Source: **TSG CN WG 3**

Title: **CRs to Rel-5 Work Item "E2EQoS"**

Agenda item: **8.5**

Document for: **APPROVAL**

Introduction:

This document contains **4** CRs to **Rel-5** Work Item **"E2EQoS"**, that have been agreed by **TSG CN WG3**, and are forwarded to TSG CN Plenary meeting #17 for approval.

Doc-2nd-	Spec	CR	Rev	Subject	Cat	Phase	Version-	Workitem
N3-020719	27.060	020	1	Support for forking in the UE	F	Rel-5	5.1.0	E2E QoS
N3-020742	29.207	033	2	Session modification initiated decision	F	Rel-5	5.0.0	E2E QoS
N3-020729	29.207	016	4	Support for forking in 29.207	F	Rel-5	5.0.0	E2E QoS
N3-020720	29.208	007	1	Support for forking in 29.208	F	Rel-5	5.0.0	E2E QoS

CR-Form-v7

CHANGE REQUEST

⌘	**27.060** CR **020**	⌘ **rev**	**1**	⌘	Current version:	**5.1.0**	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME **X** Radio Access Network ☐ Core Network ☐

Title: ⌘	Support for forking in the UE	
Source: ⌘	Ericsson	
Work item code: ⌘	e2eQoS	**Date:** ⌘ 17/07/2002
Category: ⌘	**F**	**Release:** ⌘ REL-5

Use <u>one</u> of the following categories:
F (correction)
A (corresponds to a correction in an earlier release)
B (addition of feature),
C (functional modification of feature)
D (editorial modification)
Detailed explanations of the above categories can be found in 3GPP <u>TR 21.900</u>.

Use <u>one</u> of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change: ⌘	Basic support for forking has been agreed as a requirement for Rel-5
Summary of change: ⌘	An outline of the UE procedures for handling of forking is described.
Consequences if not approved: ⌘	Inconsistent specifications for IMS

Clauses affected: ⌘	Clause 2, introduction of a new subclause 13.Y

	Y	N		
Other specs affected: ⌘	X		Other core specifications ⌘	TS 24.229, TS 29.207, TS 29.208
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

<div style="border:1px solid black; text-align:center;">**First modified section**</div>

---

2   References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies.

[1]   Void.

[2]   Void.

[3]   3GPP TS 22.060: "General Packet Radio Service (GPRS); Service Description Stage 1".

[4]   Void.

[5]   Void.

[6]   Void.

[7]   Void.

[8]   Void.

[9]   3GPP TS 23.060: "General Packet Radio Service (GPRS) Service Description Stage 2".

[10]   Void.

[11]   Void.

[12]   Void

[13]   Void.

[14]   Void.

[15]   Void.

[16]   3GPP TS 27.007: "AT command set for 3GPP User Equipment (UE)".

[17]   3GPP TS 29.061: "Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

[18]   ITU-T Recommendation E.164: "Numbering plan for the ISDN era".

[19]   ITU-T Recommendation V.42 bis: "Data communication over the telephone network – Data compression procedures for data circuit-terminating equipment (DCE) using error correction procedures".

[20]   Void.

[21]   Void.

[22]   Void.

[23]   Void.

[24]   Void.

[25]   Void.

[26]   IETF RFC 768 (1980): "User Datagram Protocol" (STD 6).

[27]   IETF RFC 791 (1981): "Internet Protocol" (STD 5).

[28]   IETF RFC 792 (1981): "Internet Control Message Protocol" (STD 5).

[29]   IETF RFC 793 (1981): "Transmission Control Protocol" (STD 7).

[30]   ITU-T Recommendation V.250 (ex V.25ter): "Serial asynchronous automatic dialling and control".

[31]   ITU-T Recommendation V.24: "List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)".

[32]   ITU-T Recommendation V.28: "Electrical Characteristics for unbalanced double-current interchange circuits".

[33]   ITU-T Recommendation V.80: "In-band DCE control and synchronous data modes for asynchronous DTE".

[34]   IETF RFC 1661 (1994): "The Point-to-Point Protocol (PPP)" (STD 51).

[35]   IETF RFC 1662 (1994): "PPP in HDLC-like framing" (STD 51).

[36]   IETF RFC 1700 (1994): "Assigned Numbers" (STD 2).

[37]   IETF RFC 1570 (1994): "PPP LCP Extensions".

[38]   IETF RFC 1989 (1996): "PPP Link Quality Monitoring".

[39]   IETF RFC 1332 (1992): "The PPP Internet Protocol Control Protocol (IPCP)".

[40]   IETF RFC 1877 (1995): "PPP IPCP Extensions for Name Server Addresses ".

[41]   IETF RFC 2153 (1997): "PPP Vendor Extensions".

[42]   IETF RFC 1334 (1992): "PPP Authentication Protocols".

[43]   IETF RFC 1994 (1996): "PPP Challenge Handshake Authentication Protocol".

[44]   IETF RFC 2686 (1999): "The Multi-Class Extension to Multi-Link PPP".

