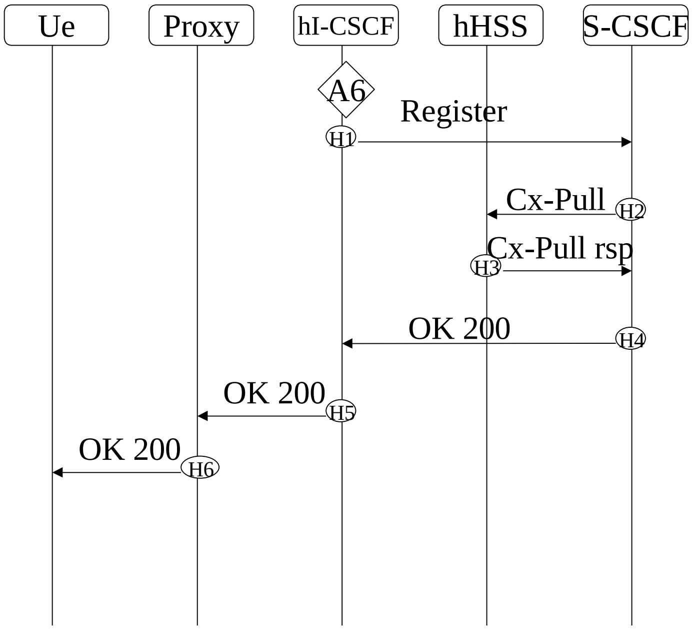

Figure B.2: Continuation of Registration – serving CSCF in home network

____

H1 Register hInterrogating CSCF to Serving CSCF

<u>**Control information**</u>
proxy name
HSS name
Subscriber Identity
home domain name

Initiation of information flow: The hInterrogating CSCF and the HSS have determined that the serving CSCF is in the home network.

Processing upon receipt: When the serving CSCF receives the information flow (H1), it understands the name of the hHSS. Based upon this, it initiates the download of the subscriber profile with information flow (H2). A name-address resolution mechanism may be utilised in order to determine the destination of information flow (H2).

____

H2 Cx-Pull Serving CSCF to hHSS

<u>**Control information**</u>
Subscriber Identity

Initiation of information flow: The serving CSCF receives information flow (H1).

Processing upon receipt: The hHSS proceeds to provide the serving CSCF with the requested subscriber profile in information flow (H3). The exact details of the subscriber profile is FFS.

____
_

H3 Cx-Pull-rsp hHSS to Serving CSCF

Control information
Subscriber profile

Initiation of information flow: The HSS receives information flow (H2).

Processing upon receipt: At this stage, it is understood that the HSS contains the name of the serving CSCF. The exact means by which this is known is FFS. Upon the receipt of the information flow (H3), the serving CSCF stores the subscriber profile. It then decides whether it will return the serving CSCF name or the hInterrogating CSCF name to the proxy (basically the name to which the interrogating CSCF and HSS has determined that the local network will forward subsequent messages, such as INVITE). The basis for this decision is operator policy.

The S-CSCF then initiates the conclusion of the registration procedures by initiating information flow (H4).

____
_

H4 OK 200 Serving CSCF to hInterrogating CSCF

Control information
Serving CSCF name

Initiation of information flow: The serving CSCF receives information flow (H3).

Processing upon receipt: The completion of the registration procedure is continued with information flow (H5) per normal SIP response processing rules. The hInterrogating CSCF releases all registration information after sending information flow (H5).

____
_

H5 OK 200 hInterrogating CSCF to proxy

Control information
Serving CSCF name or
The Interrogating CSCF name or
other contact point in the home
network.

Initiation of information flow: The hInterrogating CSCF receives information flow (H4).

Processing upon receipt: The proxy stores the network entry point returned in information flow (H5) and the address of the Ue in the local network. The proxy continues the completion of the registration procedure by forwarding the information flow (H6) to the Ue.

____
_

H6 OK 200 proxy to Ue

Control information
Proxy name

Initiation of information flow: The proxy receives information flow (H5).

