ETSI ES 282 003 V1.1.1 (2006-06)

ETSI Standard

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture

Reference

DES/TISPAN-02020-NGN-R1

Keywords

access, control

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Standard (ES) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

The present document describes the architecture of the Resource and Admission Control Subsystem (RACS) identified in the overall TISPAN NGN architecture.

1 Scope

The present document describes the functional architecture for the Resource and Admission Control Sub-System (RACS), in TISPAN NGN Release 1, in line with the service requirements described in TS 181 005 [1]. RACS is the TISPAN NGN subsystem, responsible for elements of policing control including resource reservation and admission control in the access and aggregation networks. The RACS also includes support for a Network Address Translator (NAT) at any place or set of places in the access, aggregation and core networks.

The functional architecture and system description developed in the present document is in line with the Release 1 requirements for RACS developed in ES 282 001 [2].

The present document defines RACS for fixed access networks.

NOTE: The present document uses the term "NGN" only in the context of TISPAN.

2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI TS 181 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services and Capabilities Requirements".

[2] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".

[3] IETF RFC 3312: "Integration of Resource Management and Session Initiation Protocol (SIP)".

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

[5] ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub system (NASS)".

[6] ETSI TR 180 000: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology".

[7] ETSI TS 123 107: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Quality of Service (QoS) concept and architecture (3GPP TS 23.107)".

[8] ITU-T Recommendation Y.1541: "Network performance objectives for IP-based services".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 180 000 [6] and the following apply:

Aggregation Network Segment: comprises the functional elements that enable communication between an Access Node and the core network

Application Function: Application Function (AF) is an element offering applications the control of IP bearer resources when required

NOTE: The AF is capable of communicating with the RACS to transfer dynamic QoS-related service information.

Application Session: end-to-end user session, which is setup by an AF (using SIP or another protocol), and requires one or more resource reservations to take place

NOTE: An application session may involve one, two or more end users.

BGF Service: traffic flow function performed by the BGF on media flows and/or the allocation of BGF resources

DiffServ: DiffServ networks classify packets into one of a small number of aggregated flows or "classes", based on the DiffServ code point (DSCP) in the packet's IP header

Gate: A gate operates on a unidirectional flow of packets, i.e., in either the upstream or downstream direction

NOTE: A gate consists of a packet classifier, and a gate status (open/closed). When a gate is open, the packets in the flow are accepted. When a gate is closed, all of the packets in the flow are dropped.

"Last mile" Access Network Segment: comprises the functional elements that enable communication between a CPE and an Access Node

Media Flow: uni-directional media stream of a particular type, which is specified by two endpoint identifiers, bandwidth and class of service

NAT: generic term for Network Address Translation that includes NAT-PT and NA(P)T

QoS Classes: as defined in ITU-T Recommendation Y.1541 [8] and TS 123 107 [7]

QoS Push Model: model where the Application Function requests to the RACS QoS authorization (policy control) and resource reservation

NOTE: In this model, the CPE does not itself support native application independent QoS procedures.

Resource Reservation session: set of one or more media flows, which are reserved for a period of time in order to execute an application session

NOTE: A resource reservation session may be uni-directional or bi-directional.

xDSL: type of access, i.e. a set of access network accesses supported by the NGN, based on the different flavors of the xDSL technology, that have their resources controlled by RACS

TISPAN access networks: set of access networks supported by the NGN

3.2 Abbreviations

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

AF	Application Function
A-RACF	Access-Resource and Admission Control Function
ASP	Application Service Provider
BGF	Border Gateway Function

