3GPP TSG SA WG3 Security — S3#29 **S3-030432**
15 - 18 July 2003
San Francisco, USA

3GPP TSG-SA WG2 Meeting #33 **Tdoc S2-032745**
Sophia Antipolis, France, 7th - 11th July, 2003

Title: **LS on Security Implications of Gq interface**
Response to: -
Release: **Release 6**

Source: **SA WG2**
To: **SA WG3**
Cc:

Contact Person:
Name: Brian Williams
Tel. Number: +61 3 9301 4675
E-mail Address: brian.williams@ericsson.com

Attachments: TR 23.917 v0.8.0 (most recent version)

---

1. Overall Description:

The TR 23.917 introduces a new interface (Gq) from an application function to the PDF. The Gq interface may be inter- or intra-operator, or to a third party.

SA WG2 has now approved a work item for the introduction of the Gq interface into the SA WG2 specifications.

2. Actions:

To SA WG3.

ACTION: TSG SA2 kindly asks TSG SA3 to consider the security implications of the Gq interface which may be intra-operator or to a third party, and to identify the requirements for security that apply to this interface, and provide direction for what authentication, authorisation and protection mechanisms shall be employed for this interface.

3. Date of Next TSG-SA WG2 Meetings:

TSG-SA WG2 Meeting #34	18th – 22nd August 2003	Brussels, Belgium.
TSG-SA WG2 Meeting #35	27th – 31st October 2003	Asia.

3GPP TR 23.917V0.8.0 (2003-05)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Dynamic Policy control enhancements for end-to-end QoS; (Release 6)

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Remove GSM logo from the cover page for pure 3rd Generation documents.

Select keywords from list provided in specs database.

Keywords

<keyword[, keyword]>

3GPP

Postal address

3GPP support office address

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

Internet

http://www.3gpp.org

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

1 Scope

This document studies how the policy control is used for IMS and interacts with the appropriate IMS and non-IMS application servers. This document investigates the feasibility of the interface between the PDF and application entities (e.g. P-CSCF in the IM domain). The feasibility study determines the requirements and architecture for this work.

2 References

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

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

[1] 3GPP TR 21.905: "3G Vocabulary".

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

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

[4] 3GPP TS 29.207: " End to end Quality of service (QoS); stage 3".

3 Definitions, symbols and abbreviations

For the purposes of the present document, the terms and definitions given in [1] and the following apply.

3.1 Definitions

3.2 Symbols

3.3 Abbreviations

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

ABC Axxx Bxxx Cxxx

Other abbreviations used in the present document are listed in 3GPP TR 21.905 [1].

4 Introduction

In release 5, the service-based local policy control provides a way to manage the access network through dynamic policies over the Go interface.

The release 5 IMS work uses a policy decision function (PDF) that is only applicable for IMS and tightly linked to the SIP session control. This does not enable a generic service policy to be applied to both IMS and non-IMS services.

Within Release 5 the PDF is shown as being a logical entity of the P-CSCF. Standardising the interface between the PDF and application entities (e.g. P-CSCF in the IM domain) was pushed back to release 6.

In this document the means by which policy control is used for IMS and interacts with the appropriate IMS and non-IMS applications, is studied.

The objectives are to:

- Enable general policy control over IP bearer resources and SIP services to evolve separately.
- Enable more flexibility in engineering and policy control of IP bearer resources.
- De-couple policy functions from IMS entities.

5 Background

As shown in figure 1, in release 5, the IM Subsystem is closely coupled with the UMTS Core Network.

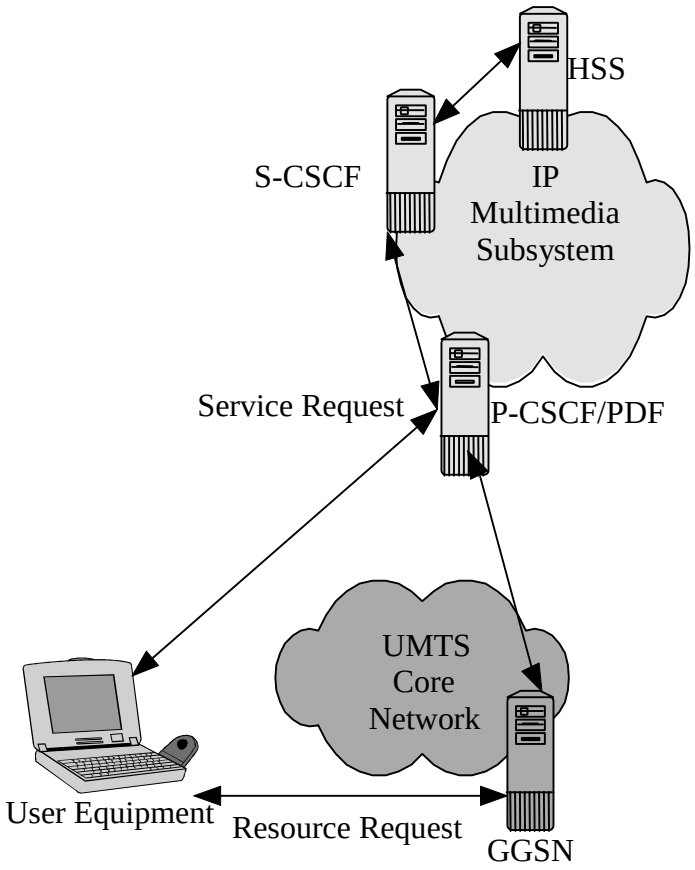


Figure 1: Policy Architecture in release 5

Although the PDF and P-CSCF are two separate logical entities, the release 5 3GPP specifications present the PDF as being an integral part of the P-CSCF. The consequence of this close coupling is that only the IP Multimedia Subsystem may authorize UMTS resources for their customers. The means for other services than IMS to authorize UMTS resources has not been standardised in Release 5.

6 Objectives

Opening the interface between the PDF and the P-CSCF may greatly simplify introduction of new services and enable operators to leverage their ownership of the access network by introducing opportunities for service-based control of the access for a whole range of services (potentially including third party services) in an operator controlled manner.

Decoupling of the PDF & P-CSCF could:

- Enable service based local policy control over IP bearer resources and SIP services to evolve separately.
- Facilitate future application of service based local policy control over IP bearer resources for non-SIP services (e.g., streaming services, etc.) that the operator will want to deploy.
- Improve network scalability/stability by allowing the decoupled functions to be scaled/upgraded independently according to network requirements.
- Encourage more flexibility in engineering and policy control of IP bearer resources. This means that policy control mechanisms for IP bearer resources related to SIP- & non-SIP-based

services, as well as their related IP bearer resources, can be controlled either together or separately.

In order to obtain all these benefits related to distributed policies, a generic protocol should be used allowing any service domain to provide session authorization to their customers in a particular access network.

Figure 2 shows the IM Subsystem as well as other services, in relation to the UMTS Core Network. Decoupling of the PDF from the P-CSCF enables policy control to be applied for other services than SIP IMS services.

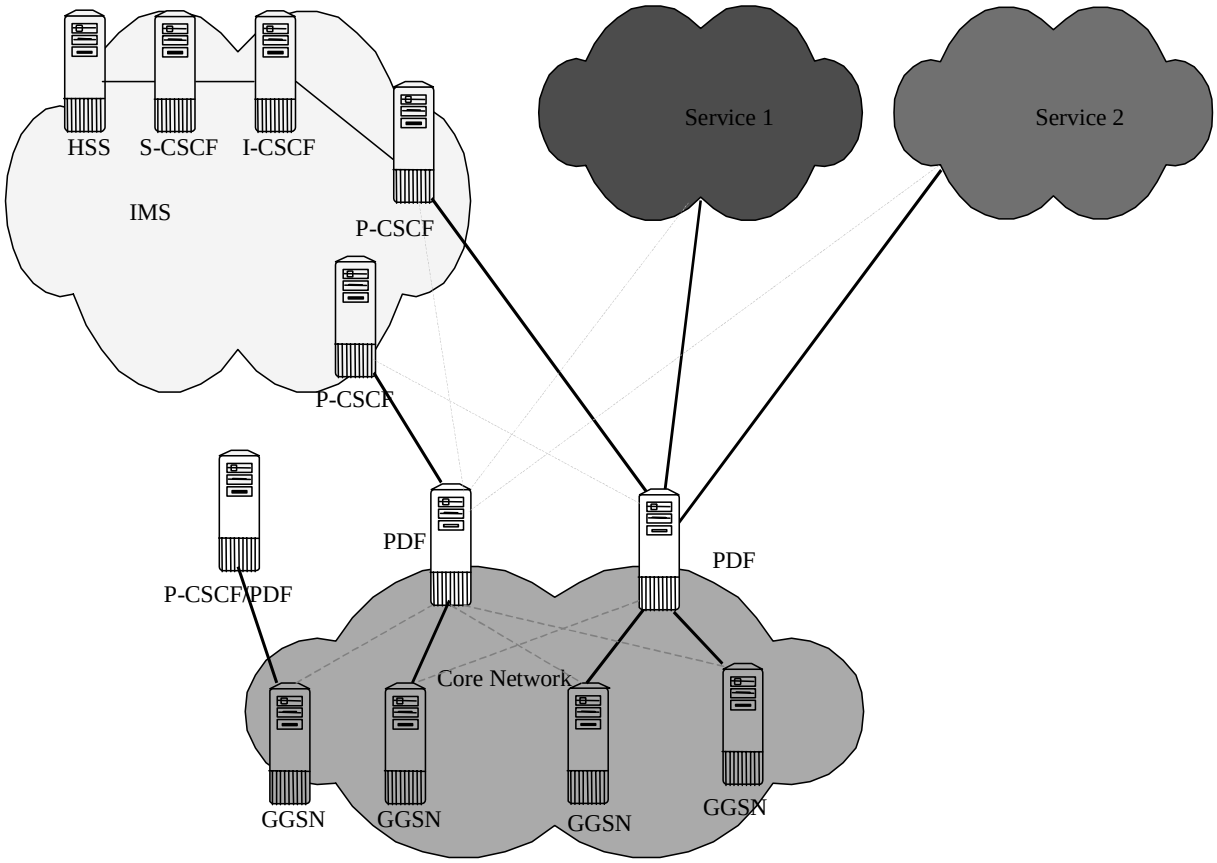


Figure 2: Policy applied to IMS and other services, also showing an integrated P-CSCF/PDF

The benefit of the service-based policy control for services including the following will be investigated in this technical report.