Processing upon receipt: The Ue stores the name of the proxy to be contacted for subsequent communications with the network. It is FFS whether returning one proxy name to the Ue precludes the use of multiple CSCFs..

B.3.3 Registration Information Flow C : Continuation of Registration – serving CSCF in visited network

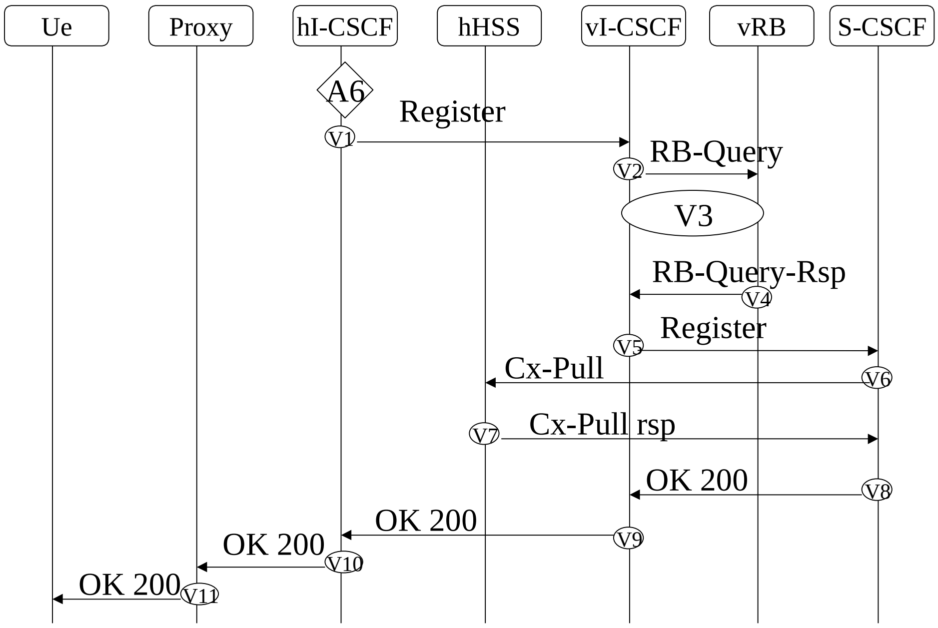

Figure B.3: Continuation of Registration – serving CSCF in visited network

NOTE: In figure B.3, the vRB and the vInterrogating CSCF refer to a resource broker and Interrogating CSCF in the visited network when the serving CSCF is located in the visited network.

____
_

V1 Register hInterrogating CSCF to vInterrogating CSCF (local network)

Control information
proxy name
HSS name (or network contact point name)
Subscriber Identity
Required Capabilities
local domain name

Initiation of information flow: The vInterrogating CSCF and the HSS have determined that the serving CSCF is in located in the local network.

Processing upon receipt: When the vInterrogating CSCF receives the information flow (V1), it communicates with the RB in the local network to determine the location of serving CSCF. This is initiated with information flow (V2).

____
_

V2 RB-Query vInterrogating CSCFv to vRB

Control information

Required Capabilities

Initiation of information flow: Receipt of information flow (V1).

Processing upon receipt: Information flows (V2) (V3) and (V4) are treated together.

____

V3 - between vInterrogating CSCF and vRB

Control information
Required Information

Initiation of information flow: Receipt of information flow (V1) and (V2).

Processing upon receipt: The vRB and the vInterrogating CSCF determine the name of the serving CSCF in the local network..

____

V4 RB-Query-Response vRB to vInterrogating CSCF

Control information
FFS

Initiation of information flow: Receipt of information flow (V2) and procedure (V3).

Processing upon receipt: At the receipt of information flow (V3) the Interrogating CSCFv has become aware of the name of the serving CSCF. The continuation of the registration procedure is initiated with information flow (V5).