[45]   IETF RFC 1990 (1996): "The PPP Multilink Protocol (MP)".

[46]   IETF RFC 2472 (1998): "IP Version 6 over PPP".

[47]   3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[48]   3GPP TS 23.221: "Architectural requirements".

[49]   IETF RFC 2373 (1998): "IP version 6 Addressing Architecture".

[50]   3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3"

[51]   3GPP TS 24.229: " IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".

[52]   3GPP TS 29.207: "Policy control over Go interface".

[53]   3GPP TS 29.208: "End-to-end QoS signalling flows".

13.Y Support for forking

A UE originating a SIP session shall be able to handle several forked responses. Forking may occur in a downstream SIP proxy outside the 3GPP network. In case of service-based local policy, the same authorization token is received for all the forked responses for that session.

 For every forked response the UE shall reserves additional bearer resources if, and only if, such resources have not already been reserved by a previously received forked response for the same session. When the first final answer is received, the UE shall terminate all the other early dialogues are terminated and release the resources that are no longer required are released. This may imply that non-required PDP contexts are deactivated and the remaining PDP contexts are updated (i.e. removal of IP flows, downgrading of QoS) to match the requirements of the first final answer.

On the terminating side, if a UE receives several forked requests for the same session, it shall accepts the first request and proceeds to set up the corresponding SIP session. Subsequent requests for the same session are shall be rejected.

Detailed call control procedures for forking are specified in 3GPP TS 24.229 [51]. Specific procedures related to the Go interface are specified in 3GPP TS 29.207 [52] and 3GPP TS 29.208 [53].

| **End of modified sections** |

CR-Form-v7

CHANGE REQUEST

| ⌘ | **29.208** CR **007** | ⌘ **rev** | **1** | ⌘ | Current version: | **5.0.0** | ⌘ |

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐   ME ☐   Radio Access Network ☐   Core Network **X**

Title: ⌘	Support for forking in 29.208	
Source: ⌘	TSG_CN WG3	
Work item code:⌘	e2eQoS	***Date:*** ⌘ 10/07/2002
Category: ⌘ **F**		***Release:*** ⌘ Rel-5

Use <u>one</u> of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP <u>TR 21.900</u>.

Use <u>one</u> of the following releases:
2   *(GSM Phase 2)*
R96   *(Release 1996)*
R97   *(Release 1997)*
R98   *(Release 1998)*
R99   *(Release 1999)*
Rel-4   *(Release 4)*
Rel-5   *(Release 5)*
Rel-6   *(Release 6)*

Reason for change: ⌘	Limited support for forking is defined in the stage 2 requirements for Rel-5 (TS 23.228)
Summary of change:⌘	When forking occur in a downstream proxy outside the IM CN Subsystem, the UE and PCF/PCSCF shall be able to handle multiple forked responses for the same session. The various forked responses may have different QoS requirements. The maximum authorized QoS for a media flow shall be equal to the maximum QoS requested for that media flow by any of the forked responses.
Consequences if not approved: ⌘	Non-alignment with stage 2 requirements. The IM CN Subsystem may not be able to interoperate with external SIP networks where forking may occur

Clauses affected: ⌘	Added 7.3

	Y	N		
Other specs ⌘	X		Other core specifications ⌘	TS 24.229, TS 29.207, TS 27.060
affected:		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Start of modified text.

7.1.1   SDP parameters to Authorized IP QoS parameters mapping in PCF

The QoS authorization is to be based on the parameters Maximum Authorized DiffServ PHB and Maximum Authorized Data Rate UL/DL.

The PCF shall use the mapping rules in table 7.1.1.1 to derive the Authorized IP QoS parameters Maximum Authorized Data Rate DL/UL and the Maximum Authorized DiffServ PHB from the SDP Parameters. In case of forking, the additional rule in section 7.3 shall apply.

**Table 7.1.1.1: Rules for derivation of the Maximum Authorized Data Rates
and Maximum Authorized DiffServ PHB per media flow in the PCF**

Authorized IP QoS Parameter per media flow	Derivation from SDP Parameters

Maximum Authorized Data Rate DL and UL per media flow (see note 1)	/* Check if the media use codec(s) */
	IF [(<media> = ("audio" or "video")) and (<transport> = "RTP/AVP")] THEN
	
	   /* Check if Streaming */
	   IF a=("sendonly" or "recvonly") THEN
	     Maximum Authorized Data Rate DL/UL per media flow is set equal to Maximum Bitrate DL/UL. See reference [5] ;
	Editor's note: Whether Maximum Authorized Data Rate per media flow is set to Maximum or Guaranteed Bitrate is ffs.
	