BGS	Border Gateway Services
C-BGF	Core Border Gateway Function
CCI	Charging Correlation Information
CLF	Connectivity session Location and repository Function
CPE	Customer Premises Equipment (i.e. (routed) modem, residential gateway, integrated access device)
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Service Code Point
FQDN	Fully Qualified Domain Name
Ia	Interface Ia
I-BCF	Interconnection Border Control Function
I-BGF	Interconnection Board Gateway Function
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
L2TF	Layer 2 Termination Function
NA(P)T	Network Address and optional Port Translation
NASS	Network Attachment Sub-system
NAT	Network Address Translation
NAT-PT	NAT Address Translation and Protocol Translation
NGN	Next Generation Network
P-CSCF	Proxy-CSCF
PDF	Policy Decision Function
PPP	Point to Point Protocol
QoS	Quality of Service
Ra	Reference point a
RACS	Resource and Admission Control Subsystem
RCEF	Resource Control Enforcement Function
Re	Reference point e
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
Rq	Reference point q
SBP	Service Based Policy control
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SPDF	Service-based Policy Decision Function
TCP	Transmission Control Protocol
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
UDP	User Datagram Protocol
UE	User Equipment
UNI	User-to-Network Interface
VoIP	Voice over IP
VPN	Virtual Private Network

4 General description of RACS

4.1 High Level functional overview

RACS is the NGN subsystem responsible for elements of policy control, resource reservation and admission control. RACS also includes support for Border Gateway Services (BGS) including Network Address Translator (NAT).

RACS essentially provides policy based transport control services to applications. This enables applications to request and reserve transport resources from the transport networks within the scope of RACS.

In NGN Release 1, RACS scope extends to the access network and to points of interconnection between core networks.

By offering a set of generic policy based transport control services to applications, RACS ensures that any existing or future application shall be able to request transport resources appropriate to that service as long as the application supports the interface to RACS defined in this architecture specification. By offering a level of hidden interaction between applications and the transport resources themselves, RACS also ensures that applications do not need to be aware of the underlying transport networks. As an example, RACS allows for real-time multi-media services (VoIP, Videoconferencing, Video on Demand, on-line gaming) to request some particular bandwidth and/or address mediation capabilities for the service from the network. RACS, as the network element responsible for policy based transport control evaluates these requests in the context of the predefined policy rules which the network operator has provisioned. The RACS reserves the appropriate resources and admits the request provided the request passes the policy tests and the appropriate resources are available in the transport network. Therefore, RACS offers the means for an operator to enforce admission control and set the respective bearer service policies. It provides the means for value-added services to obtain network resources that are necessary to offer services to the end-user.

RACS is resource-reservation session aware but application session agnostic (i.e. it can support transport resource reservations for both session based and non-session based applications).

RACS also provides access to services provided by the Border Gateway Function. Examples of those services are gate control, NAT and hosted NAT transversal.

Basically, RACS offers to Applications Functions (AF) the following functionality on a one per RACS resource reservation session request basis:

- Admission Control: RACS implements Admission Control to the access and aggregation segment of the network. One can imagine various types of admission control going from a strict admission control where any overbooking is to be prevented, to admission control that allows for a certain degree of over subscription or even a trivial admission control (where the authorization step is considered sufficient to grant access to the service).

- Resource reservation: RACS implements a resource reservation mechanism that permits applications to request bearer resources in the access and aggregation networks.

- Policy Control: RACS uses service based local policies to determine how to support requests from Applications for transport resources. Based on available information about resource availability and on other policy rules (e.g. priority of the application) RACS determines if a request can be supported and (if successful) RACS authorizes appropriate transport resources and defines L2/L3 traffic polices that are enforced by the bearer service network elements.

- NAT transversal: RACS controls the transversal of far end (remote) NAT.

- NAT/Gate control: RACS controls near-end NAT at the borders of the NGN core network and at the border between a core network and an access network.

RACS offers services to Application Functions (AF) that may reside in different administrative domains.

4.2 Functional requirements

The functional requirements of the RACS, for NGN Release 1, are developed in the present document in line with TS 181 005 [1].

The RACS is the NGN component that shall provide the following functions:

1) The RACS shall provide policy based transport control services (e.g. policy control, resource reservation, policing, gate control and IP address mediation) to Application Functions (AFs).

2) The RACS services shall not be specific to any Application Function (AF) or service subsystem.