____

V5 Register vInterrogating CSCF to Serving CSCF

Control information
proxy name
HSS name
Subscriber Identity
local domain name

Initiation of information flow: The vInterrogating CSCF and the RB have determined the serving CSCF.

Processing upon receipt: When the serving CSCF receives the information flow (V5), it understands the name of the hHSS, or a contact name provided by the home network. Based upon this, it initiates the download of the subscriber profile with information flow (V6). A name-address resolution mechanism may be utilised in order to determine the destination of information flow (V6).

____

V6 Cx-Pull Serving CSCF to hHSS

Control information
Subscriber Identity

Initiation of information flow: The serving CSCF receives information flow (V5).

Processing upon receipt: The HSS performs any necessary security checks, and then proceeds to provide the serving CSCF with the requested subscriber profile in information flow (V7). It may be that information flow (V7) is not directly between the serving CSCF and HSS, but it might be via firewalls or proxies. This is FFS. The exact details of the subscriber profile is FFS.

____
_

V7 Cx-Pull-rsp hHSS to Serving CSCF

Control information
Subscriber profile

Initiation of information flow: The HSS receives information flow (H6).

Processing upon receipt: At this stage it is understood that the HSS contains the name of the serving CSCF. The exact means by which this is performed is FFS. Upon the receipt of the information flow (V7) the serving CSCF stores the subscriber profile. It then decides whether it will return the serving CSCF name or the vInterrogating CSCF name to the proxy (basically the name to which the vInterrogating CSCF and RB desires the local network to forward subsequent messages, such as INVITE).

The Serving CSCF then initiates the conclusion of the registration procedures by initiating information flow (V8).

____
_

V8 OK 200 Serving CSCF to vInterrogating CSCF

Control information
Serving CSCF name

Initiation of information flow: The serving CSCF receives information flow (V8).

Processing upon receipt: The vInterrogating CSCF continues the completion of the registration procedures by returning information flow (V9). The vInterrogating CSCF releases all registration information after sending information flow (V8).

____
_

V9 OK 200 vInterrogating CSCF to hInterrogating CSCF

Control information
Serving CSCF name

Initiation of information flow: The vInterrogating CSCF receives information flow (V8).

Processing upon receipt: The completion of the registration procedure is continued with information flow (V10). The hInterrogating CSCF releases all registration information after sending information flow (V10). It is FFS whether the hI-CSCF informs the HSS of the serving CSCF name in the visited network or the HSS remembers the contact name provided in the incoming registration flow.

____
_

V10 OK 200 hInterrogating CSCF to proxy

Control information
Serving CSCF name

Initiation of information flow: The proxy receives information flow (H4).

Processing upon receipt: The proxy stores the network entry point returned in information flow (V10) and the address of the Ue. The proxy continues the completion of the registration procedure by forwarding the information flow (V11) to the Ue.

____
_

V11 OK 200 proxy to Ue

Control information
Proxy name

Initiation of information flow: The proxy receives information flow (V10).

Processing upon receipt: The Ue stores the name of the proxy to be contacted for subsequent communications with the network. It is FFS whether returning one proxy name to the Ue precludes the use of multiple CSCFs.

B.4 Stored Information

The following table provides an indication of the information stored in the indicated nodes during and after the registration process.

Node	Before Registration	During Registration	After Registration
UE - in local network	- Credentials - Home Domain		- Credentials - Home Domain - Proxy Name/Address
Proxy CSCF - in local network	- Routing Function - Local Network capabilities - potential list of Visited Serving CSCFs?	- Network Entry point - UE Address - Supplies potential list of Visited Serving CSCFs?	- Network Entry point - UE Address
Interrogating CSCF - in Home network	- HSS Address	- Serving CSCF address/name - Access to Potential list of Serving CSCFs?	- No State Information
Interrogating CSCF (visited) - in visited network	- HSS (visited – not associated with subscriber) Address	- Serving CSCF (visited) - Access to Potential list of serving CSCFs?	- No State Information
HSS	- User Service Profile	- Local network capabilities? - Access to Potential list of serving CSCFs?	- Serving CSCF address/name - Proxy address/name?
Serving CSCF (Home)	- No state information	- HSS Address/name - Subscriber profile	- May have call state Information - HSS