	   /* Conversational as default !*/
	   ELSE
	     Maximum Authorized Data Rate DL/UL per media flow is set equal to Maximum Bitrate DL/UL. See reference [6] ;
	Editor's note: Whether Maximum Authorized Data Rate per media flow is set to Maximum or Guaranteed Bitrate is ffs.
	   ENDIF ;
	
	/* Check for presence of bandwidth attributes */
	ELSEIF b=AS:<bandwidth-value> is present THEN
	   Maximum Authorized Data Rate DL/UL per media flow = "bandwidth-value" ;
	
	/* SDP do not give any guidance! **/**
	ELSE
	   Maximum Authorized Data Rate DL/UL per media flow is set according to operator policy ;
	ENDIF ;

Maximum Authorized DiffServ PHB per media flow (see note 2)	IF [(<media> = ("audio" or "video")) and (a="sendrecv")] THEN
	   Maximum Authorised DiffServ PHB per media flow = "EF" ;
	ELSEIF [(<media> = ("audio" or "video")) and (a=("sendonly" or "recvonly"))] THEN
	   Maximum Authorised DiffServ PHB per media flow = "AF4" ;
	ELSEIF <media> = ("application" or "control") THEN
	   Maximum Authorised DiffServ PHB per media flow = "AF3" ;
	ELSE Maximum Authorised DiffServ PHB per media flow = "BE" ;
	END ;

NOTE 1: For a RTP media flow the Maximum Authorized Bandwidth DL/UL are the sum of the RTP flow DL/UL and the associated RTCP flow DL/UL. NOTE 2: The Maximum Authorized Traffic Class for a RTCP flow is the same as the corresponding RTP flow.	

The PCF shall per ongoing session store the Authorized IP QoS parameters per media flow.

When the GGSN requests the Authorized UMTS QoS parameters for an activated/modified PDP Context carrying one or more media flows (eventually with associated RTCP signalling), the PCF shall use the rules in table 7.1.1.2 to calculate the Authorized IP QoS parameters.

**Table 7.1.1.2: Rules for calculating the Maximum Authorized Data Rate
and Maximum Authorized Diffserv PHB Parameters per Binding Information in the PCF**

Authorized IP QoS Parameter per Binding	Calculation Rule

Maximum Authorized Data Rate DL and UL per Binding Information	Maximum Authorized Data Rate DL/UL per Binding Information is the sum of all Maximum Authorized Data Rate DL/UL per media flow for all the media flows identified by the Binding Information
	
	IF Maximum Authorized Data Rate DL/UL per Binding Information > 2047 kbps THEN
	    Maximum Authorized Data Rate DL/UL per Binding Information = 2047 kbps /* See ref [8] */
	
	END;

Maximum Authorized Diffserv PHB per Binding Information	Maximum Authorized Diffserv PHB per Binding Information = MAX [Maximum Authorized Diffserv PHB per media flow among all the media flows carried by the current PDP Context] (The MAX function ranks the possible Maximum Authorized Diffserv PHB values as follows: "EF" > "AF4" > "AF3" > "BE")

End of modified section

….

Start of next modified section

7.2.2   SDP parameters to Authorized UMTS QoS parameters mapping in UE

If the PDP Context is activated or modified in an IMS context then it is recommended that the UE uses the mapping rules in table 7.2.2.1 to derive the Maximum Authorized Bandwidth UL/DL.

Table 7.2.2.1 also has a mapping rule for derivation of Maximum Authorized Traffic Class. In future releases this mapping rule may change. For the reason of future compatibility, the release 5 mapping rule is optional for the UE.

In the case this mapping rule is implemented then it is recommended that the UE use the mapping rule in table 7.2.2.1 to derive the Maximum Authorised Traffic Class from the SDP Parameters.

When the maximum authorized QoS for a media flow in forked responses is derived, the additional rule in section 7.3 shall apply.

**Table 7.2.2.1: Rules for derivation of the Maximum Authorized Bandwidth DL/UL
and the Maximum Authorized Traffic Class per media flow in the UE**

Authorized UMTS QoS Parameter per media flow	Derivation from SDP Parameters

Maximum Authorized Bandwidth DL and UL per media flow	/* Check if IMS context (the criteria for this check is an UE manufactures issue) */
	IF IMS context THEN
	
	/* Check if the media use codec(s) */
	   IF [(<media> = ("audio" or "video")) and (<transport> = "RTP/AVP")] THEN
	
	     /* Check if Streaming */
	     IF a=("sendonly" or "recvonly") THEN
	      Maximum Authorized Bandwidth DL/UL set equal to Maximum Bitrate DL/UL. See reference [5] ;
	Editor's note: Whether Maximum Authorized Bandwidth is set to Maximum or Guaranteed Bitrate is ffs.
	
