Technical Specification Group Services and System Aspects
Meeting #28, 06 - 08 June 2005,
Quebec, Canada

TSGS#28(05)0337

Source: **SA WG2**

Title: **CR to TS 23.207: Update of binding information handling (Rel-6)**

Document for: **Approval**

Agenda Item: **7.2.3**

SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers Cur	SA2 Doc	WI	Clauses affected
SP-050337	23.207	0087	-	Rel-6	F	Update of binding information handling	6.4.0	S2-051275	TEI-6	2, 5.2.1, 5.2.2, 5.3.2, 6.2

3GPP TSG-SA WG2 Meeting #46 ***Tdoc ⌘S2-051275***
Athens, Greece, 9th – 13th May 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **23.207** **CR** **0087** ⌘**rev** **-** ⌘ Current version: **6.4.0** ⌘

*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 ☒

Title:	⌘	Update of binding information handling			
Source:	⌘	SA WG2			
Work item code:	⌘	TEI6	***Date:***	⌘	04/05/2005
Category:	⌘	**F**	***Release:***	⌘	Rel-6

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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	The Release 5 limitation that only IP flows of one AF session are allowed on the same PDP context was removed within Release 6. Although the stage 3 specifications (TS 29.207 Rel-6) provides this enhanced functionality, stage 2 has not been updated yet.
Summary of change:	⌘	A sentence about the limitation is deleted. Instead, it is clarified in the relevant sections that one or more sets of the binding information may have to be handled for the same PDP context. The reference to the stage 3 specification for the Gq interface is updated.
Consequences if not approved:	⌘	Contradicting statements in stage 2 and stage 3 specifications may lead to incorrect implementations.

Clauses affected:	⌘	2, 5.2.1, 5.2.2, 5.3.2, 6.2				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

Start of 1st 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, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 22.288: "Service requirements for the IP Multimedia – stage 1".

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

[3] 3GPP TS 23.107: "QoS Concept and Architecture".

[4] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – stage 2".

[4a] 3GPP TS 29.207: " Policy control over Go interface ".

[4b] 3GPP TS 29.208: " End to end Quality of Service (QoS) signalling flows".

[4c] 3GPP TS 29.~~xxx~~209: “Policy control over Gq interface”.

[5] 3GPP TS 22.105: "Vocabulary for 3GPP Specifications".

[6] RFC 2475: "An Architecture for Differentiated Services (DiffServ)".

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

[8] RFC 2748: "Common Open Policy Service protocol (COPS)".

[9] RFC 2205: "Resource ReSerVation Protocol (RSVP)".

[10] RFC 2209: "Resource ReSerVation Protocol (RSVP) Message Processing Rules".

[11] RFC 2210: "The use of RSVP with IETF integrated Services".

[12] RFC 1633: "Integrated Services in the Internet Architecture: an Overview".

[13] RFC 3261: "SIP: Session Initiation Protocol".

[14] RFC 2327: "Session Description Protocol".

[15] RFC 2998: "A Framework For Integrated Services Operation Over DiffServ Networks".

[16] RFC 2750: "RSVP Extensions for Policy Control".

[17] RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[18] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[19] 3GPP TS 23.060: “General Packet Radio Service (GPRS) Service description; Stage 2”

[20] 3GPP TS 23.221: "Architecture requirements".

End of 1st modified section

Start of 2nd modified section

5.2.1 GGSN

This clause provides functional descriptions of capabilities in GGSN. The capabilities are part of IP BS Manager (see 5.1.1.1) or corresponding user plane functions. Determination of exactly which functions are required to support interoperator and multi-vendor aspects are not addressed in this clause.

The **DiffServ Edge Function** shall be compliant to the IETF specifications for Differentiated Services [6]. The IETF Differentiated Services architecture will be used to provide QoS for the external bearer service.

Parameters for the DiffServ Edge Function (i.e. classifiers, meters, packet handling actions) may be statically configured on the GGSN, derived from PDP Context parameters and/or derived from RSVP signalling.

DiffServ functions configured on the basis of PDP Context parameters consist of marking user packets. The DSCP to be used is derived from the PDP Context parameters according to statically configured rules.

Statically configured DiffServ functions may include classifiers, meters, markers, droppers and shapers acting on uplink traffic.

The **Service-based Local Policy Enforcement Point** controls the quality of service that is provided to a combined set of IP flows. The policy enforcement function includes policy-based admission control that is applied to the bearer associated with the flows, and configuration of the policy based "gating" functionality in the user plane. Service-based local policy decisions are either "pushed" to or requested by the GGSN via the Go interface.

Policy-based admission control ensures that the resources that can be used by a particular set of IP flows are within the "authorized resources" specified via the Go interface. The authorized resources provide an upper bound on the resources that can be reserved or allocated for the set of IP flows. The authorized resources are expressed as a maximum authorised bandwidth and QoS class. The QoS class identifies a bearer service (which has a set of bearer service characteristics associated with it). The PDF generates a maximum authorized QoS class for the set of IP flows. This information is mapped by the **Translation/mapping function** in the GGSN to give the authorized resources for UMTS bearer admission control.