- Services not related to IMS
    - 3GPP PSS based streaming services
- Services related to IMS
    - IMS signalling bearer
    - IMS emergency sessions

7 Architecture

7.1 Introduction

There are three main elements to the rel6 policy control architecture:

- the GGSN
- the PDF
- the server in the operator's or service provider domain (e.g. P-CSCF for the IM Subsystem), or "Application Function".

7.2 Description of functional entities

7.2.1 GGSN

The Gateway GPRS Support Node (GGSN) is defined in TS 23.002 [2].

The procedures for information transfer between the GGSN and the PDF are defined in TS 23.207 [3] and TS 29.207 [4].

7.2.2 PDF

The Policy Decision Function (PDF) acts as a Policy Decision Point for service based local policy control.

7.2.3 Application Function

The Application Function is an element controlling applications that require the use of IP bearer resources (e.g. UMTS PS domain/GPRS domain resources). One example of an application function is the P-CSCF.

The Application Function represents the application level intelligence for any service running over the IP bearer which needs service based policy control, and should not be confused with SIP Application Servers, OSA Application Server, or CAMEL IM-SSF defined in TS 23.228.

7.3 Relationship between functional entities

The following principles apply for the GGSN/PDF/Application Function relationships for the rel6 policy control architecture, in line with release 5:

There are multiple instances of the Application Functions, GGSNs and PDFs.

The GGSN and the associated PDFs exist within the same operator's network and are provisioned to know about each other (e.g., configured with a list of allowed names/addresses).

The AF and the PDF need not exist within the same operator's network. They may be provisioned to know about each other or one may discover the other and establish a secure relationship.

The GGSN, Application Function and PDF involved in establishing the session are not known a priori.

There are pre-defined trust relationships between the GGSN and the PDF.

Further, the following rules apply:

- One GGSN may get policy information from multiple PDFs. Different PDFs do not take decisions on the same resources of a single GGSN.
- A given PDF may give policy information to a number of GGSNs
- One PDF shall be able to serve more than one Application Function
- For IMS services which PDF the GGSN needs to go to is identified by the authorization token
- The GGSN knows which PDFs are part of its network. This is for security reasons. The GGSN must have a list of valid PDFs to prevent a UE from tampering with the authorization token in order to redirect the GGSN to a fake PDF.
- A given Application Function may interact with a number of PDFs, although on a per-session basis, it shall interact with only a single PDF.

For IMS, where P-CSCF is the Application Function:

- The authorization token is generated by the PDF and contains its identifier (FQDN)
- A given PDF may interact with a number of P-CSCFs

For service based policy control, the AF does not interact with the GGSN directly; instead, it interacts with the PDF and the PDF acts on certain events as instructed by the AF.

7.4 Functions with Policy Control

[Editor's Note: This section identifies the individual functions that are provided for policy control. Under each individual function, a description of the function and the distribution over the functional elements can be made. It can also indicate open questions for each function.]

7.4.1 Authorise QoS resources

There may be links between the AF and PDF policies to authorise the use of QoS resources.

The AF provides the service determined decision information.

The PDF provides the final policy decision controlling the allocated QoS resources for the authorized media stream to the GGSN.

When the AF requests the token from the PDF, it indicates whether or not the PDF should contact the AF at UE resource reservation.

The Authorise QoS resources function can be invoked between PDF and AF at session establishment and/or at bearer establishment.

The UE decides whether to aggregate or separate flows. The total QoS authorised may depend on which flows the UE decides to multiplex. Depending on the flows and the application, there may be some multiplexing gain (e.g. it may be that some flows never transmit at the same time).

As the AF can request to be contacted at UE resource reservation, it can interact with the PDF so that the PDF enforces downgraded bandwidth usage if the UE has asked for more bandwidth than the AF allows.

Further, the AF may provide information to the PDF in order for the PDF to authorise aggregate of flows.

In the case the AF does not request to be contacted at UE resource reservation, and that no additional information is available at the PDF, the PDF authorisation will be based on the addition of bandwidth of flows proposed by the UE.

For some services, the authorisation decision may be time dependent (e.g. a different authorisation is applicable at a different time). Further, different services may make the authorisation decision for the flow at the AF at the time the flow is identified, and others may make this authorisation decision at the AF at the time the bearer is established. If a time dependent decision at the AF needs to be made at bearer establishment, the AF shall request the PDF to contact the AF at UE resource reservation.

7.4.2 Exchange of information for charging correlation

IMS charging information is available from the P-CSCF for the PDF which is required to transfer it to the GGSN.

GPRS charging info available in the PDF is required to be transferred to the AF.

7.4.3 Enable flow

The AF determines when a flow is to be enabled to pass through the access network.

The PDF opens the gate in the GGSN when ordered from the AF.

7.4.4 Disable flow

The AF determines when a flow is to be disabled from passing through the access network.

The PDF closes the gate in the GGSN when ordered from the AF.

7.4.5 Revoke authorisation

The AF determines when a previous authorisation decision is no longer approved, and orders the removal of the previously authorised resources.

The PDF revokes the QoS resources when ordered by the AF. This results in removing the allocated resources in the GGSN.

The authorisation can be revoked altogether i.e. revoke the token and all related authorisations. An example trigger for this is a session release message received at the AF.

If the session changes at the Application Function, an update of the previous authorisation may be given to the PDF.

7.4.6 Indicate bearer release/failure

Information available at the PDF on the bearer resource release or failure is passed through to the AF.

7.4.7 Confirm bearer reservation

The PDF may forward bearer reservation indications to the AF which confirms whether the previous resource authorisation should still be applicable.

7.5 Description of interfaces

The Rel6 policy control makes usage of:

- The interface between the GGSN and the PDF (Go interface) for service based local policy control.

  The Go interface ensures that the PDF policy decisions are applied at the GGSN over the UMTS PS domain/GPRS and over the Gi interface.

- The interface between the Application Function (e.g. P-CSCF for the IM Subsystem) and the PDF (Gq interface) for service-based policy control.

  The Gq interface ensures that the PDF policy decisions are applied for the service requesting access to IP bearer resources.

  Gq interface may be intra- or inter-domain. Gq supports integrity protection and authentication in case, the Application Function is outside the operator domain.

7.6 Binding mechanism handling

This refers to the binding between any session information that may be provided by the Application Function, and the authorisation of QoS resources usage for that application, by the PDF. The binding mechanism for service based policy control uses an authorisation token. The authorization token is passed among the PDF, AF and GGSN and is linked with session bearer information. Since PDFs, AFs, and GGSNs, may exist in many to many relationships, the specific GGSN and PDF and the specific PDF and AF supporting a particular session must be known to each other. The AF may be provisioned to know about the PDF or the AF and PDF may discover each other by other means.

In response to a session bearer authorization request from the AF, an authorization token is generated by the PDF and is passed back to the AF. The following are possible:

1. The PDF authorizes QoS resources usage for that application for a particular session and user. The authorization token is only valid for the duration of the session for the specific user.
2. The AF requests multiple authorization tokens. The PDF provides the requested number of authorization tokens. Each of these tokens may later be allocated to a session, and then used for subsequent QoS resource usage authorization procedures for the duration of the session for the specific user.

This authorization token is used in the initial communications between the PDF and the GGSN to identify bearers related to this session. If the authorization token is not yet related to a session bearer authorization request it is also used in the initial communications between the PDF and the AF. It contains the address of the PDF that has assigned the authorization token. The AF later passes this authorization token to the UE which then passes it when requesting a bearer from the GGSN.