	     /* Conversational as default !*/
	     ELSE
	      Maximum Authorized Bandwidth DL/UL set equal to Maximum Bitrate DL/UL. See reference [6] ;
	Editor's note: Whether Maximum Authorized Bandwidth is set to Maximum or Guaranteed Bitrate is ffs.
	     ENDIF ;
	
	   /* Check for presence of bandwidth attributes */
	   ELSEIF b=AS:<bandwidth-value> is present THEN
	    Maximum Authorized Bandwidth DL/UL = "bandwidth-value" ;
	
	   /* SDP do not give any guidance! /
	   ELSE
	    Maximum Authorized Bandwidth DL/UL as specified by the UE manufacturer ; ENDIF ;
	
	ELSE
	  No authorization is done ;
	ENDIF ;

Maximum Authorized Traffic Class per media flow	/* Check if IMS context (the criteria for this check is an UE manufactures issue) */
	IF IMS context THEN
	IF [(<media> = ("audio" or "video")) and (a="sendrecv")] THEN
	  Maximum Authorised Traffic Class = "Conversational" ;
	ELSEIF [(<media> = ("audio" or "video")) and (a=("sendonly" or "recvonly"))] THEN
	  Maximum Authorised Traffic Class = "Streaming" ;
	ELSEIF <media> = ("application" or "control") THEN
	  Maximum Authorised Traffic Class = "Interactive" ;
	
	ELSE Maximum Authorised Traffic Class = "Background" ;
	END ;
	
	ELSE
	  No authorization is done ;
	ENDIF ;

It is recommended that the UE per ongoing session store the Authorized UMTS QoS parameters per media flow.

Furthermore it is recommended that the UE checks that the requested UMTS QoS parameters Traffic Class and Maximum Bitrate UL/DL not exceeds the values of the corresponding Authorized UMTS QoS parameters (calculated according to the rules in table 7.2.2.2) before activating/modifying a PDP Context.

**Table 7.2.2.2: Rules for calculating the Maximum Authorized Bandwidths
and Maximum Authorized Traffic Class Parameters per PDP Context in the UE**

Authorized UMTS QoS Parameter per PDP Context	Calculation Rule

Maximum Authorized Bandwidth DL and UL per PDP Context	/* Check if IMS context (the criteria for this check is an UE manufactures issue) */
	IF IMS context THEN
	
	   Maximum Authorized Bandwidth DL/UL per PDP Context is the sum of all Maximum Authorized Bandwidth DL/UL per media flow for all the media flows carried by the PDP Context ;
	
	IF Maximum Authorized Bandwidth DL/UL per PDP Context > 2047 kbps THEN
	   Maximum Authorized Bandwidth DL/UL per PDP Context = 2047 kbps /* See ref [8] */
	END;
	
	ELSE
	   No authorization is done ;
	ENDIF ;

Maximum Authorized Traffic Class per PDP Context	/* Check if IMS context (the criteria for this check is an UE manufactures issue) */
	IF IMS context THEN
	
	   Maximum Authorised Traffic Class per PDP Context = MAX [Maximum Authorised Traffic Class per media flow among all the media flows carried by the PDP Context] ;
	
	ELSE
	   No authorization is done ;
	ENDIF ;
	
	(The MAX function ranks the possible Maximum Authorised Traffic Class values as follows: Conversational > Streaming > Interactive > Background)

End of modified section

…

Start of added section

7.3 Support for forking

For an initiated session the UE and the PCF may receive several forked responses, ref. 3GPP TS 29.207 [7]. The various forked responses may have different QoS requirements for the same media flow. In the case of forked responses, the maximum authorized QoS for a media flow shall be equal to the highest QoS requested for that media flow by any of the active forked responses. This applies both to the UE and to the PCF.

End of added section

CR-Form-v7

CHANGE REQUEST

⌘	**29.207** CR **016**	⌘ **rev** **4** ⌘	Current version:	**5.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐   ME ☐ Radio Access Network ☐ Core Network **X**

Title: ⌘	Support for forking in 29.207	
Source: ⌘	TSG_CN WG3	
Work item code: ⌘	e2eQoS	**Date:** ⌘ 10/07/2002
Category: ⌘	**F**	**Release:** ⌘ Rel-5

Use <u>one</u> of the following categories:
F (correction)
A (corresponds to a correction in an earlier release)
B (addition of feature),
C (functional modification of feature)
D (editorial modification)
Detailed explanations of the above categories can
be found in 3GPP <u>TR 21.900</u>.

Use <u>one</u> of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change: ⌘	Limited support for forking is defined in the stage 2 requirements for Rel-5 (TS 23.228)
Summary of change: ⌘	When forking occur in a downstream proxy outside the IM CN Subsystem, the PCF/PCSCF shall be able to handle multiple forked responses for the same session. The same authorization token is used for all the early dialogues. The "logical or" of the resource requests of all the forked responses is authorized via the Go interface. When the first final answer is received, the authorization information in PCF and GGSN is updated to match the requirements of the related early dialogue.
Consequences if not approved: ⌘	Non-alignment with stage 2 requirements. The IM CN Subsystem may not be able to interoperate with external SIP networks where forking may occur

Clauses affected: ⌘	2, 5.2.1.1, added 5.2.2

	Y	N		
Other specs ⌘	X		Other core specifications ⌘	TS 24.229, TS 29.208, TS 27.060
affected:		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘	

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Start of first modified section.

2   References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

[2]   3GPP TS 23.002: "Network architecture".

