3GPP TSG-CN Meeting #25 **NP-040333**
8th – 10th September 2004. Palm Springs, USA.

Source: **TSG CN WG3**

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

Agenda item: **8.5**

Document for: **APPROVAL**

Introduction:

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

WG_tdoc	Spec	CR	R	Cat	Title	Rel	C_Ver	Work Item
N3-040587	29.207	131	2	F	COPS DEC message handling	Rel-5	5.8.0	E2EQoS
N3-040588	29.207	132	2	A	COPS DEC message handling	Rel-6	6.0.0	E2EQoS
N3-040589	29.207	133	2	F	COPS-PR "Request State" flag not set for authorization failure decision	Rel-5	5.8.0	E2EQoS
N3-040590	29.207	134	2	A	COPS-PR "Request State" flag not set for authorization failure decision	Rel-6	6.0.0	E2EQoS

3GPP TSG-CN WG3 Meeting #33 **Tdoc ⌘N3-040587**
Sophia Antipolis, France. 16th to 20th August 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.207** **CR** **131** ⌘**rev** **2** ⌘ Current version: **5.8.0** ⌘

*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:	⌘	COPS DEC message handling
Source:	⌘	TSG_CN WG3
Work item code:	⌘	E2EQoS
Date:	⌘	09/08/2004
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:

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:	⌘	Unclear handling of packet classifiers in case of solicited authorization decision on PDP context modification. Clear handling is only described for unsolicited authorization decision in Clause 5.1.3: "When the GGSN receives an unsolicited authorisation decision from the PDF, the GGSN shall also install the new set of packet classifiers, removing any existing packet classifiers that are not included in the new set."
Summary of change:	⌘	Same handling for solicited authotization decision as for unsolicited: When the GGSN receives a solicited authorisation decision from the PDF, the GGSN shall install the new set of packet classifiers, removing any existing packet classifiers that are not included in the new set.
Consequences if not approved:	⌘	GGSN could fail to remove previous packet classifiers, and thus allow no longer desired IP flows.

Clauses affected:	⌘	5.1.2			
		Y	**N**		
Other specs Affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

5.1.2 Modification of previously authorized PDP context

The GGSN is responsible for notifying the PDF when a procedure of PDP context modification of a previously authorized PDP context is performed. A modification of a previously authorized PDP Context may occur for example when a new media component is added or when the codec change requires new resources. To authorise the PDP context modification the GGSN shall send an authorisation request to the PDF including the binding information received from the UE in the following cases:

- Requested QoS exceeds "Authorised QoS";
- New binding information is received.

The GGSN on receiving the PDP context modification request from the UE will verify the authorisation. If the GGSN does not have sufficient information to authorize the PDP context modification request then the GGSN shall interrogate the PDF for modification request authorisation.

If the requested QoS is within the already "Authorized QoS" and the binding information is not changed, the GGSN need not send an authorization request to the PDF.

If the PDF does not respond with a decision message to an authorization request sent by the GGSN or the communication between the GGSN and the PDF fails, the GGSN shall reject the PDP context modification with the error code "Authorizing entity temporarily unavailable" (see annex D).

When the GGSN receives an authorisation decision as response from the PDF containing a set of packet classifiers, the GGSN shall install this set of packet classifiers, removing any existing packet classifiers that are not included in this set.

The GGSN is responsible for notifying the PDF, by sending a COPS Report State (RPT) message, when the procedure of the PDP context modification is performed in the following cases:

- Requested QoS maximum bit rate is 0 kbit/s;
- Requested QoS maximum bit rate changes from 0 kbit/s.