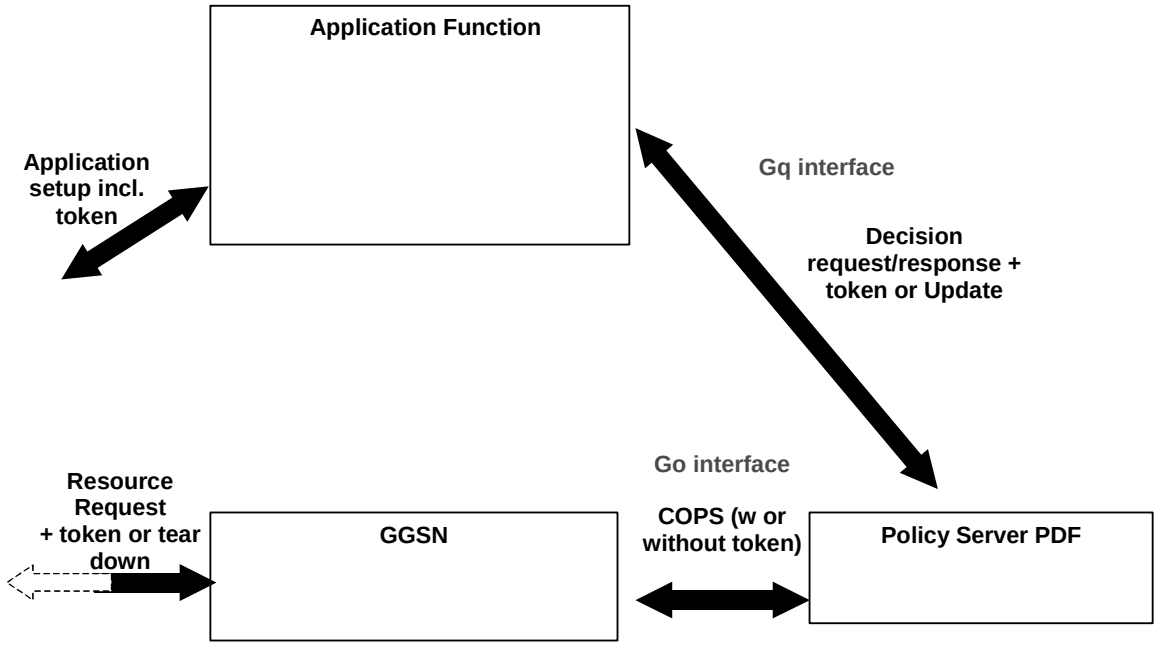
The flows in Section 8.3 ‘Authorisation of QoS resources’ show an example of this binding case.

8 Information flows

For distributed policies, a generic protocol should be defined allowing any Application Function to provide session authorization to their customers in a particular access network. A number of different scenarios are described here which all have the common point of requiring a dynamic policy decision.

8.1 General operation of Gq interface

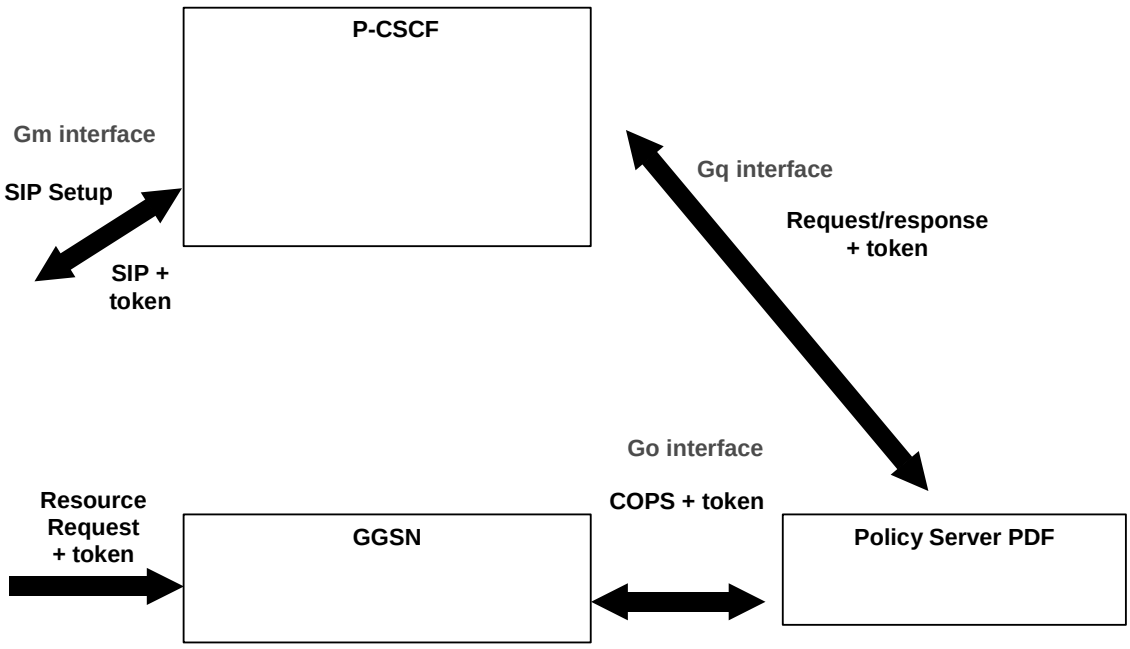
The GGSN resources are used by an Application Function. The interface between the Application Function and the PDF is used for service based policy control. The PDF exchanges requests/indications with the Application Function.



8.2 Example usage with IMS

8.2.1 IMS Session setup

The following picture shows a high-level view of release 5 information flows over the Gm and Go interface, during session setup, as well as information exchange over the Gq interface between P-CSCF and PDF.



Over the Gm interface, SIP session control is exchanged between UE and P-CSCF.

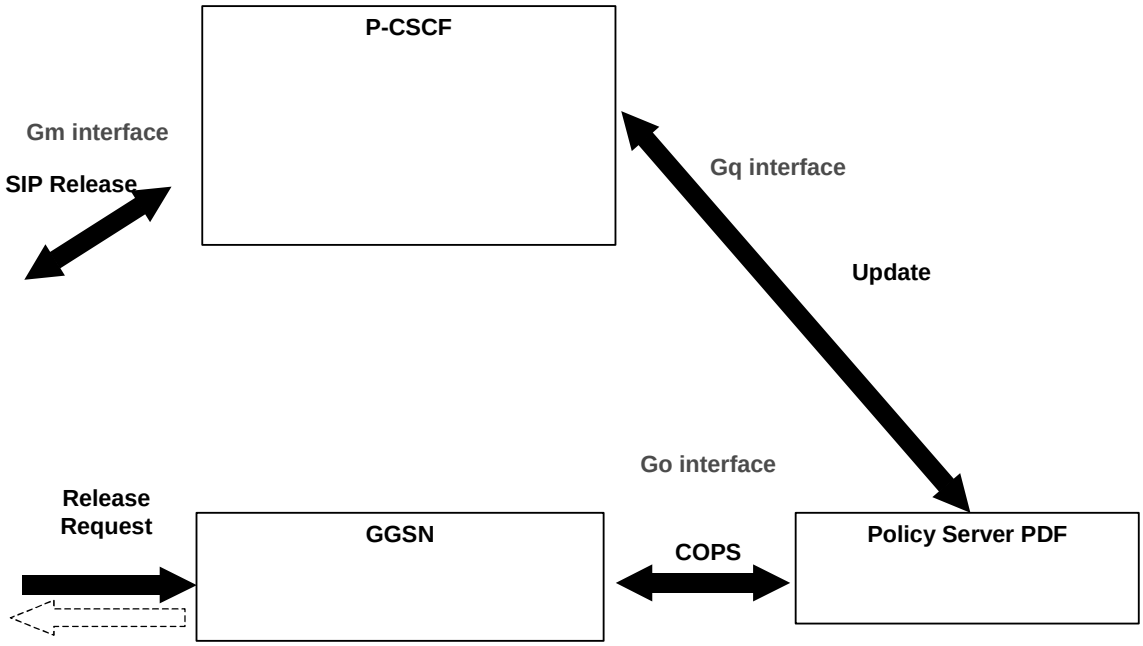
Over the Gq interface, information is exchanged between the Application Function (P-CSCF) and the PDF, for policy decisions.

At the GGSN, resources are requested for the related session. Policy is enforced at the GGSN following information exchanged with the PDF over the Go interface.

The authorisation token is exchanged over those interfaces as required.

8.2.2 IMS Session teardown

The following picture shows a high-level view of release 5 messaging over the Gm and Go interface, during session teardown, as well as information exchange over the Gq interface between P-CSCF and PDF.



Over the Gm interface, SIP session control is exchanged between UE and P-CSCF.

Over the Gq interface, information is exchanged between the Application Function (P-CSCF) and the PDF, for policy decisions.

At the GGSN, resources are released for the related session. Update information is exchanged between the GGSN and the PDF over the Go interface.

8.3 Authorisation of session QoS resources

This is the initial interaction between PDF and AF.

When the AF requests the authorization token from the PDF, it indicates whether or not the PDF should contact the AF at UE resource reservation. The PDF generation of the authorization token is

shown in the flow “Authorisation of service, session establishment”. In the case where the AF provides session QoS information, the PDF returns a success indication with an authorization token when the identified QoS is within operator policy. In the case where the AF does not provide session QoS information, the PDF may return an authorization token to be used in a subsequent authorisation procedure.

The AF provides information about whether or not the PDF should contact the AF when the QoS is modified by the UE, for example if there is a change in the allocation of flows to the authorized resources.

The PDF can only provide this modification information to the AF if it receives corresponding information from the Go interface.

8.3.1 Authorisation of QoS resources, session establishment

The following flow shows the authorisation of the QoS resources at session establishment. This step is necessary for the AF to request the generation of any authorization token by the PDF.