		(limited – as per network scenario) - Proxy address/name	Address/name - Subscriber information - Proxy address/name
Resource Broker (RB)	- Contains information regarding Serving CSCFs in the network where S-CSCF is being selected. Details of this function is for FFS	- Via I-CSCF &/or HSS, provides resource information to select S-CSCF	- Same as before registration
Serving CSCF (visited) (Need not be Proxy CSCF)	- Local Service information - No state information	- HSS (Home) Address/name - Subscriber profile (Limited – as per operator agreement) - Proxy address/name	- May have state Information - HSS (home) Address/name - Subscriber information (limited - as per operator agreement) - Proxy address/name

Note: "?" indicates that further study is required on this item.

Annex C (Informative): General Service Control methods

The following options for the control and execution of call related services can be identified (NOTE: This list is not exhaustive):

- **CAMEL access to SIP networks**
- **OSA approach**
- **JAIN - Parlay**
- **Internet proposals for SIP Sever Programming**
    - Call Processing Language (CPL)
    - Common Gateway Interface (CGI) for SIP
    - SIP Servlet API
    - Java enhanced SIP

The following figure provides an overview about the different service provisioning opportunities supported by an generalised Release 2000 architecture(see also [1] and [2]).

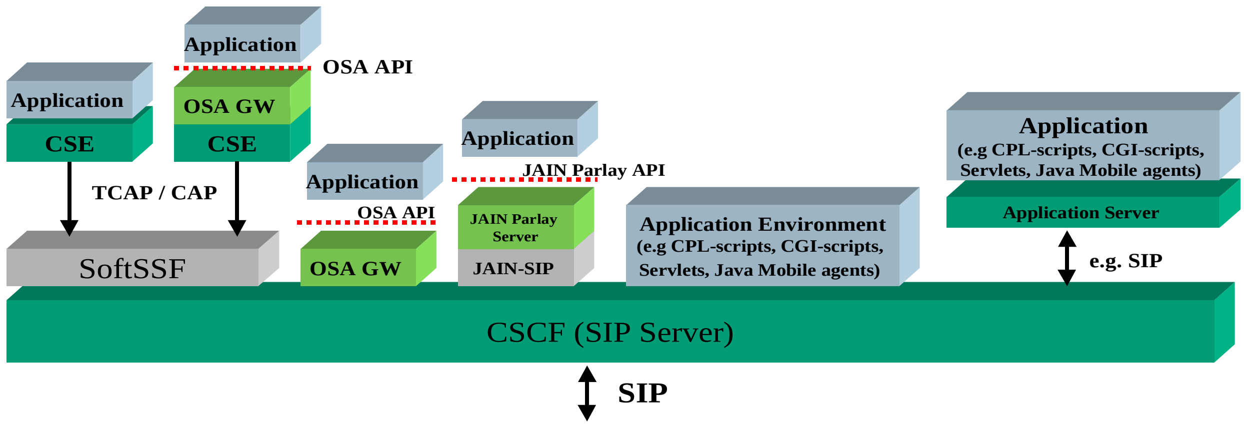

Figure C.1: Generalised Service architecture

C.1 CAMEL approach

For the continuation of the CAMEL approach, a "softSSF" to act as an overlay between the IP telephony call control and the Intelligent Network is invented. This 'softSSF' provides the necessary mapping between the SIP protocol state machine and the CAP/INAP Basic Call State Model (BCSM). For further details see [5].

C.2 OSA approach

The Open Service Architecture defines an open API for the design, implementation, control and execution of services and applications provided by third party service providers (see [6]).

The OSA approach could be used in two different ways:

- **OSA Gateway on top of the CSE:**

  For further details see [7].

- **OSA Gateway on top of the CSCF:**

  A mapping of the OSA-API functions to SIP might be feasible. It is not required to standardise the interface between the OSA-GW and the CSCF.