In the user plane, policy enforcement is defined in terms of a "gate" implemented in the GGSN. A gate is a policy enforcement function that interacts through Go interface with PDF as the Policy Decision Point for QoS resource authorisation at the IP BS level for a unidirectional flow of packets. Gate operations as defined in TS23.228 are to control and manage media flows based on policy, and are under the control of PDF. A gate operates on a unidirectional flow of packets, i.e., in either the upstream or downstream direction. A gate consists of a packet classifier, and a gate status (open/closed). When a gate is open, the packets in a flow are accepted, and are thus subject to the DiffServ edge treatment. When a gate is closed, all of the packets in the flow are dropped.

The gate shall be applied to the PDP contexts where SBLP applies, and for such PDP contexts the information received in the TFT is ignored. In the downlink direction, packets are processed against each gate in turn until a match is found. If a match is not found, packet processing shall then continue against filters installed from UE supplied TFTs for PDP contexts where SBLP is not applied according to specification TS 23.060.

In the uplink direction, packets received on a PDP context with SBLP based filters shall be matched against those filters. If a match is found, the packet shall be passed if the gate associated with that filter is open processed according to the gate functions. If the gate is closed, or if the packet does not match any of the packet filters, the packet shall be silently discarded.

The packet classifier associated with a gate is a micro-flow classifier including the standard 5-tuple: (source IP address, destination IP address, source port, destination port, protocol), identifying a set of packets associated with a unidirectional flow.

Elements of the 5-tuple that cannot be derived from the SDP according to a set of rules shall be wild-carded.

The **Binding Mechanism Handling** associates the PDP context bearer with one or more IP flows in order to support service-based local policy enforcement. Binding information is included in PDP Context Activation or Modification messages to associate the PDP context bearer with SBLP policy decision information provided by the PDF associated with the IP flow(s). The GGSN may receive one or more sets of the binding information during an activation or modification of a PDP context. Each set of binding information consists of an authorisation token and the flow identifier(s) related to the IP flow(s) within the same session. In order to allow SBLP policy information to be "pulled" from the PDF, the binding information shall allow the GGSN to determine the address of the PDF to be used. The GGSN shall forward the binding information received from the UE to the PDF. If multiple sets of binding information are received by the GGSN, it shall forward them to the PDF.

When binding information is received, the GGSN shall ignore any UE supplied TFT, and the filters in that TFT shall not be installed in the packet processing table. When sending the binding information to the network, the UE shall populate the TFT filters with wildcard values.

End of 2nd modified section

Start of 3rd modified section

5.2.2 UE

This clause provides functional descriptions of capabilities in UE. The capabilities are part of IP BS Manager (see 5.1.1.1) or corresponding user plane functions. Determination of exactly which functions are required to support interoperator and multi-vendor aspects are not addressed in this clause.

DiffServ Edge Function acts as a DiffServ (DS) boundary for the traffic from applications running on the UE. As specified in RFC2475, DS boundary node must be able to apply the appropriate PHB to packets based on the DS code point. In addition, DS boundary nodes may be required to perform traffic conditioning functions. When GGSN DiffServ marking is used, the DiffServ edge function in the UE is not needed.

RSVP/IntServ Function provides the capability for the UE to request end-to-end QoS using RSVP messages as defined in IETF standards. RSVP messages may also be used by the network to inform the DSCP to be used by the UE. RSVP messages shall include the authorization token and flow identifier(s) in a policy data object if the authorization token is available in the UE. RSVP may be used to trigger PDP context activation/modification. The inter-working between MT and TE is FFS.

Binding Mechanism associates the PDP context bearer to the IP flow(s) to support SBLP policy enforcement in the GGSN. The binding information containing the authorization token and flow identifier(s) provides the binding mechanism, and is included by the UE in the PDP Context Activation and Modification messages. The UE may include one or more sets of the binding information. Each set of binding information consists of an authorisation token and the flow identifier(s) related to the IP flow(s) within the same session. The ~~authorization token~~ binding mechanism may also be used to bind a RSVP session with a SIP session by including the ~~authorization token and flow identifier(s)~~ one or more sets of binding information in RSVP messages. The AF provides the authorization token to the UE during AF session set-up. E.g. for IMS services, the authorization token is provided to the UE by the P-CSCF during SIP session establishment.

For each bi-directional media flow, the UE shall ensure that the 64 bit IPv6 address prefix of the source address of outgoing packets is the same as the prefix of the destination address supplied for incoming packets.

End of 3rd modified section

Start of 4th modified section

5.3.2 Information Exchanged via Go Interface

The COPS protocol supports several messages between a client and server.

Additional 3GPP Go-specific information elements must be included in COPS messages to support the SBLP control functions identified in Section 5.3.1. Consistent with the COPS framework, the Go interface is identified by a "client type" allocated for a 3GPP Go COPS client (GGSN).