For a particular user and session, the PDF generates one authorization token which is valid for the related session and user.

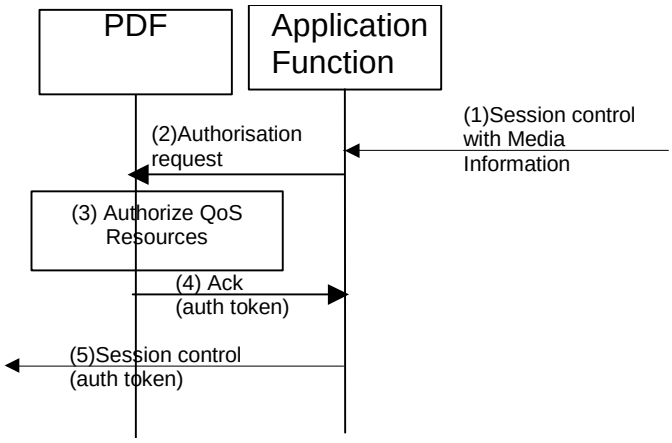


Figure 3: Authorize QoS resources, session establishment

1) A trigger is received at the AF, e.g. a session Control message containing media information is received by the Application Function.

2) The Application Function sends a request for authorization token and optionally session information to the PDF. Some services may require further interaction between the AF and the PDF to provide the full session information, e.g. for IMS session establishment (mobile terminated).

3) If the PDF received the session information, the PDF shall authorize the required QoS resources for the session and install the IP bearer level policy in its internal database based on information from the Application Function. If the session QoS information was not received in Step 2 above, the QoS authorisation is deferred.

4) The PDF reports successful or deferred QoS authorisation of the session, to the Application Function. The requested Authorisation Token shall be included.

5) Upon successful or deferred authorization of the session, session control messaging continues, with the supplied Authorisation Token being passed on the UE.

It is also possible that the AF may initiate a request for multiple authorization tokens to use for future sessions, in which case the PDF can generate multiple authorization tokens. When the AF receives multiple authorization tokens from the PDF, it may allocate these to sessions without re-contacting the PDF.

8.3.2 Authorisation of QoS resources, bearer establishment

At bearer establishment, the PDF can contact the AF. This may be done in the case that the previous interaction at session establishment requested this, or when the previous interaction did not include QoS information for authorisation at that time. This further step is used for confirmation of reservation as required by the AF.

The following flow shows the authorisation of the QoS resources at bearer establishment.

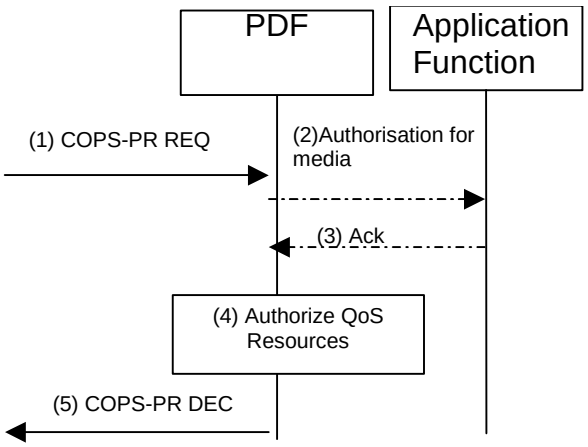


Figure 4: Authorize QoS resources, bearer establishment

1) A COPS-PR REQ is received over the Go interface at the PDF.

2) A PDF generated authorization token enables the PDF to identify the authorisation status information. If the previous PDF interaction with that AF had requested this, or if the previous interaction with the AF did not include QoS information, the PDF sends an authorisation message to that Application Function.

3) The Application Function sends the authorisation information (e.g. QoS, filter information) to the PDF.

4) The PDF shall authorize the required QoS resources for the session and install the IP bearer level policy in its internal database. This is based on information from the Application Function in the case AF information was received.

5) The PDF sends further Go messaging.

8.3.1 Example of authorisation of QoS resources, P-CSCF is Application Function

One example of usage of the authorisation flow above is at IMS session setup. This scenario is shown below:

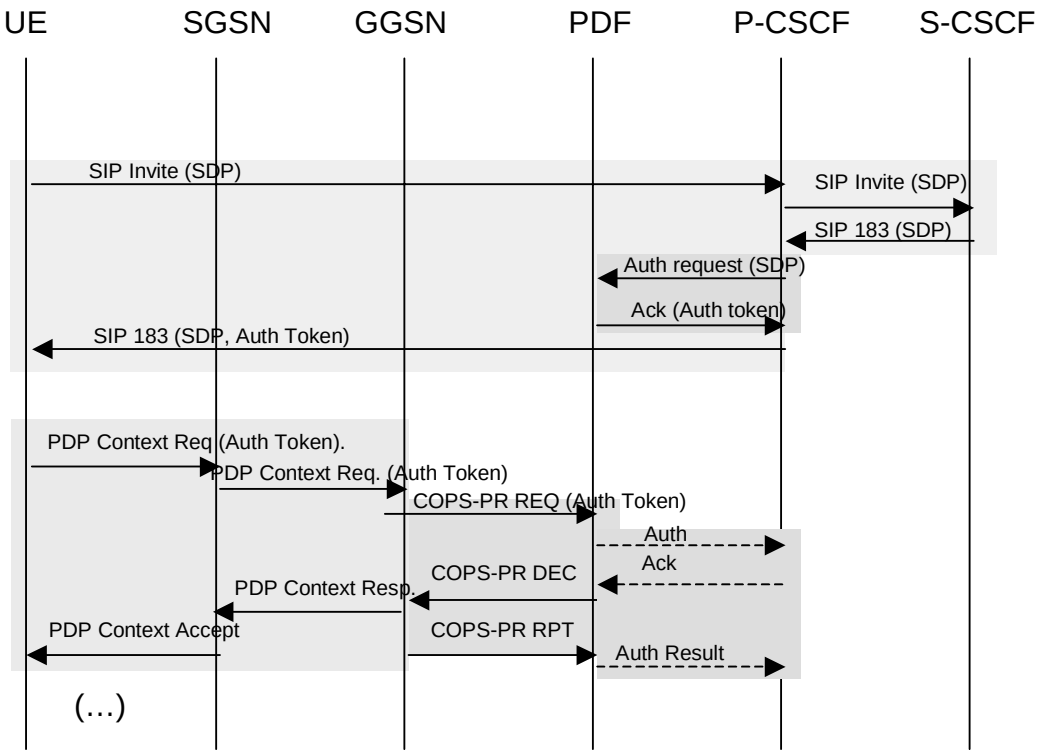


Figure 5: Example Information flow for IMS session set-up

The P-CSCF sends an authorisation request message to the PDF to request an authorisation token. The message may include SDP information. All possible interactions between P-CSCF and PDF at this stage are not shown in this call flow. The P-CSCF may provide sufficient information to enable the PDF to make authorization decisions.

The PDF uses the information received from the P-CSCF in order to authorize the necessary QoS resources.

An authorisation token is generated by the PDF. The authorisation token is a globally unique value. This authorisation token includes the PDF identifier. The PDF identifier ensures that the GGSN knows which PDF to contact for Go interface flows.

The PDF sends an acknowledgement message to the P-CSCF containing the Authorisation Token.

If the P-CSCF had requested to be instructed at resources setup, the PDF further interacts with the P-CSCF on bearer establishment. The P-CSCF makes an IMS decision on the authorisation and sends authorisation information to the PDF. The PDF makes an authorisation decision which is communicated to the GGSN. The successful installation of the decision is reported to the P-CSCF.

8.4 Approval of QoS commit

The PDF uses information received from the application function, in order to enable the authorised QoS resources.

The PDF controls the gate(s) but opens the gate(s) only if it gets an indication from the Application Function. Depending on operator configuration the Application Function may also enable the authorised QoS resources during the authorization procedure.

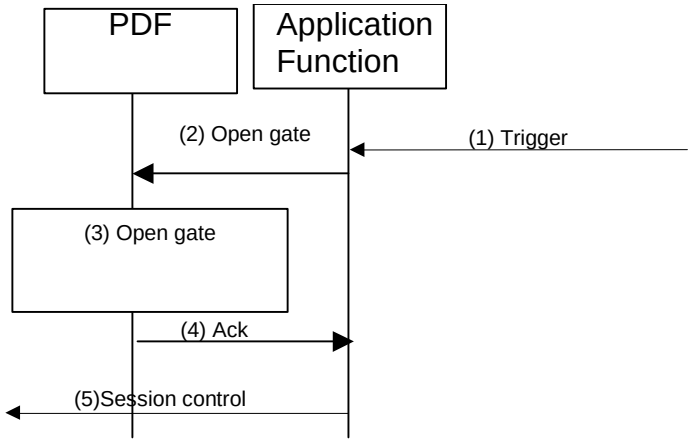


Figure 6: Approval of QoS commit

1) A trigger is received at the AF e.g. a Session Control message is received by the Application Function, or an internal action at the AF triggers the need to enable the flow for the application.

2) The Application Function sends an open gate indication to the PDF.

3) The PDF enables use of authorised QoS resources.

4) The PDF reports the successful operation to the Application Function.

5) Session control continues.