3) The RACS services shall be made available to all service control subsystems as well as to the Applications domain.

4) The RACS services are chosen by an Application Function(AF) at a given time for use in the context of the application service provided by the application.

5) For Release 1, RACS shall only provide policy based transport control services within the access networks and at points of interconnection between core networks. There is no requirement for RACS to provide service coverage for core networks themselves or to customer networks.

6) The RACS shall hold a logical view of the different transport segments within its control. As one example, for xDSL access, this must include at least the last-mile and the aggregation network. RACS sets the bearer/transport function with network-level attributes that match to the service (Bandwidth, QoS, etc). RACS shall be capable of supporting the NGN access types and should support all the following scenarios:

   - a resource reservation where admission control is only required for the "last-mile" access network segment (but is not required for the aggregation network segment);

   - a resource reservation where admission control is only required for the aggregation network segment (but is not required for the "last mile" access network segment);

   - a resource reservation where admission control is required for both "last mile" access network and aggregation network segments.

7) The RACS shall provide a mechanism to the Application Function (AF) entity through which it can reserve resources in the access network, i.e. RACS reserves resources on behalf of AFs.

8) The RACS shall offer services to Application Functions (AFs) that may reside in different administrative domains.

9) The RACS shall be able to authenticate and authorize the Application Function (AF).

10) The RACS shall support transport control service requests from Application Functions (AF) for uni- and bi-directional, symmetric and asymmetric, unicast and multicast, up- and downstream traffic. However, multicast is not further developed in RACS Release 1.

11) The RACS shall notify the Application Function (AF) in the case that a previously allocated resource must be relinquished. This may be triggered by an administrative decision or a faulty condition.

12) The RACS shall support requests from Application Functions (AFs) to modify the parameters of their existing transport resource reservations. Requests of this type may result in a new admission control step and/or installing of new L2/L3 traffic policies.

13) The RACS shall provide feedback messages to the Application Function (AF) either approving or rejecting the transport control service reservation, commit or modify requests.

14) The RACS shall be able to export charging information and resource reservation session metrics. For Release 1 charging should be limited to off-line charging.

15) The RACS shall support a "Push" model for initiating policy based transport control service requests. In this model service requests are "pushed" to RACS from the Application Function (AF). RACS services these requests, and if the service requests from the AFs are in line with policies established by the operators and stored in the subsystem, and if appropriate transport resources are available, then RACS "pushes" requests down to the transport layer to obtain the appropriate transport resources.

16) The RACS is not aware of application session, it shall be aware of a set the media flows in a resource reservation request, which may in turn belong to one or multiple application sessions.

17) The RACS shall be able to react on prioritization request signalled by an Application Function (AF) for transport control by modifying allocated resources.

18) The RACS shall be capable of supporting multiple Application Functions (AFs).

19) The RACS shall support a versatile set of resource management schemes, suitable for coping with all target deployment architectures.

    - a Single-stage resource management model, providing resource management services in a mode where reserved resources are immediately available upon successful reservation;
    - a Two-stage reserve-commit resource management model, that can be leveraged in support of services that aim to support charging per service-invocation, and require as such service-theft-prevention solutions;
    - An Authorize-reserve-commit resource management model, supporting service-based local policy control under coordination of a network-hosted application function.

20) The RACS shall support appropriate overload control mechanisms in order to prevent overload within the RACS itself and also within the requesting AFs. This applies to all RACS to AF interfaces. However, the overload control mechanism is not further developed in this architecture document.

21) The RACS shall be prepared to support at least eight different priority types defined in such a way that any number of them may be simultaneously active. This number of priorities is envisaged to support different priorities for national usage (e.g. emergency service).

22) The RACS shall support allocation of resources in the transport network that have different traffic characteristics, for example packet loss.

23) The RACS shall support both soft-state and hard-state resource management approaches. Soft-state operation will assure robustness of resource management services in an environment with multiple applications. In both cases:

    - granularity of resource reservation, removal and modification facilities shall be at the level of individual service flows;
    - the RACS shall support facilities for the explicit removal of previously established resource reservations;
    - the RACS shall support facilities for the explicit modification of previously established resource reservations.