C.3 JAIN Parlay

The Parlay Group publishes technology-independent specifications that define a set of interfaces in the form of methods, events, parameters and their semantics. Similar to the Parlay Group, the JAVA APIs for Integrated Networks (JAIN) Community provides a Java standardisation of desktop and server technology for different network technology. For more details see [8].

C.4 Internet proposals

Different solutions for the programming of SIP Services within the IETF were proposed. This approaches include the usage of e.g. Call Processing Language (CPL), Common Gateway Interface (CGI) for SIP, SIP Servlets APIs, JAVA enhanced SIP (JES).

The service logic can either reside on the SIP servers themselves, or in special computers (Application /Feature Server) separate from the SIP servers (CSCF). In the latter case, some protocol is needed for the interface between the server and the service logic. This can again be (enhanced) SIP – in which case the CSCF would in principle act as a SIP proxy, it could be a (new) special purpose protocol, or can be some form of Remote Procedure Call.

C.5 Conclusions

Criterias to be considered for further investigations:

- provide a secure access to the network resources from third parties,
- allow sufficient protection of the network against accidental or malicious usage of network resources,
- access to network resouces should be ease-of-use for service providers,
- If ordinary end-users are going to configure their communication services the solution need to be fairly straightforward.

These two aspects, safety and simplicity, are independent, and it has been argued that they point to the need for two levels of programmability-one for trusted, advanced developers and or system administrators, and one for untrusted end users (see also [1], [4]). To avoid two different interface it would be preferable to have only one technical solution which fulfils all requirements.

Annex D (Informative): IP Specific Elements in PDP Context Activation and Modification Message

[Editorial Note: The details of the IP specific elements in PDP context activation/modification message needs further study within the S2 QoS drafting group.]

If an IP BS Manager exists both in the UE and the GGSN, it is possible that these IP BS Managers communicate directly with each other by using relevant signalling protocols, e.g., RSVP. However, it is forseen that low end mobiles will not be able to support RSVP signalling, nevertheless these mobiles are required to be able to support end-to-end QoS requests from the application layer.

It is conceivable that there is a need to allow IP specific elements to be passed from the UE to the GGSN, between peer IP BS managers, without the necessity for signalling protocol support in the UE.

Figure D.1 below shows the two QoS control levels (the UMTS bearer level and IP bearer level) and is an example of how the IP BS manager at the GGSN may exercise admission control. The requested IP level QoS bandwidth received in the IP specific element from the UE for a particular flow may be informed to the GGSN beforehand for the GGSN DiffServ edge to determine if the flow can be allowed to a certain DiffServ class or an egress point based on the service level agreement (SLA).