8.4.1 Example of approval of QoS Commit, P-CSCF is Application Function

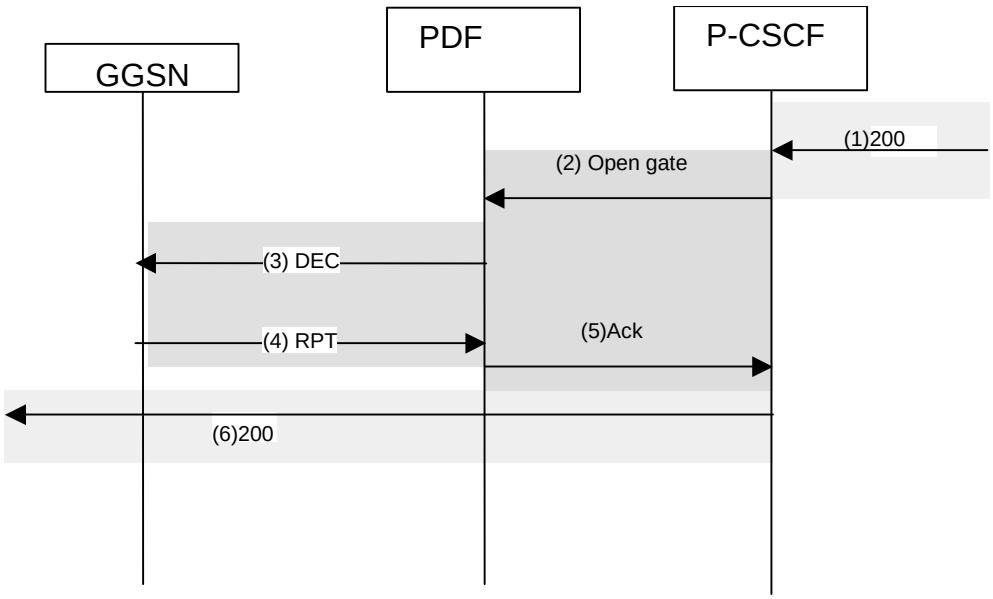


Figure 7: Example IMS flow of approval of QoS Commit

1) The P-CSCF receives the 200 OK response to the INVITE request.

2) The P-CSCF sends a message to the PDF to indicate the opening of the gate.

3) The PDF shall send a COPS DEC message to the GGSN to open the 'gate' e.g., enable the use of the authorised QoS resources.

4) The GGSN receives the COPS DEC message and opens the 'gate' e.g., enables the use of the authorised QoS resources, and sends a COPS RPT message back to the PDF.

5) The PDF informs the P-CSCF that the gate was successfully open.

6) The P-CSCF forwards the 200 OK message to the UE for the originating side and for the terminating side, to the terminating S-CSCF.

8.5 Authorisation of modification of network resources

This procedure is used when a modification of network resources happens which is outside of the limits that were authorized at network resource activation (or last modification).

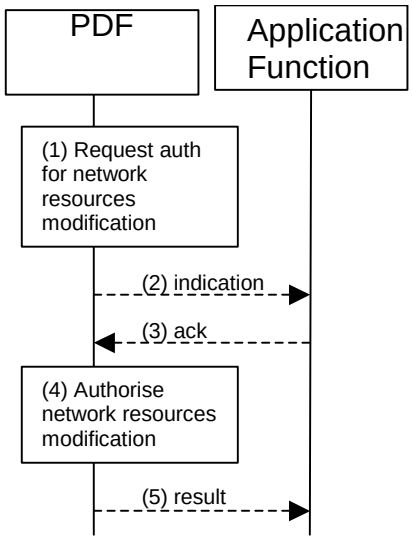


Figure 8: Authorisation of network resources modification

1) The PDF is requested to authorise a network resources modification

2) The PDF may give this bearer modification indication to the Application Function. This may be the case if this was requested from the AF at initial authorisation, and if PDF requires more information from the AF before authorising the network resources modification.

3) The AF shall send information for authorization of this modification.

4) The PDF authorises the network resources modification

5) In case the PDF had contacted the AF in 2) then the successful installation of the decision is reported to the AF

8.5.1 Authorisation of network resources modification, PDP context modification to IMS

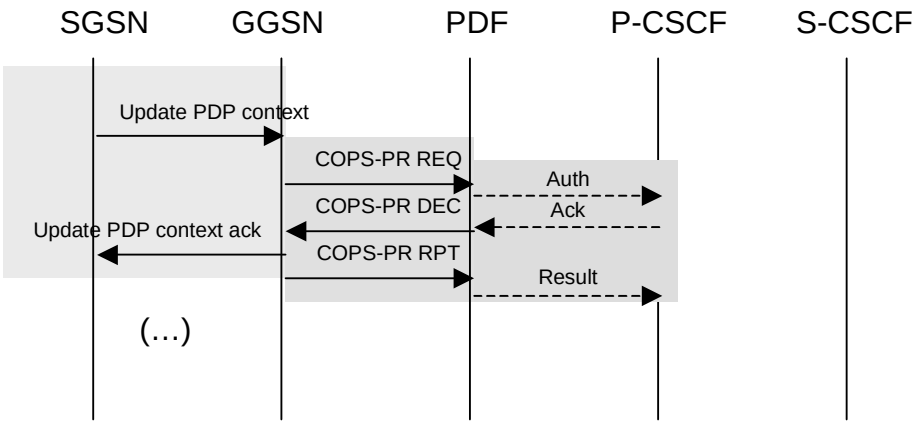


Figure 9: Example of information flow for authorisation of PDP context modification towards IMS

The PDF is requested to authorize the modification of the network resources previously authorized.

This is done via the Go interface with the COPS-PR REQ message.

The PDF may authorize the modification request at this point. If required for the authorization to proceed, the PDF may send an authorization request to the P-CSCF. In this case, the P-CSCF shall send an answer with information for authorization of this modification and the PDF shall report the result to the P-CSCF.

8.6 Indication of network resources events

This procedure is used when an event, e.g. a loss of coverage, happens in network resources. It does not require the PDF to perform an authorisation for this modification.

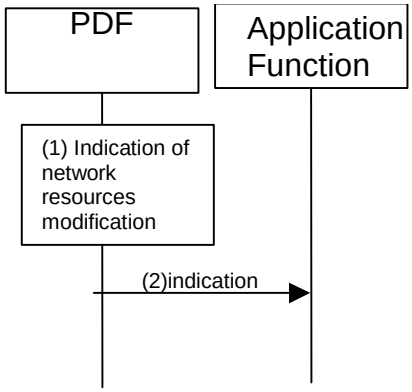


Figure 10: Indication of network resources modification

1) The PDF is instructed of a network resources modification

2) If this modification matches the criteria for which that the AF had requested to be informed, the PDF shall give this bearer modification indication to the Application Function

8.6.1 Indication of network resources modification, PDP context modification to IMS

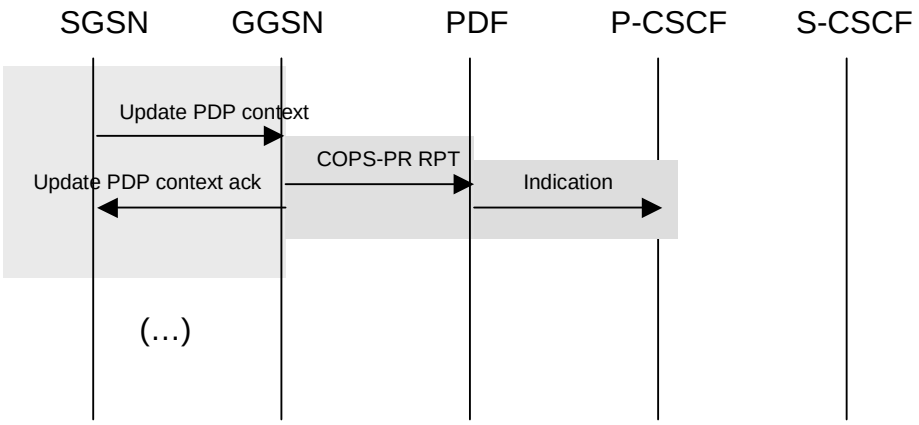


Figure 11: Example of information flow for indication of PDP context modification towards IMS

The PDF is informed about the modification of the network resources previously authorized.

This is done via the Go interface with the COPS-PR RPT message.

In this case, the PDF had received an indication from the P-CSCF to report any modification, therefore the PDF sends an indication to the P-CSCF.

8.7 Revoke Authorization for the session

8.7.1 Revoke Authorization for the session, Application Function initiated

This procedure is used e.g. upon session release. This step may contain the removal of the QoS resources. If not then this is done separately with a removal of QoS commit procedure.

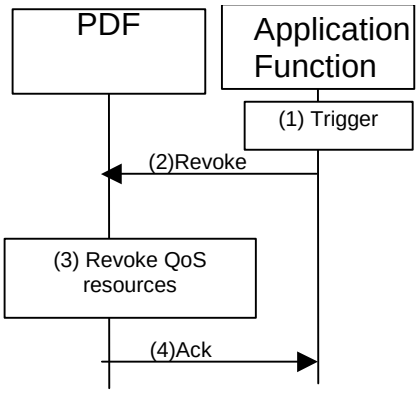


Figure 12: Revoke Session Authorization, Application Function initiated

1) A trigger is received at the AF e.g. a session control message exchange, or an internal action at the AF triggers the need to revoke the authorization, or the AF received an indication of network resources removal and decides to revoke the authorization

2) The Application Function sends a message to the PDF to indicate the revocation.