24) The RACS shall provide the necessary functions to support subsystems in the Service Layer that implement a segmented resource management model [3]. An example of such a subsystem is the IMS, where resource reservation for each participating party in an application session (e.g. multi-party conversational SIP-based sessions) is needed.

5 RACS Architecture

5.1 QoS Management Functions in Fixed Access Networks

In order to define the RACS architecture it is necessary to identify the possible QoS management functions in fixed access networks. Those functions can be categorized according to their QoS control capabilities and business models. An abstraction is made here of the possible business models in the fixed environment.

To ensure QoS aware NGN service delivery, the following two architectures for dynamic QoS control are considered for RACS:

- Guaranteed QoS - service delivery with absolute bounds on some or all of the QoS parameters, such as throughput, latency, jitter and loss. This is achieved by performing admission control and enforcement of admission control decisions in the access network, via throughput control and traffic policing.
- Relative QoS - the relative QoS model implies traffic class differentiation by applying appropriate QoS mechanisms. The IP QoS profile defining the QoS parameters is dynamically updated in the IP edge.

Support of QoS unaware ("Best Effort") networks as well as support of networks that have statically provisioned QoS differentiation does not require any RACS functionality.

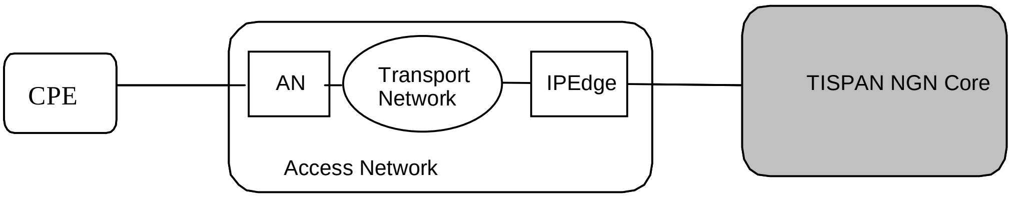


Figure 1: Access Network Model

The architecture supports both QoS control architecture models - guaranteed and relative - allowing the access provider to select the most suitable QoS architecture for their needs.

When relative QoS is used, the QoS differentiation shall be performed at the IP edge, e.g. compliant with the DiffServ Edge functionality defined in IETF specifications for Differentiated Services [4]. Moreover, RACS should take into account the ability of some CPE to provide QoS differentiation, e.g. by applying DiffServ marking, and take steps to allow this to have effect only where it is required by operator defined RACS local policies.

For guaranteed QoS control, enforcement of QoS admission control decisions (throughput control and traffic policing) shall be performed in the IP edge and may also be performed in the CPE and/or Access Node.