[3]   3GPP TS 23.207: "End to end quality of service concept and architecture".

[4]   3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[5]   IETF RFC 2475: "An Architecture for Differentiated Services".

[6]   IETF RFC 2753: "A Framework for Policy-based Admission Control".

[7]   IETF RFC 2748: "The COPS (Common Open Policy Service) Protocol".

[8]   IETF RFC 3084: "COPS Usage for Policy Provisioning (COPS-PR)".

[9]   IETF RFC 3159: "Structure of Policy Provisioning Information (SPPI)".

[10]   IETF RFC 2205: "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification".

[11]   IETF RFC tbd: "Session Authorisation for RSVP" (draft-ietf-rap-rsvp-authsession-02.txt).

[12]   3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core network protocols; Stage 3".

[13]   3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services".

[xx]   3GPP TS 24.229: " IP Multimedia Call Control Protocol based on SIP and SDP"

End of modified section

…

Start of next modified section

5.2.1.1   SBLP authorisation decision

The information needed for the PCF to perform media authorization is passed by the P-CSCF upon receiving a SIP message that contains SDP. The SDP contains sufficient information about the session, such as the end-points' IP address and port numbers and bandwidth requirements.

All media components in the SDP are authorised. The media components contain one or more IP flows each represented by a flow identifier. Cf. the definition of flow identifier in clause 3.1. A flow identifier is expressed as a 2-tuple as follows:

<Media component no, IP flow no.>

where both are numbered starting from 1.

0   3

Media component no.	IP flow no.

As an example, if the second "m=" - line in the SDP information contains one RTP media specification, the following flow identifiers would be assigned:

IP flow	Flow id.
RTP	<2,1>
Associated RTCP	<2,2>

The P-CSCF shall send policy setup information to the PCF upon every SIP message that includes an SDP payload. This ensures that the PCF passes proper information to perform media authorization for all possible IMS session setup scenarios. The policy setup information provided by the P-CSCF to the PCF for each media component shall contain the following:

- Destination IP address;

- Destination port number;

- Transport Protocol id;

- Media direction information;

- Direction of the source (originating or terminating side);

- Indication of the group that the media component belongs to;

Editor's note: The format of this group indication in SIP/SDP is subject to CN1's decision.

- Media type information;

- Bandwidth parameter;

- Indication of forking/non-forking.

Additionally, upon the P-CSCF receives the ICID in SIP signalling, it shall send the ICID to the PCF.

The PCF stores the authorised policy information, and generates an Authorisation Token to identify this decision. The Authorisation Token is passed back to the P-CSCF for inclusion in the SIP signalling back to the UE.

The Authorisation Token is in the form of a Session Authorisation Data Policy Element as described in [11]. The PCF shall include an AUTH_ENT_ID attribute containing the Fully Qualified Domain Name of the PCF and the SESSION_ID attribute.

Upon receiving the bearer authorization request from the GGSN, the PCF shall authorize the request according to the stored service based local policy information for the session identified by the binding information in the request.

- Decision on the binding information:

    The authorisation shall contain the decision on verifying the binding information. The PCF shall identify whether the binding information indeed corresponds to an initiated SIP session.

    The authorization shall also contain decision on the list of flow_IDs contained in the bearer authorisation request sent by the GGSN representing the list of media components intended to be carried in the same PDP Context. This decision shall verify that these media components are indeed allowed to be carried in the same PDP Context. The PCF shall make this decision by comparing the list of flow_IDs contained in the bearer authorization request received from the GGSN to the media component grouping indication information received from the P-CSCF.

In case the UE violates the IMS level indication, and attempts to set up multiple IMS media components in a single PDP context despite of an indication that mandated separate PDP contexts, the PCF shall enforce the rejection of this PDP context request by sending the an INSTALL and REMOVE decision to the GGSN.

If the binding information and the list of flow_IDs are successfully authorised (verified) as per the means described above, the PCF shall also communicate the authorisation details for each media component to the GGSN.

The authorisation details contain the "Authorised QoS" and the packet classifier(s) of the associated IP flows. In case of an aggregation of multiple media components within one PDP context, the combination of the "Authorised QoS" information of the individual media components is provided as the "Authorised QoS".

Based on the media direction information and the direction of the source provided by the P-CSCF, the PCF shall define the direction (upstream or downstream) of the "Authorised QoS" and the packet classifier(s).

- Packet classifier(s):

    The PCF shall use the destination IP address(es), destination port number(s) and transport protocol id(s) to formulate a packet classifier(s).

    - The source IP address and source port number, which are part of the standard 5-tuple for packet classifying, are not provided by the P-CSCF. Therefore, the source IP address and source port number are wildcarded by the PCF in the packet classifier.

        Editor's note: The wildcarding of the source IP address maybe updated depending on the SA2's decision.

    - The PCF shall send the destination address and the destination port number for each IP flow associated with the media component.