3) The PDF when it is informed of the revocation, revokes the related QoS resources which had been previously authorised. The PDF also records that the associated token value is no longer used.

   The revoke signalling between AF and PDF shall support indicating a revoke for the whole service previously authorised.

4) The PDF indicates the successful execution of the revoke indication.

8.7.2 Revoke Authorization for the session, PDF initiated

In this scenario the PDF initiates the release of the session. This may only happen in case the AF allows the PDF to revoke the service. If the PDF is allowed to revoke the service, this may happen for a number of reasons e.g. there is some time restriction.

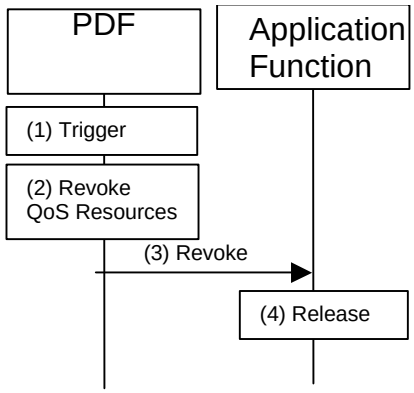


Figure 13: Revoke Session Authorization, PDF initiated

1) The PDF decides to revoke the authorization

2) The PDF revokes the related QoS resources which had been previously authorised. The PDF also records that the associated token value is no longer used.

3) The PDF indicates the revoke of the authorisation to the AF.

4) The AF releases the session or terminates the service by e.g. sending appropriate control messages.

8.7.3 Revoke for IMS Session release, P-CSCF is Application Function, P-CSCF initiated

One example of usage of the revocation flow above is at IMS session teardown. One IMS teardown possible scenario using the revocation flow is shown below.

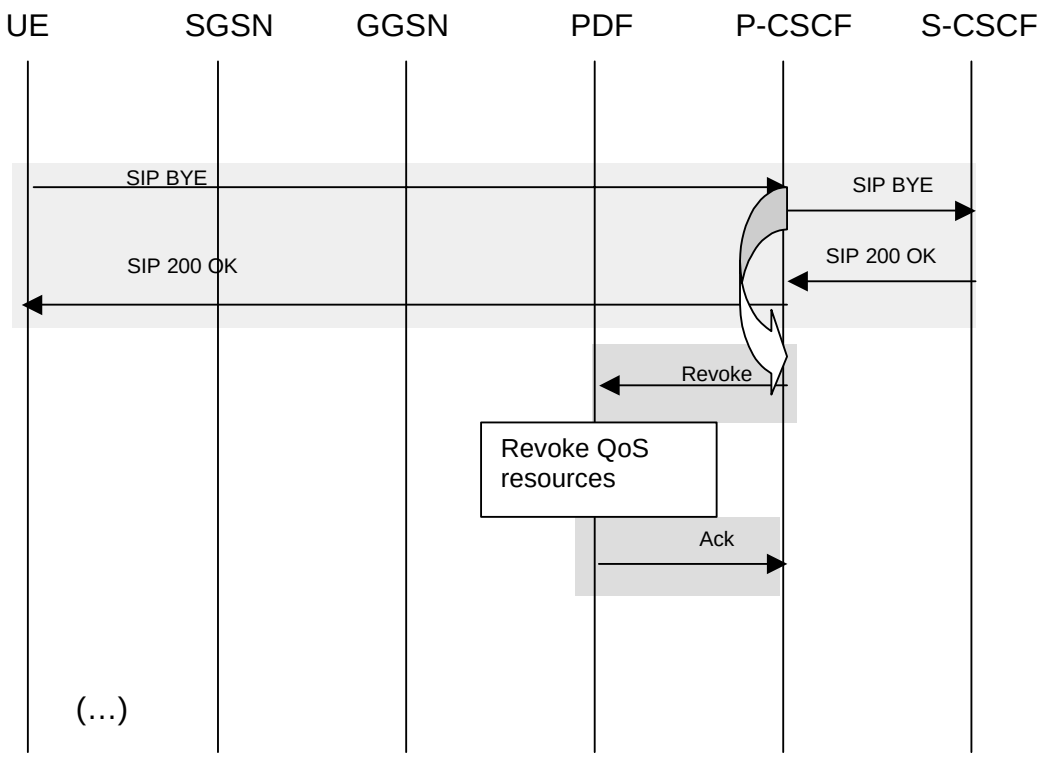


Figure 14: Example of information flow for IMS session release, P-CSCF initiated

In this scenario, upon receiving SIP BYE the P-CSCF sends a message to the PDF to revoke the authorisation. This indicates to the PDF that the token value needs to be released and all related authorisations are no longer valid. The PDF then revokes the related QoS resources.

8.8 Update Authorization for the session

If the session changes at the Application Function, an update of the previous authorisation may be given to the PDF. This is shown in the flow below:

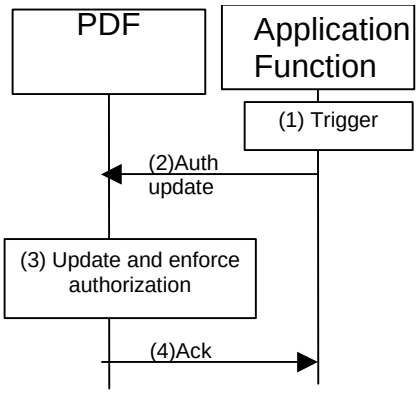


Figure 15: Update Authorisation for the session

1) At the AF, e.g. through modification of the session at session control level, there is a need to give updated information to the PDF.

2) The AF gives the updated information to the PDF

3) The PDF enforces the updated authorisation via the appropriate Go procedures, e.g. via the revoke GPRS and IP resources procedure.

4) The PDF sends an acknowledgement to the AF

8.9 Removal of QoS commit

The "Removal of QoS commit" procedure is used e.g. when a media component of a session is put on hold. (e.g. in case of a media re-negotiation or call hold).

The PDF uses information received from the Application Function, at the session control level, in order to disable the authorised QoS resources. The PDF controls the gate(s) but closes the gate(s) only if it gets an indication from the Application Function. Depending on operator configuration the Application Function may also disable the authorised QoS resources during the revoke authorization procedure.

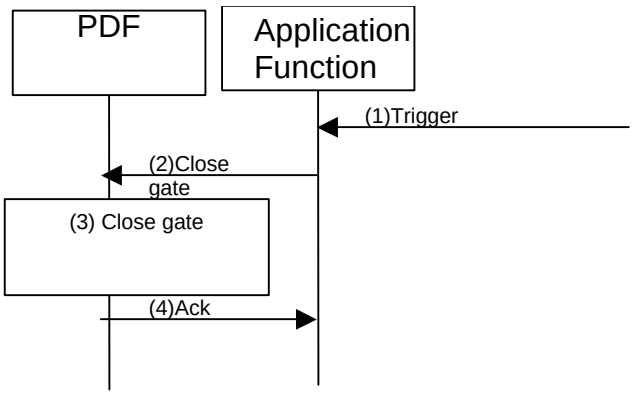


Figure 16: Removal of QoS commit

1) A trigger is received at the AF e.g. a session control message exchange, or an internal action at the AF triggers the need to stop the flow for the application.
2) The Application Function sends a close gate indication to the PDF.
3) The PDF takes the appropriate actions to close the gate
4) The PDF reports that the gate was closed.

8.9.1 Removal of QoS Commit, P-CSCF is Application Function

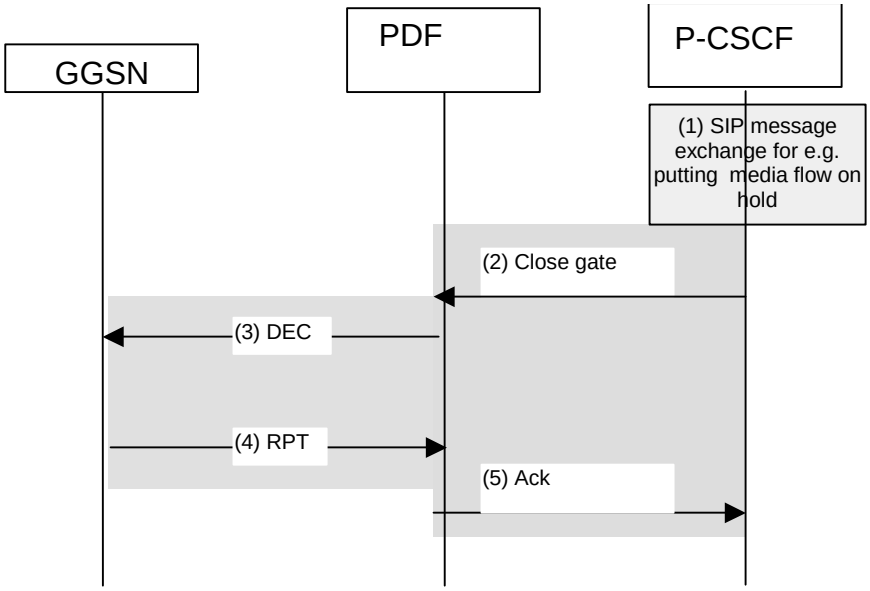


Figure 17: Example of IMS flow for Removal of QoS commit

1) SIP message exchanges for e.g., putting a media flow on hold are carried out.