3GPP TSG-CN WG3 Meeting #33 ***Tdoc ⌘N3-040588***

Sophia Antipolis, France. 16th to 20th August 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.207** **CR** **132** ⌘ **rev** **2** ⌘ Current version: **6.0.0** ⌘

*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 ☒

Title:	⌘	COPS DEC message handling
Source:	⌘	TSG_CN WG3
Work item code:	⌘	E2EQoS
Date:	⌘	09/08/2004
Category:	⌘	**A**
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:	⌘	Unclear handling of packet classifiers in case of solicited authorization decision on PDP context modification. Clear handling is only described for unsolicited authorization decision in Clause 5.1.3: "When the GGSN receives an unsolicited authorisation decision from the PDF, the GGSN shall also install the new set of packet classifiers, removing any existing packet classifiers that are not included in the new set."
Summary of change:	⌘	Same handling for solicited authotization decision as for unsolicited: When the GGSN receives a solicited authorisation decision from the PDF, the GGSN shall install the new set of packet classifiers, removing any existing packet classifiers that are not included in the new set.
Consequences if not approved:	⌘	GGSN could fail to remove previous packet classifiers, and thus allow no longer desired IP flows.

Clauses affected:	⌘	5.1.2

		Y	N		
Other specs Affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

5.1.2 Modification of previously authorized PDP context

The GGSN is responsible for notifying the PDF when a procedure of PDP context modification of a previously authorized PDP context is performed. A modification of a previously authorized PDP Context may occur for example when a new media component is added or when the codec change requires new resources. To authorise the PDP context modification the GGSN shall send an authorisation request to the PDF including the binding information received from the UE in the following cases:

- Requested QoS exceeds "Authorised QoS";
- New binding information is received.

The GGSN on receiving the PDP context modification request from the UE will verify the authorisation. If the GGSN does not have sufficient information to authorize the PDP context modification request then the GGSN shall interrogate the PDF for modification request authorisation.

If the requested QoS is within the already "Authorized QoS" and the binding information is not changed, the GGSN need not send an authorization request to the PDF.

If the PDF does not respond with a decision message to an authorization request sent by the GGSN or the communication between the GGSN and the PDF fails, the GGSN shall reject the PDP context modification with the error code "Authorizing entity temporarily unavailable" (see annex D).

When the GGSN receives an authorisation decision as response from the PDF containing a set of packet classifiers, the GGSN shall install this set of packet classifiers, removing any existing packet classifiers that are not included in this set.

The GGSN is responsible for notifying the PDF, by sending a COPS Report State (RPT) message, when the procedure of the PDP context modification is performed in the following cases:

- Requested QoS maximum bit rate is 0 kbit/s;
- Requested QoS maximum bit rate changes from 0 kbit/s.

3GPP TSG-CN WG3 Meeting #33 **Tdoc ⌘N3-040589**
Sophia Antipolis, France. 16th to 20th August 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.207** **CR** **133** ⌘**rev** **2** ⌘ Current version: **5.8.0** ⌘

*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:	⌘	COPS-PR "Request State" flag not set for authorization failure decision
Source:	⌘	TSG_CN WG3
Work item code:	⌘	E2EQoS
Date:	⌘	09/08/2004
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:

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:	⌘	Unclear if COPS-PR "Request State" flag needs to be set for authorization failure decision. The GGSN could expect this "Request State" flag as trigger to send DRQ message at authorization failure of an initial authorization request, see RFC 3084, Clause 3.3..
Summary of change:	⌘	COPS-PR "Request State" flag not set for authorization failure decision.
Consequences if not approved:	⌘	GGSN could fail to send DRQ message, causing state not to be removed at the PDF.

Clauses affected:	⌘	4.3.2.3, 5.1.1, 6.3.2

	Y	N		
Other specs Affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

4.3.2.3 Binding mechanism handling

The binding information is used by the GGSN to identify the correct PDF and subsequently request service-based local policy information from the PDF. Each set of binding information consists of an authorisation token and one or more flow identifier(s).

During the session set-up the PDF generates an Authorisation Token for the IMS session as described in RFC 3313 [22]. The Authorisation token shall be sent to the P-CSCF which forwards it to the UE in the SIP signalling. The PDF shall allocate its PDF identifier as part of the Authorization Token. This identifier shall be in the format of a fully qualified domain name.

The PDF receives the binding information and a Client Handle as part of a REQ from the GGSN. The PDF shall store the Client Handle for each flow identifier identified by the binding information for subsequent message exchanges.