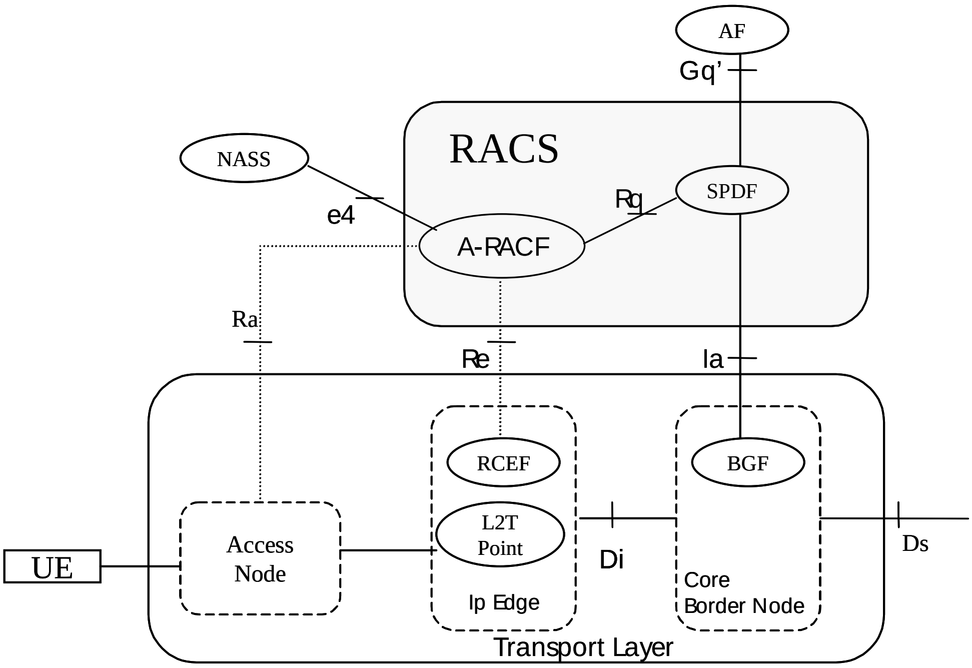
The RACS supports the "proxied QoS reservation request with policy-push" as a QoS resource reservation mechanism. In this case, the CPE does not itself support native application independent QoS signalling procedures. When a CPE invokes a specific service of an AF using the NGN signalling (e.g. SIP), the AF will issue a request to the RACS for QoS authorization (policy control) and resource reservation.

RACS policy decisions are pushed to the policy enforcement function (IP edge) in the NGN access (e.g. xDSL).

5.2 RACS functional architecture

5.2.1 General

The overall functional architecture of the RACS is shown in figure 2.



NOTE: Besides the A-RACF and SPDF this specification addresses the aspects of the RCEF, BGF and AF that are associated to RACS. The overall functionality related to AF, RCEF and BGF is defined in [2].

Figure 2: RACS Functional Architecture

The NGN Service Layer encompasses an Application Function (AF), which offers services that require control of IP bearer resources. Examples of an AF are the P-CSCF and I-BCF in the case of IMS. The AF maps the application layer QoS information, e.g. the P-CSCF maps parameters defined in SDP, into QoS request information to be sent via the Gq' interface to the SPDF.

The SPDF provides the AF with a single point of contact. The A-RACF is always in the access network and supports the resource reservation method as defined in clause 5.1. The A-RACF receives requests from the SPDF. Based on these requests and policy information stored in the A-RACF, the A-RACF may accept or reject these requests for the transport resources within its control.

For resource and admission control the architecture provides a clear separation between layers that allows an application service to run over different access networks without impacting the application capabilities as long as the resources are available. Although A-RACF can be seen as a generic function, it may maintain different instances of resource models, depending on the different types of access.

The RACS (A-RACF) interacts with the Network Attachment SubSystem (NASS) via the e4 reference point.

The Ra reference point represents different methods by means of which A-RACF interacts with the access and aggregation networks. The Ra reference point will not be standardized in Release 1.

The RCEF and the L2TF are two different Functional Entities that are usually grouped into a physical entity called IP Edge Node. They are accessed via the Re interface which will not be standardized in Release 1.

The Layer 2 Termination Function (L2TF) is the point where the L2 communication with the CPE is terminated.

The Resource Control Enforcement Function (RCEF) is a logical element in the transport layer that enforces the traffic policies by means of which RACS can assure the use of the resources.

The BGF is located anywhere in the transport network. It may be found between an Access Network and a Core Network (C-BGF) or between two Core Networks (I-BGF). The explicit identification of these two instances of the BGF is intended to ensure clarity in the scenario descriptions.

Table 1 summarizes the services performed in the RCEF, C-BGF and I-BGF, under the control of the RACS.

Table 1: Functionality of RCEF, C-BGF and I-BGF

RCEF	C-BGF	I-BGF
Open/close gates	Open/close gates	Open/close gates
Packet marking	Packet marking	Packet marking
	Resource allocation (per flow)	Resource allocation (per flow)
	NAT	NAT
	Hosted NAT traversal	
Policing of down/uplink traffic	Policing of down/uplink traffic	Policing of down/uplink traffic
	Usage metering	Usage metering

Different BGF instances may implement different subsets of the services identified in table 1, based on the operator's policy.