2) The P-CSCF sends a message to the PDF to indicate the closing of the gate.

3) The PDF shall send a COPS DEC message to the GGSN to close the 'gate'.

4) The GGSN receives the COPS DEC message, closes the gate, and sends a COPS RPT message back to the PDF.

5) The PDF informs the P-CSCF that the gate was successfully closed.

8.10 Indication of network resources removal

This procedure is used e.g. upon GGSN deletion of PDP context. It may trigger the PDF to revoke the authorization. It may trigger the PDF to instruct the Application Function.

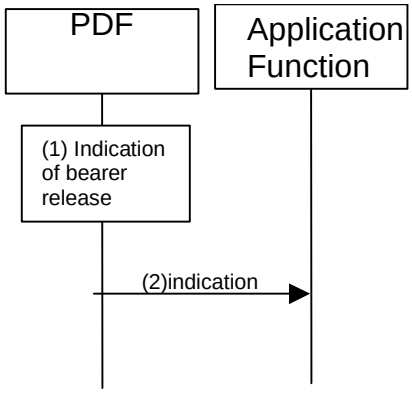


Figure 18: Indication of bearer removal

1) The PDF is instructed of a network resources removal

2) The PDF may revoke the authorization. The PDF may give this bearer removal indication to the Application Function.

8.10.1 Indication of network resources removal, PDP context release to IMS

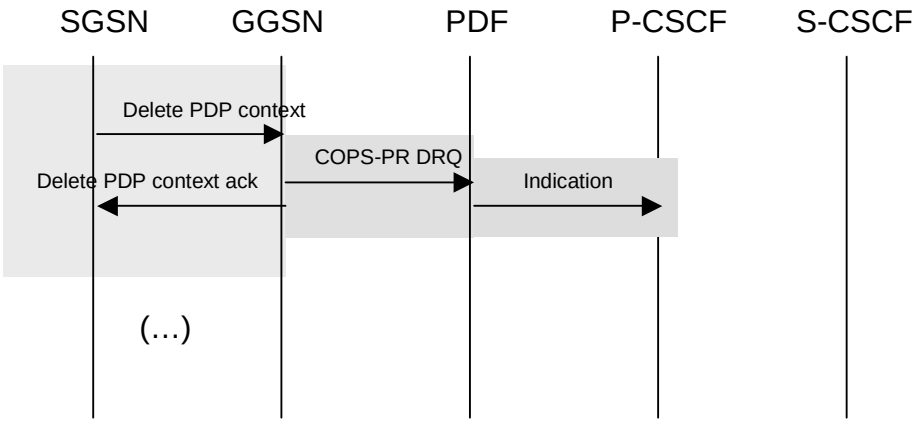


Figure 19: Example of information flow for indication of PDP context release towards IMS

The PDF is informed about the deletion of the network resources previously authorized.

This is done via the Go interface with the COPS-PR DRQ message.

The PDF may revoke the authorization and may send an indication to the P-CSCF.

9 Function Requirements

This section identifies the requirements for support of the architecture:

General Requirements

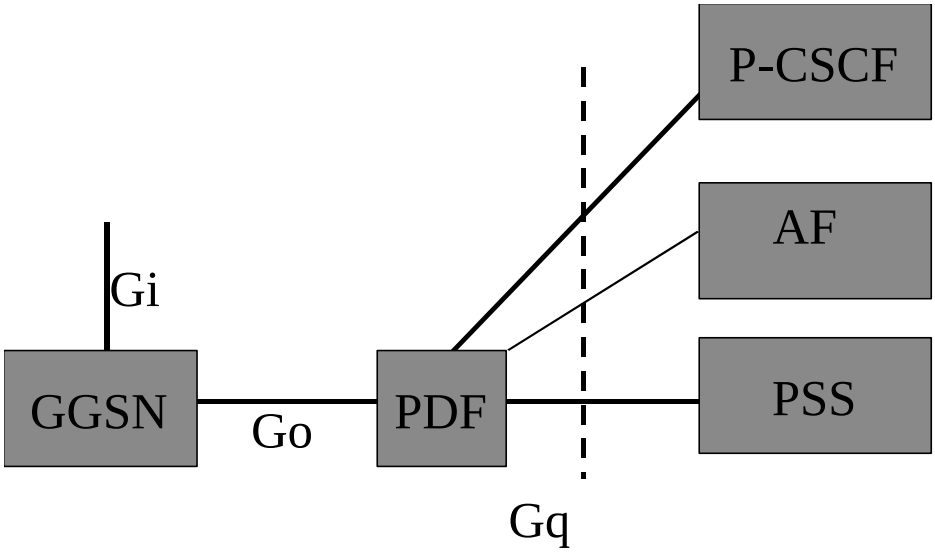
1. Regardless of how the architecture evolves, the release 5 solution with a Go interface between the PDF/P-CSCF and GGSN must be retained for backwards compatibility. Development of the Go protocol is out of scope of this TR.

2. The Gq protocol should be service agnostic.

Service Requirements

FFS

10 Example of rel6 policy control usage with a PSS application



An RTSP session to the PSS server constitutes the signalling, with a separate bearer set up for the media stream(s) which may utilise RTP/RTCP but which may be some other protocol, dependent on the source and the media type.

When the UE makes a session request in the PS domain (i.e. a PDP context request) the GGSN requests authorisation from the PDF via the Go interface, using the authorisation token that the UE included in the PDP context request.

The PDF informs the GGSN of the agreed session parameters and the GGSN will allow, decline or negotiate down the request after cross checking this with the parameters requested by the UE.

The scenario described here for PSS services would require the PSS server to support the Gq interface, and the UE to support passing the authorisation token, which are mechanisms not supported in the existing PSS application. The impact on the existing PSS services as defined in TS 26.233 and compatibility between old and new equipment should be studied. Specifically some issues listed are as follows:

- The impacts on PSS services, which are created (including support for 3GPP users) to access streaming services including services outside of the operators domain (currently available in the Internet today). These do not work with this mechanism unless additional changes are made towards PSS-PDF role.

Application of policies beyond an operator domain is subject to roaming agreements. If we use the PDF for PSS, a PSS server outside of the operator's domain, requires either access to the PDF of the operator's domain, or access to an AF in that domain. Hence user experience in the roaming scenario can vary if proper roaming agreements and SLAs are not in place.

- It is necessary to avoid widely different policies within different operators, as this will likely cause service disruption towards user experience due to frequent changes in the service-QoS mapping table in the UE when roaming.

- Applying policy requires an added authorization mechanism (compared to when always allowing any PSS, where this authorization mechanism does not happen).

-SDP usage for a streaming service may not be available to the PSS server, in such cases new mechanism will be needed to provide the information to PSS and then to PDF.

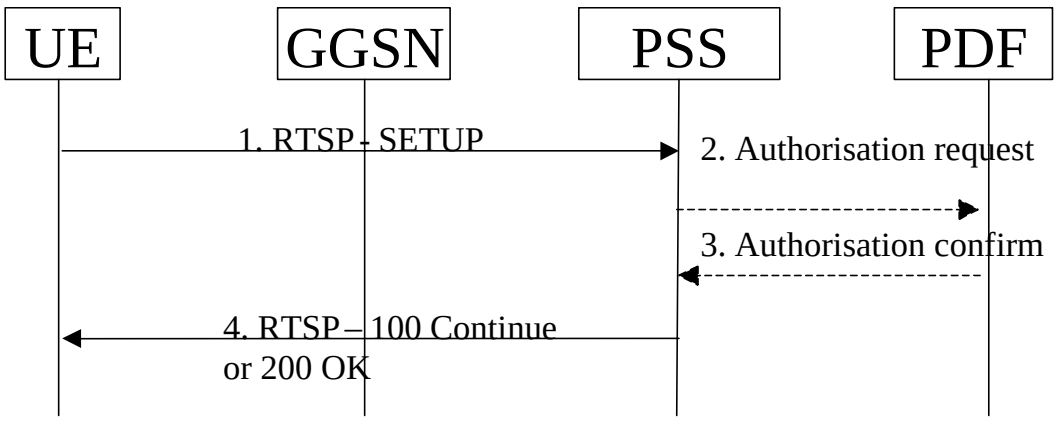
The flows for PSS system are shown below. The flows assume that GGSN, PSS & PDF are all aware of each other's existence and within an operator's domain. The session release flows shown below show a UE initiated session release.

It should also be noted that the PSS server in the current PSS service scenarios does not initiate session release towards the terminals, sessions are either abruptly terminated or terminated via redirection towards a message service.

For radio loss, the GGSN can report the change in the network conditions, via the procedure described in 23.917 8.6 Indication of network resources events

10.1 Per User Authorisation

When the UE makes the first RTSP request to the PSS server, the PSS server knows which PDF to contact and obtains the media authorisation token from the PDF. This is then passed to the UE in a header in the RTSP response message.



Per User Authorisation

1) The PSS server receives SETUP request from the terminal.