The authorisation token is applied by the PDF to identify the IMS session. If no IMS session can be found for an authorisation token, or if the authorization token for the Client Handle has been modified, or if the PDF is otherwise unable to authorise the binding information, the PDF shall send a COPS decision message carrying both an INSTALL and REMOVE decision. The INSTALL decision shall identify an authorisation failure to the GGSN, and may include further details identifying the cause. The REMOVE decision shall subsequently remove this state from the GGSN. The "Request State" flag shall not be set within the REMOVE decision. For an initial authorisation, the GGSN will send a COPS Delete Request State (DRQ) message to the PDF to clean up the corresponding COPS handle state.~~PDF shall then initiate a remove for the authorisation request.~~

Next modified section

5.1 GGSN

5.1.1 Initial authorization at PDP context activation

The GGSN may receive binding information during the activation of a secondary PDP context by the UE. To perform initial authorization at the secondary PDP context activation the GGSN shall send an authorisation request to the PDF including the binding information received from the UE.

The GGSN identifies the required PDF from the authorisation token of the binding information. The authorisation token is formatted according to the structure of the policy element AUTH_SESSION defined in RFC 3520 [11]. The policy element AUTH_SESSION shall include the AUTH_ENT_ID and the SESSION_ID attributes. The GGSN checks for that Policy Element and retrieves the AUTH_ENT_ID attribute from this. If this is in the form of a Fully Qualified Domain Name, then this is used to identify the correct PDF.

The GGSN authorisation request message to the PDF shall allow the GGSN to request policy information for authorisation of the IP flows identified by the flow identifiers within the binding information carried by a PDP context.

When the GGSN receives the PDF decision, the GGSN shall enforce the policy decision. To enforce the policy decision, the GGSN shall install the packet filters received from the PDF, and ignore the UE supplied TFT.

If the PDF decision information indicates that the binding information provided by the GGSN is authorised, the GGSN shall proceed with activation of the secondary PDP context. The GGSN shall map the authorized QoS resources into authorized resources for the bearer admission control.

To ensure charging correlation, the GGSN shall send the GCID and GGSN address information to the PDF after the successful establishment of the secondary PDP context, i.e. with the report following the initial authorization decision.

When the PDF detects that the binding information provided by the GGSN is not associated with an ongoing SIP session at application layer, or is otherwise unable to authorise the binding information, the GGSN will receive a COPS decision message from the PDF carrying both an INSTALL and REMOVE decision. The "Request State" flag is not set within the REMOVE decision. The reason for the rejection is indicated by the INSTALL decision with an appropriate authorisation request failure reason. The GGSN shall reject the secondary PDP context activation with a corresponding error code, see annex D. The GGSN shall subsequently remove this state according to the REMOVE decision. For an

initial authorisation request, the GGSN shall then send a COPS Delete Request State (DRQ) message to the PDF to remove the state in the GGSN and the PDF.

When the GGSN sends an authorization request to the PDF but the PDF does not respond with the decision message or the communication between the GGSN and the PDF fails, the GGSN shall reject the secondary PDP context activation with the error code "Authorizing entity temporarily unavailable" (see annex D).

Next modified section

6.3.2 Message description

The following messages and events are available on the Go interface (after the initial policy provisioning described in subclause 6.3.1.5):

- Authorisation_Request (REQ) (GGSN→PDF):

  This event allows the GGSN to request authorisation data from the PDF. It contains the following information:

  - Client Handle;
  - Binding Information.

  The R-type = 0x08 for configuration request is used here and M-type = 0x02 create event state is used here.

- Authorisation_Decision (DEC)(PDF→GGSN), contains an INSTALL decision:

  This event provides the GGSN with the relevant authorisation data. The event contains the following information:

  - Client Handle;
  - ICID(s) (only in the initial Authorisation_Decision). Only one ICID is transferred in this Release. The form of the ICID is defined in 3GPP TS 32.225 [21];
  - Unidirectional set (this parameter shall appear once for each direction (uplink and downlink)):
    - Direction indicator;
    - "Authorised QoS";
    - Gate description (this parameter shall appear once for each required gate for this direction):
      - Filter Specification - The information about the authorised IP end points addresses and ports is detailed below. The Filter Specification parameters are:
        - Source IP address;
        - Destination IP address;
        - Source ports;
        - Destination ports;
        - Protocol ID.

          The Source and Destination ports are described with a range consisting of a minimum and maximum value. If only one port is authorised, the minimum value and maximum value of the range are identical.