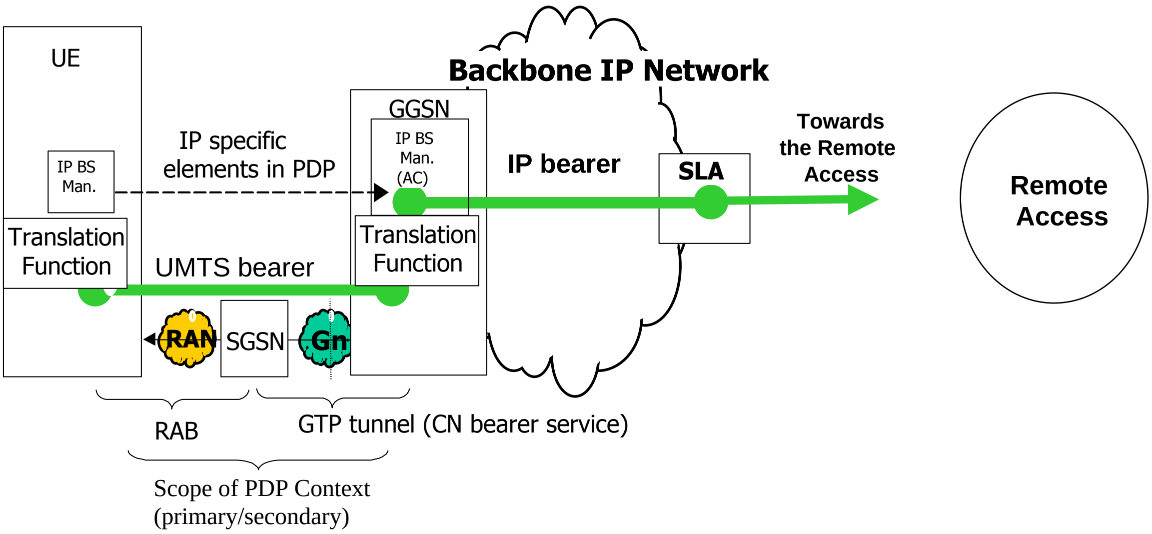

Figure D.1: Providing end-to-end QoS by means of transferring IP specific elements in PDP context activation/modification message between the UE and the GGSN and exercising policy enforcement / admission control in the GGSN

Within the IP policy architecture applicable to UMTS, the IP Policy Control makes decisions in regard to network based IP policy using policy rules, and communicates these decisions to the IP BS Manager in the GGSN, which is the IP policy enforcement point. Enforcement of policy may cover, among other things, the following requirements:

1. Authorisation of UMTS bearers from the application.

2. Control of opening and closing the gate for data to enter the network, controlled from the application server through the policy server.

3. **Control of the level and destination of data permitted to pass the gate and enter the network, controlled from the application server through the policy server.** In order for the GGSN to enforce policy conformant to the requirements above there is a need to transfer information which belongs to the IP level between the peer IP BS manager entities in the UE and GGSN. To facilitate clean separation between the UMTS bearer level and the IP bearer level, this transfer of IP level information should be carried out in a manner that is transparent to the UMTS BS managers. The IP level information may include, for example in the RSVP case, the traffic flow specification contents, required IP level QoS, and destination IP address as described in Scenario 6. For the DiffServ case, QoS information for the DiffServ classifier functionality and DiffServ class admission control may be included as described in Scenario 5.

The following candidates for the IP specific elements in PDP context activation/modification messageare identified:

1) Optional IP specific information is carried in the PDP context transparent to the UMTS BS managers, between peer IP BS managers, from the UE to the GGSN. The PDP context may contain a set of QoS attributes: "UMTS Specific IP QoS Attributes."

2) Extending the Traffic Flow Template concept to convey information to the GGSN related to the uplink flow (new mechanism), together with the use of existing TFT mechanism for the downlink flow. Bandwidth requirements etc. may be obtained by mapping the UMTS QoS parameters to the IP level QoS parameters, and also possibly extending the UMTS QoS parameters.

Annex E (Informative): Change History

Document history		
V0.0.0	1999-10	Document created
V0.1.0	2000-01	Reference architecture description added in Chapter 5. New Section 5.1. QoS end-to-end functional architecture added in new Chapter 9.1
V0.2.0	2000-03	Definitions added in Ch 3. Architecture principles added in Ch 5.1. BSS/GERAN added in the reference architecture. Text on reference points added in Ch 5.2. New Ch 9.1.
V0.3.0	2000-05	Modifications according to results from S2's drafting sessions in Helsinki, London and Stockholm during April and May 2000.
V0.4.0	2000-06	Modifications according to S2 #13 in Berlin.
V0.5.0	2000-06	Including comments on V0.4.0
V0.6.0	2000-06	A modification according to S2's drafting session in Sophia Antipolis, June 12-14 and the e-mail approval following that meeting.
V1.0.0	2000-06	No changes as compared to v.0.6.0
V1.0.1	2000-07	Editorial update by MCC to correct styles and layout
Editor for 3GPP SA2 TR 23.821 is:		
Name Christer Lind Company Telia Research AB Tel.: +4640105137 Fax: +4640307029 Email : Christer.A.Lind@telia.se		
This document is written in Microsoft Word version 7/97.		