- "Authorized QoS":

    The "Authorised QoS" information (consisting of maximum DiffServ Class and Data Rate) for a media component is extracted from the media type information and bandwidth parameter of the SDP. The PCF shall map the media type information into a DiffServ Class which is the highest class that can be used for the media. As an example, the audio media type shall be mapped into Expedited Forwarding PHB.

    The PCF shall extract the Data Rate value from the "b=AS" SDP parameter. The "b=AS" parameter in the SDP shall contain all the overhead coming from the IP-layer and the layers above, e.g. UDP, RTP. The Data Rate shall also include the overhead coming from the possible usage of RTCP.

NOTE: The overhead coming from the IP-layer and the layers above is also included in the UMTS QoS bitrate parameters and the IP QoS parameters (e.g. RSVP flowSpec).

When the GGSN uses IP QoS parameters for resource reservation, the Data rate value shall be considered as the maximum value of the 'Token Bucket Rate' IP QoS parameter. When the GGSN uses UMTS QoS parameters, the Data rate value shall be considered as the maximum value of the 'Guaranteed bitrate' parameter for real-time bearers.

    Editor's note: Mapping the Data rate value for the real time into 'Guaranteed bitrate' or 'Maximum bitrate' parameter is for FFS.

For non-real-time bearers the Data rate value shall be considered as the maximum value of the 'Maximum bitrate' parameter.

In case of an aggregation of multiple media components within one PDP context, the PCF shall provide the "Authorised QoS" for the bearer as the combination of the "Authorised QoS" information of the individual media components. The DiffServ Class in the "Authorised QoS" for the bearer shall contain the highest PHB amongst the ones applied for the individual media components and indicates the highest UMTS traffic class that can be applied to the PDP context.

    Editor's note: It shall be possible the group identifiers to restrict the individual media components carried by the same PDP context to have the same PHBs.

The Data Rate of the "Authorised QoS" for the bearer shall be the sum of the Data Rate values of the individual media components and it is used as the maximum Data Rate value for the PDP context.

The PCF may include the gate enabling command as part of the authorisation decision. Alternatively, the PCF may provide a separate decision for opening the gate.

The PCF shall send the IMS charging identifier provided by the P-CSCF as part of the authorisation decision to the GGSN.

Upon receiving the modified SDP information from the P-CSCF, the PCF shall update the media authorization information for the session. The PCF may push this updated authorisation information to the GGSN. Under certain condition e.g. revoke of authorization, the PCF shall push the updated policy decision to the GGSN.

End of modified section

…

Start of next modified section

5.2.1.2   SBLP revoke decision

The PCF shall send a revoke authorisation decision to the GGSN upon SIP session release. The revoke authorisation decision shall be sent as a separate decision to the GGSN corresponding to the previous SBLP authorisation decision.

Additionally, when a media component which is bound to a PDP context is removed from a SIP session and the UE has not performed the corresponding modification of the PDP context within an operator specific time the PCF shall revoke the authorisation for the set of media components on that PDP context.

The timer shall be terminated if the PCF receives a new authorisation request with the same handle where that media component has been removed, or by termination of the PDP context.

5.2.2 Support for forking

The PCF shall be able to handle forking when SBLP is applied. Forking can occur as specified in 3GPP TS 23.228 [4]

 The related UE procedures are described in 3GPP TS 24.229 [xx].

5.2.2.1 Authorization of resources for forked responses

When a SIP session has been originated by a connected UE, the P-CSCF may receive multiple provisional responses due to forking before the first final answer is received. The PCF shall allocate the same authorization token to all the forked responses and the corresponding early dialogues.

The UE and the P-CSCF- become aware of the forking only when the second provisional response arrives. For this, and any subsequent provisional response, the PCF shall identify the existing authorization information for that session. The PCF shall authorize any additional media components and any increased QoS requirements for the previously authorized media components, as requested by the forked response. Thus, the QoS authorized for a media component shall be equal to the highest QoS requested for that media component by any of the forked responses. Authorization is done by the procedures for authorization request in sections 5.1.1 and 5.1.2 and SBLP decisions in section 5.2.1.1.

Additional packet classifiers as required by the subsequent responses are sent to the GGSN by the session modification initiated decision specified in section 5.2.1.2x.

5.2.2.2 Updating the authorization information at the final answer

The PCF shall keep the authorization information requested for each of the individual early dialogues till the first final answer is received. Then the related early dialogue is progressed to establish the final SIP session. All the other early dialogues are terminated. The authorization information for the SIP session is updated to match the requirements of the remaining early dialogue only. Several actions may be needed in the PCF:

- Only the packet classifiers and the QoS indicated by the first final answer shall remain authorized. This information shall be sent to the GGSN by the session modification initiated decision specified in section

5.2.1.2x. This should be done without delay in order to reduce the risk for initial clipping of the media stream, and minimising possible misuse of resources.

- The authorization for PDP contexts that were used only for the terminated early dialogues, shall be revoked as specified in section 5.1.43.