          A filter specification describing more than one IP flow shall be only used in case of identical Protocol IDs, IP addresses and successive port numbers (e.g. RTP and RTCP IP flow of a media component). Furthermore, the gate status of all IP flows described by this filter specification shall be identical, too.

The Base and IP Filter definitions from the IETF Framework PIB [15] shall be used in the 3GPP Go PIB to represent the filter specification. Only a subset of the available filter attributes shall be used. The attributes frwkIpFilterDscp, and frwkIpFilterFlowId in the filter description shall have their values set to –1, indicating a "match-all" wildcard condition, in effect a "not used" condition. The attribute frwkBaseFilterNegation shall have its value set to "false" to indicate not using negation, in effect a "not used" condition. The GGSN shall ignore them if they are set otherwise. Wildcarding of filter elements is detailed in Annex B.

- Gate status (opened/closed)

The R-type = 0x08 for configuration request is used here and M-type = 0x02 create event state is used here.

- Authorisation_Failure (DEC) (PDF→GGSN), contains an INSTALL and a REMOVE decision:

This event provides the GGSN with an indication of an authorisation failure, and may carry additional reason details. The event contains the following information:

- Client Handle;
- Authorisation failure (including any provided reason information).

The R-type = 0x08 for configuration request is used here and M-type = 0x04 terminate event state is used here.

The COPS Decision Flags object 0x02 ("Request-State" flag) shall not be set for the REMOVE decision.

- Gate Decision (DEC) (PDF→GGSN), contains an INSTALL decision:

The Gate Decision indicates to the GGSN the new status of the gate(s) established for a client handle (PDP context). The gate status indicates to the GGSN that the gate shall be opened or closed. Only the gate(s) for which the status is changed are indicated by this event. The event contains the following information:

- Client Handle;
- Unidirectional set (this parameter shall appear once for each direction for which gates are being updated (uplink and/or downlink)):
  - Direction indicator;
  - Gate description (this parameter shall appear once for each gate to be modified for this direction) :
    - Filter Specification - The information about the authorised IP end points addresses and ports is detailed below. The Filter Specification parameters are:
      - Source IP address;
      - Destination IP address;
      - Source ports;
      - Destination ports;
      - Protocol ID.

        The Source and Destination ports are described with a range consisting of a minimum and maximum value. If only one port is authorised, the minimum value and maximum value of the range are identical.

        A filter specification describing more than one IP flow shall be only used in case of identical Protocol IDs, IP addresses and successive port numbers (e.g. RTP and RTCP IP flow of a media component). Furthermore, the gate status of all IP flows described by this filter specification shall be identical, too.

        The Base and IP Filter definitions from the IETF Framework PIB [15] shall be used in the 3GPP Go PIB to represent the filter specification. Only a subset of the available filter attributes shall be used. The attributes frwkIpFilterDscp, and frwkIpFilterFlowId in the filter description shall have their values set to –1, indicating a "match-all" wildcard condition, in effect a "not used" condition. The attribute frwkBaseFilterNegation shall have its value set to "false" to indicate not using

negation, in effect a "not used" condition. The GGSN shall ignore them if they are set otherwise. Wildcarding of filter elements is detailed in Annex B.

- Gate status (opened/closed)

NOTE: The opening of the gate may occur at the same time / be part of the authorisation decision event.

The R-type = 0x08 for configuration request is used here and M-type = 0x03 update event state is used here.

- Report (RPT) (GGSN→PDF):

  The GGSN sends a COPS RPT message as a response to a decision (DEC) message back to the PDF reporting that it enforced or not the Authorisation_Decision or the Authorization_Failure_Decision (Authorization_Report) or the Gate_Decision (Gate_Report).

  The events contain the following information:

  - Client Handle;
  - Success / Failure.

  In addition, the Authorization_report of the initial Authorisation_Decision includes:

  - GCID;
  - GGSN address.

- Report of state changes:

  The GGSN sends the report of state change message to the PDF reporting that the maximum bit rate for the PDP context is modified to 0 kbps or that the maximum bit rate for the PDP context is changed from 0 kbps.