Unless where stated explicitly, the remaining text of the present document refers to the term BGF for both C-BGF and I-BGF, regardless of its location in the network.

5.2.2 Charging

The RACS requirements for charging are restricted in Release 1 to providing support for offline charging by the RACS functions that can be located in different administrative domains: the SPDF, A-RACF and AF.

The RACS functional entities, SPDF and A-RACF shall be capable of providing the following information for charging purposes:

- Charging Correlation Information (CCI).
- Requestor Info.
- Subscriber Info.

- Service Priority.
- Media Description.
- Commit ID.
- Time Stamp.
- Reason.

The means to transfer this information is not standardized in the present document.

A Charging Correlation Information (CCI) is a globally unique identifier that may be generated by the SPDF if it was not provided by the AF. This identifier may also be forwarded to the A-RACF.

The Subscriber Info represents the Subscriber-Id and the Globally Unique IP Address present in the request.

The Reason shall represent conditions such as successful, unsuccessful and abnormal conditions. The charging capabilities in RACS does not impose any further requirements in the charging requirements for Release 1.

5.2.3 Functional elements

5.2.3.1 SPDF

5.2.3.1.1 SPDF main functions

The Service Policy Decision Function (SPDF) is a logical policy decision element for Service-Based Policy control (SBP).

The SPDF makes policy decisions using policy rules defined by the network operator. Based on the outcome, resources requests may be sent to an A-RACF and/or BGF. Finally the decision is communicated back to the requesting AF.

The SPDF chooses the local policy to be applied to a request from an AF based on the combined meaning of the Requestor Name, Service Class, Service Priority, Reservation Class, or any other combination of those information elements. The SPDF maps the local policy into the parameters to be sent to the A-RACF and/or BGF.

The SPDF hides the underlying network topology from applications. This allows the SPDF to offer a common view to the AF (e.g. P-CSCF) regardless of the underlying network topology and particular access technology in use.

The SPDF performs the following functions:

- Checks if the request information received from the AF is consistent with the policy rules defined in the SPDF.
- Authorizes the requested resources for the AF session. The SPDF shall use the request information received from the AF to calculate the proper authorization (i.e. authorization of certain media components).
- Determines the location of the BGF and/or A-RACF in accordance with the transport capabilities required.
- Request resources of the A-RACF.
- Request one or more services from the BGF (listed in table 1).
- Hides the details of the RACS from the AF.
- Hides the details of the transport layer from the AF.
- Performs resource mediation by mapping requests from an AFs towards an appropriate A-RACF and/or BGF.

5.2.3.1.2 Reference points

The reference point between the AF and SPDF is Gq'. The Gq' enables the NGN Subsystems to interact with the Resource and Admission Control Subsystem (RACS) for authorization, resource reservation and Border Gateway Services (BGS).

The reference point between the SPDF and the A-RACF is Rq. The SPDF interacts with the A-RACF to ask for an admission control decision for the QoS resources required for the AF session via the Rq reference point. The authorization decision provided by the SPDF to the AF is dependent on the admission control decision taken by the A-RACF.

The reference point between the SPDF and the BGF is Ia. The SPDF interacts with the BGF to ask services as listed in table 1. This reference point is used for communication between the SPDF and C-BGF and between the SPDF and I-BGF.

The SPDF shall be able to establish relationships with multiple A-RACFs. These A-RACFs can be all in the same or in different access networks. The SPDF shall have the ability to identify the correct A-RACF when a request is received from the AF.

The Gq' reference point allows that the AF and the SPDF are in different administrative domains. The Rq reference point also allows that the SPDF and the A-RACF are in different administrative domains.

5.2.3.1.3 User profile

The SPDF does not require access to user profile information.