- The PCF shall await new authorization requests for remaining PDP contexts with updated binding information to remove any media components that were authorized for the terminated early dialogues only.   If necessary (i.e. after timeout), the authorization for these PDP contexts shall be revoked as specified in section 5.2.1.32

For example, assume that three forked responses for a certain media component indicate the bandwidths 10, 30 and 20 kbps, respectively. This media component will first be authorized for 10 kbps and then upgraded to 30 kbps, which will be its final value for the early dialogue phase. If the first final answer corresponds to the third forked, provisional response, then QoS is finally downgraded to 20 kbps.

End of updated text

CR-Form-v7

CHANGE REQUEST

⌘	**29.207**	CR	**033**		⌘**rev**	**2**	⌘	Current version:	**5.0.0**	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title: ⌘	Session modification initiated decision	
Source: ⌘	TSG_CN WG3	
Work item code: ⌘	E2EQoS	**Date:** ⌘ 1/08/2002
Category: ⌘	**F**	**Release:** ⌘ REL-5

Use one of the following categories:
F (correction)
A (corresponds to a correction in an earlier release)
B (addition of feature),
C (functional modification of feature)
D (editorial modification)
Detailed explanations of the above categories can
be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change: ⌘	TS 29.207 currently specifies the handling for a number of session modifications. However, the mechanism to handle session modifications for bandwidth and port numbers which can happen for a number of reasons including forking which handling is currently not defined.

These session modifications change the authorisation information that has been sent to the GGSN. In cases where only the filters are changed, the UE is not required to initiate a PDP context modification so the PCF cannot rely on a new authorisation request to update the filters in the GGSN.

In cases where the maximum authorised QoS has been decreased, it is possible that the PDP context is below the new QoS authorisation so no PDP context modification may occur, and the PCF cannot revoke the authorisation since it is not being exceeded.

In the cases above, the PCF must initiate an unsolicited update to the previous authorisation decision since it cannot rely on a new authorisation request being received to update this information. |
Summary of change: ⌘	Introduces unsolicited push of new authorisation information (QoS and packet classifiers). If the current QoS for the PDP context exceeds the new authorised limit, the GGSN shall initiate a network initiated modification.
Consequences if not approved: ⌘	Session modifications that affect bandwidth and packet classifiers are not supported.
Clauses affected: ⌘	Additions to 4.3.1.1, 4.3.2.1, new sections 5.1.3 and 5.2.1.2 inserted, old sections 5.1.3, 5.1.4, and 5.2.1.2 renumbered (no references found to these

		Y	N		
	renumbered chapters)				
Other specs ***Affected:***	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First amended section

4.3.1.1   Service-based local policy enforcement point

The Service-based Local Policy Enforcement Point (PEP) is a logical entity which resides in the GGSN and communicates with the PCF regarding Service-based local policy control. Hereafter in the present document, the GGSN is assumed to contain the PEP implicitly unless otherwise stated. The GGSN sends requests to and receives decisions from the PCF. The GGSN may cache the policy decision data of the PCF decisions. This cached information may be used later for a local policy decision allowing the GGSN to make policy control decision about the QoS authorization for PDP context modifications without requiring additional interaction with the PCF.

The following service-based local policy enforcement point functionalities in the GGSN are identified:

- Authorisation request:

  The GGSN requests authorisation information from PCF for the media components carried by a PDP context. The GGSN enforces the PCF decisions related to the media components carried by a PDP context.

  The GGSN shall enforce unsolicited authorisation decisions which update the QoS and packet classifiers.

- Authorisation report:

  The GGSN shall also report to the PCF its success or failure in carrying out the PCF decision.

- Policy based admission control:

  The GGSN includes policy-based admission control that is applied to the bearers associated with the media components, and configures the policy based "gating" functionality in the user plane.

  Policy-based admission control ensures that the GPRS bearer carrying media components, which is activated in the GGSN, is authorised by the PCF decision.

  Additionally, policy-based admission control ensures that the resources, which can be used by each particular media component, are within the "Authorised QoS" specified by the PCF. This information is mapped by the Translation/mapping function in the GGSN to give the authorised resources for GPRS bearer admission control.

  To ensure charging correlation, the PEP shall send the GPRS charging identifier and the GGSN address to the PCF.

- Policy based gating functionality:

  Policy based gating functionality represent the control of the GGSN over the Gate Function in the user plane, i.e. the forwarding of IP packets associated with a media component. In the user plane, a "gate" is defined for each direction of a media component. The PCF provides the gate description and the commands to open or close the gate. The gate description is received from the PCF in the authorisation decision. The command to open or close the gate shall be sent either in the authorisation decision or in subsequent decisions from the PCF.

Next amended section

4.3.2.1   Service-based local policy decision point

The PCF functions as a Policy Decision Point for the service-based local policy control. The PCF makes policy decisions based on session and media related information obtained from the P-CSCF. The PCF shall exchange the decision information with the GGSN via the Go interface.