  The event contains the following information:

  - Client Handle;
  - Maximum bit rate (set to 0 kbps / changed from 0 kbps).

- Delete Request State (DRQ) (GGSN→PDF):

  The GGSN informs the PDF via the delete request state message, that the PDP context is deactivated and the request state identified by the client handle is no longer available/relevant at the GGSN, so the corresponding state shall also be removed at the PDF.

  The DRQ message includes the reason why the request state was deleted.

  The event contains the following information:

  - Client Handle;
  - Reason code: value 4 "Tear", indicating the deactivation of the PDP context.

- Remove_Decision (DEC) (PDF→GGSN):

  The PDF uses the Remove_Decision to inform the GGSN that the PDF revokes the authorized resources for the client handle (PDP context). The Remove_Decision is a specific Decision message with the COPS Decision Flags object set to 0x02 ("Request-State" flag) and the Command-Code set to "REMOVE"; see IETF RFC 3084 [8].

  The event contains the following information:

  - Client Handle.

  The R-type = 0x08 for configuration request is used here and M-type = 0x04 terminate event state is used here.

3GPP TSG-CN WG3 Meeting #33 **Tdoc ⌘N3-040590**
Sophia Antipolis, France. 16th to 20th August 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.207** **CR** **134** ⌘**rev** **2** ⌘ Current version: **6.0.0** ⌘

*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 ☒

Title:	⌘	COPS-PR "Request State" flag not set for authorization failure decision
Source:	⌘	TSG_CN WG3
Work item code:	⌘	E2EQoS
Date:	⌘	09/08/2004
Category:	⌘	**A**
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:	⌘	Unclear if COPS-PR "Request State" flag needs to be set for authorization failure decision. The GGSN could expect this "Request State" flag as trigger to send DRQ message at authorization failure of an initial authorization request, see RFC 3084, Clause 3.3..
Summary of change:	⌘	COPS-PR "Request State" flag not set for authorization failure decision.
Consequences if not approved:	⌘	GGSN could fail to send DRQ message, causing state not to be removed at the PDF.

Clauses affected:	⌘	4.3.2.3, 5.1.1, 6.3.2

	Y	N		
Other specs Affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

4.3.2.3 Binding mechanism handling

The binding information is used by the GGSN to identify the correct PDF and subsequently request service-based local policy information from the PDF. Each set of binding information consists of an authorisation token and one or more flow identifier(s).

During the session set-up the PDF generates an Authorisation Token for the IMS session as described in RFC 3313 [22]. The Authorisation token shall be sent to the P-CSCF which forwards it to the UE in the SIP signalling. The PDF shall allocate its PDF identifier as part of the Authorization Token. This identifier shall be in the format of a fully qualified domain name.

The PDF receives the binding information and a Client Handle as part of a REQ from the GGSN. The PDF shall store the Client Handle for each flow identifier identified by the binding information for subsequent message exchanges.

The authorisation token is applied by the PDF to identify the IMS session. If no IMS session can be found for an authorisation token, or if the authorization token for the Client Handle has been modified, or if the PDF is otherwise unable to authorise the binding information, the PDF shall send a COPS decision message carrying both an INSTALL and REMOVE decision. The INSTALL decision shall identify an authorisation failure to the GGSN, and may include further details identifying the cause. The REMOVE decision shall subsequently remove this state from the GGSN. The "Request State" flag shall not be set within the REMOVE decision. For an initial authorisation, the GGSN will send a COPS Delete Request State (DRQ) message to the PDF to clean up the corresponding COPS handle state~~the PDF shall then initiate a remove for the authorisation request~~.

Next modified section

5.1 GGSN

5.1.1 Initial authorization at PDP context activation

The GGSN may receive binding information during the activation of a secondary PDP context by the UE. To perform initial authorization at the secondary PDP context activation the GGSN shall send an authorisation request to the PDF including the binding information received from the UE.

The GGSN identifies the required PDF from the authorisation token of the binding information. The authorisation token is formatted according to the structure of the policy element AUTH_SESSION defined in RFC 3520 [11]. The policy element AUTH_SESSION shall include the AUTH_ENT_ID and the SESSION_ID attributes. The GGSN checks for that Policy Element and retrieves the AUTH_ENT_ID attribute from this. If this is in the form of a Fully Qualified Domain Name, then this is used to identify the correct PDF.