2) Prior to the SETUP request from the client, the server has already interacted with the client (DESCRIBE, ANNOUNCE etc.) where in based on client service request, the server has identified media types, bearer

resources like bandwidth, IP address, port numbers to be used, etc. needed for the session. The PSS server contacts the PDF in order to obtain a PDF generated token. The session requirements that were communicated to the client in an SDP format are also passed by the PSS server to the PDF The PDF to be used needs to be known by the PSS server.

3) The PDF passes the authorisation token to the PSS server in the authorisation confirm.

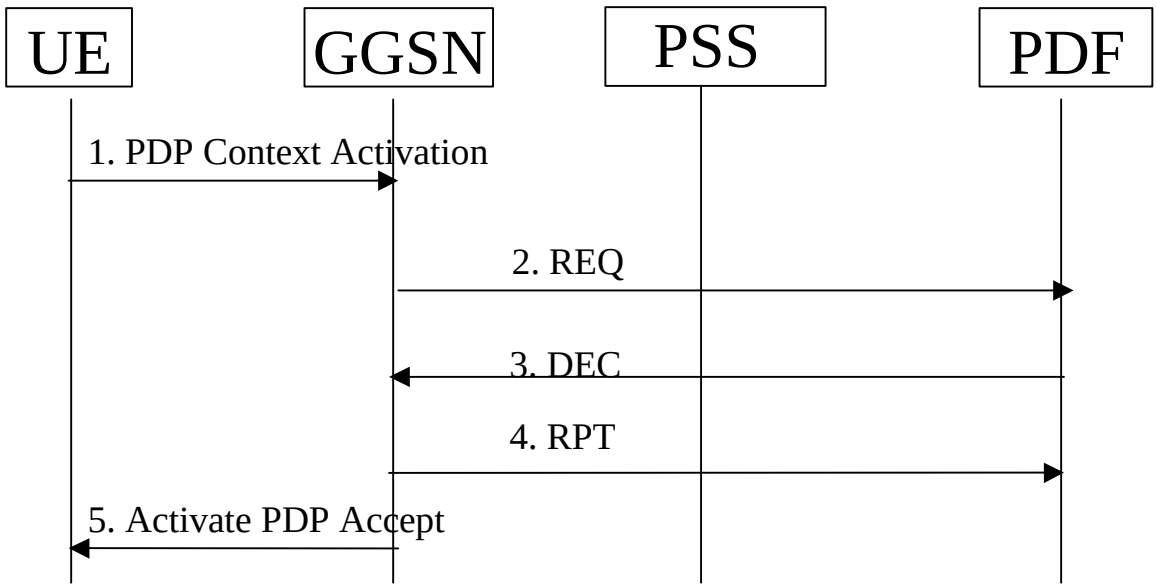
4) The PSS server includes the media authorisation token within a message body attached to the response message sent back to the UE.

10.2 Resource reservation

The GGSN, when receiving a request for a PDP context activation will, via the Go interface, request authorisation from the PDF. The authorisation token is used as the mechanism to enable the GGSN to contact the PDF that generated it.

The signalling flow is shown below. In this scenario the PSS server has not required further interaction from the PDF at resource reservation.

Note that the SGSN is involved in the PDP Context signalling but is not shown in the diagram for simplicity.



PSS Resource Reservation

1) GGSN receives the Secondary PDP Context Activate request. It should be noted that more than one Secondary PDP Context may be requested dependent on the media streams that are part of the service.

2) GGSN requests the PDF to authorise the resources. The Media authorisation token received in the PDP context activation is used to identify the session and end point for the COPS request.

3) PDF authorises the resources. It is FFS whether it is at this stage that the PDF sends COPS DEC message(s) to the GGSN to open the 'gates' e.g., enable the use of the authorised QoS resources, or whether this is done later at resources commit.

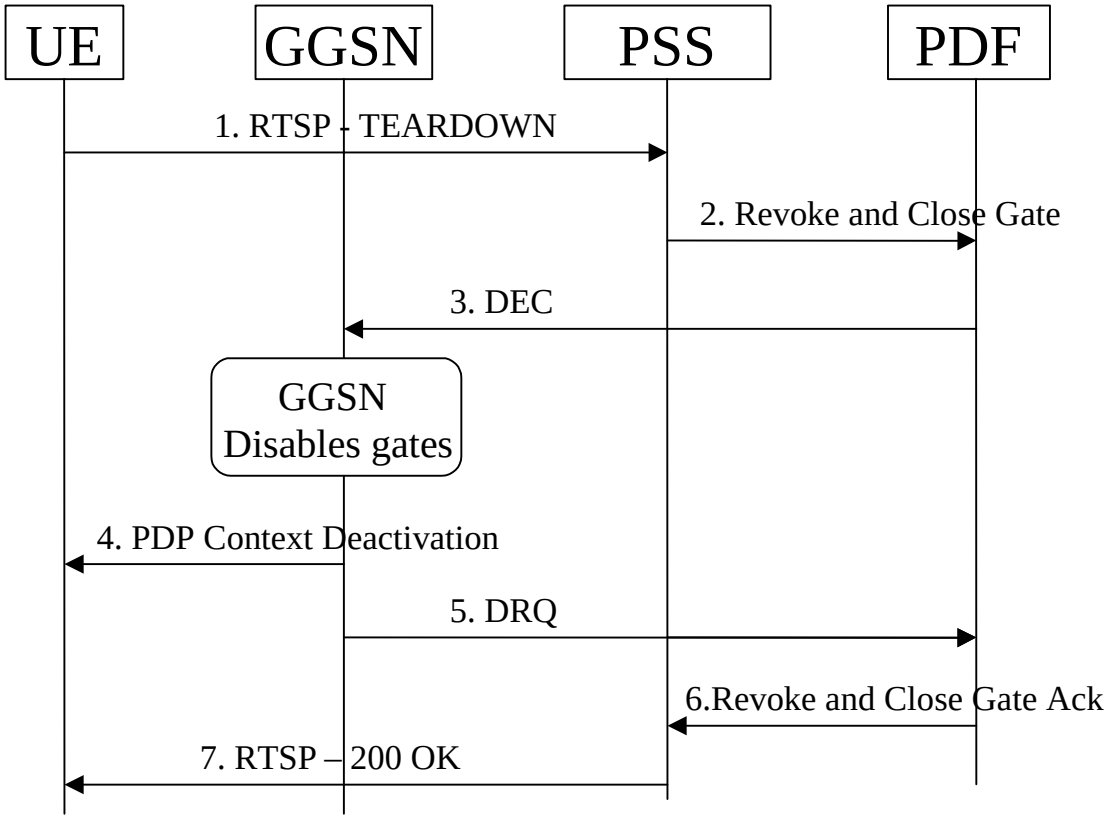
Note: The Go protocol (and thus presumably also the Gq protocol) permits the commit authorisation to be included with the authorisation decision. Since the traffic flow itself is controlled from a trusted network server rather than an untrusted end user, it is unclear under what circumstances the AF would not authorise the commit in conjunction with the initial authorisation data. How does the PSS server know that it must interact further with the PDF to commit the resources needs to be addressed.

4) GGSN sends COPS RPT message(s) back to the PDF.

5) GGSN confirms the PDP context is accepted.

10.3 Session Release

The terminal may request that the session is terminated. This is illustrated below.



PSS Revoke and Remove Resources

1) The terminal requests the termination of the session with the TEARDOWN message.

2) PSS server requests the PDF to release the resources and terminate authorisation. The PDF removes the authorisation for the media component(s) of this session.

3) PDF sends COPS DEC message(s) to the GGSN which identifies the PDP context(s) to be deactivated.

4) GGSN initiates deactivation of the PDP context(s) used for the PSS session, in case the UE has not already done so.

5) GGSN sends COPS DRQ message back to the PDF.

6) The PDF confirms the release of the resources to the PSS server.

7) The PSS server confirms completion of the Teardown procedure to the terminal.

Annex

Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
06/08/02				0.0.0	Updated proposal to SA2 reflector		
14/08/02				0.0.1	Skeleton TR input to SA2#26		
24/09/02				0.1.0	Output version from TSG SA2#26 taking into account S2-022160, S2-022573rev1, S2-022574		
24/09/02				0.2.0	Proposal to SA2 reflector to include S2-022573rev3 sent during e-mail approval.		
02/11/02				0.3.0	Output version from TSG SA2#27, taking into account S2-023094rev5, S2-023105rev2, S2-023106rev1		
02/11/02				0.3.1	Changed PCF to PDF following decision at SA2#27		
03/12/02				0.4.0	Output version from TSG SA2#28, taking into account S2-023603rev1, S2-023604rev4, S2-023606rev2, S2-023608, S2-023617, S2-023665rev1, S2-023666, S2-023667		
04/12/02				0.4.1	Changed IMS example flows to show the boxes in the same order as other figures i.e. “UE SGSN GGSN PDF P-CSCF S-CSCF”		
11/02/03				0.5.0	Output version from TSG SA2#29, taking into account S2-030338, S2-030339, S2-030340rev2, S2-030341		
11/02/03				0.5.1	Editorial modifications		
17/03/03				0.6.0	Output version from TSG SA2#30, taking into account S2-030869, S2-030927, S2-030928, S2-030938rev3		
18/04/03				0.7.0.	Output version from TSG SA2#31, taking into account S2-031354, S2-031534, S2-031598		
26/05/03				0.8.0	Output version from TSG SA2#32, taking into account S2-032017 and S2-032059		