All of the information described in the remainder of this section applies specifically to the 3GPP Go COPS client type. The events specific to the UMTS or IP bearer service would trigger the request messages from the GGSN PEP to the PDF. The information elements specific to UMTS would be standardized and carried in the 3GPP Go specific interactions between the PDF and the GGSN.

A **Request** (REQ) message from the GGSN to the PDF shall allow the GGSN to request SBLP policy information for a set of IP flows identified by one or more sets of binding information (described below).

Each set of ~~B~~binding information associates the PDP context to the IP flow(s) of an AF session, and is used by the GGSN to request SBLP policy information from the PDF. ~~The~~ Each set of binding information includes 1) an authorization token sent by the AF to the UE during AF session signalling, and 2) one or more flow identifiers used by the UE, GGSN and PDF to uniquely identify the IP media flow(s) within the same session.

The authorization token shall be unique within the scope of the operator’s domain. The authorization token conforms to relevant IETF standards on SIP Extensions for Media Authorization.

A flow identifier identifies an IP media flow associated with the SIP session. Flow identifiers are based on the ordering of media components (media description structure defined by a single 'm=' line), and port numbers within that media component in the SDP. A flow identifier combined with the authorization token shall be sufficient to uniquely identify an IP media flow.

A **Decision** (DEC) message from the PDF to the GGSN contains decision objects. A Decision object shall include one of the following commands:

- Install (Admit request/Install configuration, Commit)
- Remove (Remove request/Remove configuration)

These commands are used to:

- Authorize QoS/Revoke QoS authorization for one or more IP flows
- Control forwarding for one or more IP flows

The **responses** from the PEP to the PDF include an acknowledgement and/or an error response to commands received by the PEP. The following response messages shall be supported:

- Report State (Success/Failure/Accounting) (RPT)

The **Delete Request State (DRQ)** message from the PEP to the PDF indicates that the request state of a previously authorised bearer resource is no longer available/relevant at the GGSN so the corresponding COPS policy state shall likewise be removed at the PDF. The DRQ message includes the reason why the request state was deleted.

The Install command used to Authorize QoS contains the following policy information associated with the IP flow(s):

- Packet classifier(s)
- Authorized QoS information
- Packet handling action
- Charging information (ICID in case of IMS)

The packet classifier includes the standard 5-tuple: (source IP address, destination IP address, source port, destination port, protocol), identifying a set of packets associated with a unidirectional flow. Elements of the 5-tuple may be wild-carded.

The authorized QoS information provides an upper bound on the resources that can be reserved or allocated for the combined set of IP flows. The authorized QoS information shall contain the DiffServ class and Data rate parameter. The DiffServ class is used only to identify the maximum allowed traffic class.

NOTE: Further elements and details of the authorized QoS information are defined in 29.207.

The packet handling action defines the packet handling that should be accorded to packets matching the packet classifier. The packet handling action (gate status) shall result in packets being passed (gate open), or silently discarded (gate closed).

Charging information (ICID) allows the GGSN to be aware of the IMS_session level charging identifier of the IMS session that the Install command relates to. The PDF shall send the ICID provided by the P-CSCF as part of the authorisation (Install) decision.

The Report State contains the following information:

- Charging correlation information

Charging correlation information contains information used to correlate usage records (e.g. CDRs) of the GGSN with AF session records from the AF. For this purpose, the GGSN shall send the GCID of the PDP context and the GGSN address to the PDF as part of the authorisation report (RPT).

The messages which revoke QoS authorisation or remove configuration information provide only the information that is needed to perform the action (e.g., the COPS handle element, which is used as a way of identifying the installed decision information).

End of 4th modified section

Start of 5th modified section

6.2 IP Bearer Level / Application Level Binding Mechanism

The *binding mechanism* associates the PDP context bearer with policy information in the GGSN to support service based local policy enforcement. The SBLP policy decision information in the GGSN is based on IP media flows. The binding mechanism identifies the IP media flow(s) associated with a PDP context bearer and uses this information in selecting the policy information to apply.

The UE shall be able to include one or more sets of binding information in PDP Context Activation and Modification messages to associate the PDP context bearer with policy information. ~~The~~ Each set of binding information includes 1) an Authorization Token sent by the AF to the UE during AF session signaling, and 2) one or more Flow Identifiers which are used by the UE, GGSN and PDF to uniquely identify the IP media flow(s) within the same session. ~~It is assumed that only one binding information is carried within PDP context Activation/Modification messages in this Release.~~

The authorization token shall be unique within the scope of the operator’s domain. The authorization token conforms to relevant IETF standards.

A Flow Identifier identifies an IP media flow associated with the SIP session. Flow Identifiers are based on the sequence of media components (media description structure defined by a single 'm=' line) in the SDP, and IP flow numbers (defined in the order of increasing port numbers) within each media component.

A flow identifier combined with the authorization token shall be sufficient to uniquely identify an IP media flow.

In order to allow SBLP policy information to be "pulled" from the PDF, the authorization token shall allow the GGSN to determine the address of the PDF to be used.

End of 5th modified section