The GGSN authorisation request message to the PDF shall allow the GGSN to request policy information for authorisation of the IP flows identified by the flow identifiers within the binding information carried by a PDP context.

When the GGSN receives the PDF decision, the GGSN shall enforce the policy decision. To enforce the policy decision, the GGSN shall install the packet filters received from the PDF, and ignore the UE supplied TFT.

If the PDF decision information indicates that the binding information provided by the GGSN is authorised, the GGSN shall proceed with activation of the secondary PDP context. The GGSN shall map the authorized QoS resources into authorized resources for the bearer admission control.

To ensure charging correlation, the GGSN shall send the GCID and GGSN address information to the PDF after the successful establishment of the secondary PDP context, i.e. with the report following the initial authorization decision.

When the PDF detects that the binding information provided by the GGSN is not associated with an ongoing SIP session at application layer, or is otherwise unable to authorise the binding information, the GGSN will receive a COPS decision message from the PDF carrying both an INSTALL and REMOVE decision. The "Request State" flag is not set within the REMOVE decision. The reason for the rejection is indicated by the INSTALL decision with an appropriate authorisation request failure reason. The GGSN shall reject the secondary PDP context activation with a corresponding error code, see annex D. The GGSN shall subsequently remove this state according to the REMOVE decision. For an

initial authorisation request, the GGSN shall then send a COPS Delete Request State (DRQ) message to the PDF to remove the state in the GGSN and the PDF.

When the GGSN sends an authorization request to the PDF but the PDF does not respond with the decision message or the communication between the GGSN and the PDF fails, the GGSN shall reject the secondary PDP context activation with the error code "Authorizing entity temporarily unavailable" (see annex D).

Next modified section

6.3.2 Message description

The following messages and events are available on the Go interface (after the initial policy provisioning described in subclause 6.3.1.5):

- Authorisation_Request (REQ) (GGSN→PDF):

  This event allows the GGSN to request authorisation data from the PDF. It contains the following information:

  - Client Handle;
  - Binding Information.

  The R-type = 0x08 for configuration request is used here and M-type = 0x02 create event state is used here.

- Authorisation_Decision (DEC)(PDF→GGSN), contains an INSTALL decision:

  This event provides the GGSN with the relevant authorisation data. The event contains the following information:

  - Client Handle;
  - ICID(s) (only in the initial Authorisation_Decision). Only one ICID is transferred in this Release. The form of the ICID is defined in 3GPP TS 32.225 [21];
  - Unidirectional set (this parameter shall appear once for each direction (uplink and downlink)):
    - Direction indicator;
    - "Authorised QoS";
    - Gate description (this parameter shall appear once for each required gate for this direction):
      - Filter Specification - The information about the authorised IP end points addresses and ports is detailed below. The Filter Specification parameters are:
        - Source IP address;
        - Destination IP address;
        - Source ports;
        - Destination ports;
        - Protocol ID.

          The Source and Destination ports are described with a range consisting of a minimum and maximum value. If only one port is authorised, the minimum value and maximum value of the range are identical.

          A filter specification describing more than one IP flow shall be only used in case of identical Protocol IDs, IP addresses and successive port numbers (e.g. RTP and RTCP IP flow of a media component). Furthermore, the gate status of all IP flows described by this filter specification shall be identical, too.

The Base and IP Filter definitions from the IETF Framework PIB [15] shall be used in the 3GPP Go PIB to represent the filter specification. Only a subset of the available filter attributes shall be used. The attributes frwkIpFilterDscp, and frwkIpFilterFlowId in the filter description shall have their values set to –1, indicating a "match-all" wildcard condition, in effect a "not used" condition. The attribute frwkBaseFilterNegation shall have its value set to "false" to indicate not using negation, in effect a "not used" condition. The GGSN shall ignore them if they are set otherwise. Wildcarding of filter elements is detailed in Annex B.

- Gate status (opened/closed)

The R-type = 0x08 for configuration request is used here and M-type = 0x02 create event state is used here.