The following service-based local policy decision point functionalities are identified:

- Authorisation function:

  The PCF shall be able to provide an authorisation decision upon receiving a bearer authorisation request from the GGSN. The PCF shall authorise the request according to the stored session and media related information

received from the P-CSCF.

The PCF shall be able to provide updates to the authorisation decision at session modifications which change the QoS and packet classifiers for PDP contexts which are already established.

Editor's Note: a potential for theft of service scenario has been identified with the current mechanism for authorisation. Extensions to the authorisation mechanisms to close potential theft of service scenarios are currently under investigation, and will be specified when determined.

- Revoke function:

  The PCF may revoke the authorisation of resources at any time. Revoke Authorisation for GPRS and IP resources is communicated by the PCF to the GGSN.

- Approval of QoS Commit / Removal of QoS Commit:

  The PCF may allow or deny for the media component(s) the usage of the PDP context by controlling the correlated gate(s).

  The "Approval of QoS Commit" command may either be part of the authorisation decision, or the PCF may provide a separate decision with the "Approval of QoS Commit" command to open the gate.

  The "Removal of QoS Commit" command may either be part of the revoke authorisation decision, or the PCF may provide a separate decision with the "Removal of QoS Commit" command to close the gate.

- Actions due to Indication of bearer release:

  When the GGSN informs the PCF of bearer deactivation, the PCF shall remove the corresponding authorisation request state. Additionally, the PCF shall inform the P-CSCF about this deletion event.

- Actions due to Indication of bearer modification:

  When the PCF receives an indication of bearer modification of the maximum bitrate to or from 0 kbits/s, the PCF shall inform the P-CSCF about this modification event.

- Generation of authorisation token:

  During the session set-up the PCF generates an authorisation token for the IMS session.

- Mapping SDP parameters to "Authorized QoS" parameters:

  To perform proper authorisation, the PCF shall map the necessary SDP parameters containing session and media related information to "Authorized QoS" parameters.

- Charging identifiers exchange:

  The PCF shall send the ICID provided by the P-CSCF as part of the initial authorisation decision of all the bearer authorization requests that correspond to the respective SIP session.

  When the PCF receives the GCID together with the GGSN address from the GGSN, it shall forward these information to the P-CSCF to ensure charging correlation.

Next amended section

5.1.3   Session modification initiated decision

A session modification may occur that modifies the media components without adding or removing media lines, for example, a change in the bandwidth for the media line, or a change to the port number. The GGSN will receive unsolicited authorisation decision from the PCF due to such modifications.

When the GGSN receives an unsolicited authorisation decision from the PCF with updated QoS information, the GGSN shall update the stored authorised QoS. If the existing QoS of the PDP context exceeds the updated authorised QoS, the GGSN shall initiate a timer for the UE to modify the PDP context to decrease the QoS to within the authorised limit. At expiry of the timer, if the PDPcontext still exceeds the authorised QoS, the GGSN shall perform a network initiated PDP context modification to reduce the QoS to the authorised level.

When the GGSN receives an unsolicited authorisation decision from the PCF, the GGSN shall also install the new set of packet classifiers, removing any existing packet classifiers that are not included in the new set.

Next amended section

5.1.43   PDP context deactivation

The GGSN is responsible for notifying the PCF when a procedure of a PDP context deactivation is performed. In case of a PDP context deactivation, the GGSN shall inform the PCF of the bearer release related to the SIP session.

When a revoke authorisation for the set of media components on that PDP context is performed, the GGSN receives a decision message from the PCF for disabling the use of the "Authorised QoS" resources and deactivation of the PDP context associated with the binding information. The GGSN shall disable the use of the "Authorized QoS" resources. The GGSN shall initiate deactivation of the PDP context used for carrying these media components, in case that the UE has not performed it within an operator specific time.

Next amended section

5.1.54   User plane operation

The GGSN shall enforce the configuration of the policy based "gating" functionality according to additional authorisation information received from the PCF.

Editor's note: the exact GGSN action if the "gating" parameters provided by the PCF are not identical with the parameters from the TFT in the PDP context request is for further study.

Next amended section

5.2.1.2   Session modification initiated decision

A session modification may occur that modifies the media components without adding or removing media lines, for example, a change in the bandwidth for the media line, or a change to the port number.

When there are updates to the SDP parameters for media lines which are currently authorised, the authorisation information (QoS, packet classifiers) may change. The updated information (QoS, packet classifiers) shall be pushed down to the GGSN using an unsolicited authorisation decision.

Next amended section

5.2.1.32   SBLP revoke decision

The PCF shall send a revoke authorisation decision to the GGSN upon SIP session release. The revoke authorisation decision shall be sent as a separate decision to the GGSN corresponding to the previous SBLP authorisation decision.

Additionally, when a media component which is bound to a PDP context is removed from a SIP session and the UE has not performed the corresponding modification of the PDP context within an operator specific time the PCF shall revoke the authorisation for the set of media components on that PDP context.

The timer shall be terminated if the PCF receives a new authorisation request with the same handle where that media component has been removed, or by termination of the PDP context.