- Authorisation_Failure (DEC) (PDF→GGSN), contains an INSTALL and a REMOVE decision:

This event provides the GGSN with an indication of an authorisation failure, and may carry additional reason details. The event contains the following information:

- Client Handle;
- Authorisation failure (including any provided reason information).

The R-type = 0x08 for configuration request is used here and M-type = 0x04 terminate event state is used here.

The COPS Decision Flags object 0x02 ("Request-State" flag) shall not be set for the REMOVE decision.

- Gate Decision (DEC) (PDF→GGSN), contains an INSTALL decision:

The Gate Decision indicates to the GGSN the new status of the gate(s) established for a client handle (PDP context). The gate status indicates to the GGSN that the gate shall be opened or closed. Only the gate(s) for which the status is changed are indicated by this event. The event contains the following information:

- Client Handle;
- Unidirectional set (this parameter shall appear once for each direction for which gates are being updated (uplink and/or downlink)):
  - Direction indicator;
  - Gate description (this parameter shall appear once for each gate to be modified for this direction) :
    - Filter Specification - The information about the authorised IP end points addresses and ports is detailed below. The Filter Specification parameters are:
      - Source IP address;
      - Destination IP address;
      - Source ports;
      - Destination ports;
      - Protocol ID.

        The Source and Destination ports are described with a range consisting of a minimum and maximum value. If only one port is authorised, the minimum value and maximum value of the range are identical.

        A filter specification describing more than one IP flow shall be only used in case of identical Protocol IDs, IP addresses and successive port numbers (e.g. RTP and RTCP IP flow of a media component). Furthermore, the gate status of all IP flows described by this filter specification shall be identical, too.

        The Base and IP Filter definitions from the IETF Framework PIB [15] shall be used in the 3GPP Go PIB to represent the filter specification. Only a subset of the available filter attributes shall be used. The attributes frwkIpFilterDscp, and frwkIpFilterFlowId in the filter description shall have their values set to –1, indicating a "match-all" wildcard condition, in effect a "not used" condition. The attribute frwkBaseFilterNegation shall have its value set to "false" to indicate not using

negation, in effect a "not used" condition. The GGSN shall ignore them if they are set otherwise. Wildcarding of filter elements is detailed in Annex B.

- Gate status (opened/closed)

NOTE: The opening of the gate may occur at the same time / be part of the authorisation decision event.

The R-type = 0x08 for configuration request is used here and M-type = 0x03 update event state is used here.

- Report (RPT) (GGSN→PDF):

  The GGSN sends a COPS RPT message as a response to a decision (DEC) message back to the PDF reporting that it enforced or not the Authorisation_Decision or the Authorization_Failure_Decision (Authorization_Report) or the Gate_Decision (Gate_Report).

  The events contain the following information:

  - Client Handle;
  - Success / Failure.

  In addition, the Authorization_report of the initial Authorisation_Decision includes:

  - GCID;
  - GGSN address.

- Report of state changes:

  The GGSN sends the report of state change message to the PDF reporting that the maximum bit rate for the PDP context is modified to 0 kbps or that the maximum bit rate for the PDP context is changed from 0 kbps.

  The event contains the following information:

  - Client Handle;
  - Maximum bit rate (set to 0 kbps / changed from 0 kbps).

- Delete Request State (DRQ) (GGSN→PDF):

  The GGSN informs the PDF via the delete request state message, that the PDP context is deactivated and the request state identified by the client handle is no longer available/relevant at the GGSN, so the corresponding state shall also be removed at the PDF.

  The DRQ message includes the reason why the request state was deleted.

  The event contains the following information:

  - Client Handle;
  - Reason code: value 4 "Tear", indicating the deactivation of the PDP context.

- Remove_Decision (DEC) (PDF→GGSN):

  The PDF uses the Remove_Decision to inform the GGSN that the PDF revokes the authorized resources for the client handle (PDP context). The Remove_Decision is a specific Decision message with the COPS Decision Flags object set to 0x02 ("Request-State" flag) and the Command-Code set to "REMOVE"; see IETF RFC 3084 [8].

  The event contains the following information:

  - Client Handle.

  The R-type = 0x08 for configuration request is used here and M-type = 0x04 terminate event state is used here.