5.2.3.1.4 Priority

The AF can indicate a service priority level to the SPDF. In accordance, the SPDF has the ability to define a service priority level for the resource reservation request sent to the A-RACF. As an example, in the case of an emergency session, the AF may indicate to the SPDF that the resource is required for a AF priority session and, as a result, the SPDF indicates to the A-RACF a service priority for the requested resource.

5.2.3.1.5 Service request

Requests from the AF to the RAC Subsystem (RACS) over the Gq' reference point include information on the service required from RACS, an unique identifier for the requesting application, an unique identifier for the resource reservation session and an indication of the requested priority amongst others (see clause 5.3.4.3 for a complete list of information elements). It shall be possible for the AF to request a different RACS service for each of the flows belonging to a single resource reservation session request.

The key information elements used by an AF to specify the service requested from RACS are the Requestor Name and the Service Class (see definitions in clause 5.3.4.3), however, other parameters such as bandwidth provide additional information about the service requested.

Service information is of local significance to the operators controlling the service and transfer layers respectively, and the definition of the actual values used is outside the scope of standardization.

By combining all the information received from the AF via Gq' with local operator policies, the SPDF can derive the following information:

- whether service is to be requested from the BGF, A-RACF, both or neither of them;
- transfer layer resources that shall be used for a particular resource reservation that may include transport network partition, interconnection type (where signalling-only interconnection types may not require the insertion of an I-BGF in the media path), and interconnect resources to be used (choosing the right I-BGF in the transport domain);
- traffic characteristics to be requested for individual media flows, including QoS parameters, which may be used by the SPDF to in turn request the appropriate filters or packet marking policies to be applied in the BGF and/or to describe to the A-RACF the resource being requested.

5.2.3.1.6 Coordination function

The SPDF maps requests received from an AF into a request sent to an A-RACF and/or to a BGF.

The SPDF performs the coordination function for messages exchanged between an AF, BGF and/or A-RACF.

A bundle identification, hereafter referred as Resource Bundle-Id information, may be received in a reply granting resources from the A-RACF. The SPDF shall be able to associate this Resource Bundle-Id to the resources reservation session during the existence of this resource reservation session. The association is maintained as long as the Bundle Id is received in each relevant message, Reception of a different Bundle Id would lead to a new association, and the absence of a Bundle Id would lead the removal of that association..

In case failure conditions are effecting the A-RACF and/or the BGF, the SPDF is capable of performing the necessary coordination for release of the impacted resources (e.g. an event reporting failure in the BGF is reported to the AF and any outstanding A-RACF resources shall also be released). The reference points between the A-RACF, BGF and SPDF shall be able to transport information indicating partial or complete failure of a BGF or an A-RACF.

The SPDF shall be able to handle reports of abnormal condition from the A-RACF specifying either an individual resource reservation session or a Resource Bundle-Id. In the latter case, all current resource reservation sessions associated to this bundle shall hence be released.

In addition, the SPDF can autonomously initiate a partial or total release of resources (e.g. administrative action in the SPDF).

The sequence used by SPDF to access the A-RACF and BGF is a local decision in the SPDF, e.g. the SPDF is able to decide whether to access the A-RACF and then the BGF, or vice versa, or both in parallel. This is valid for request, modification and release. The implementation of this decision is out of the scope of the present document.

5.2.3.1.7 Charging

The SPDF shall be able to provide charging information for the Request/Modify/Release/Abort commands when necessary.

5.2.3.1.8 Deployment considerations

Due to the possible business roles in an access environment, the SPDF may be either in the same administrative domain or in a different administrative domain as the A-RACF.

The SPDF permits other instances besides IMS to request and control resources.

NOTE: As for any other functional entity, implementors may choose to combine the SPDF with the AF where this makes sense in the context of the business models, services and capabilities being supported (e.g. in the case of implementations supporting IMS services only). However, if this deployment option is adopted, there are some implications that should be taken into account:

- the service control/application subsystem that hosts the AF and the SPDF in the RACS subsystem can no longer belong to two different administrative domains;
- a SPDF (and associated transport network resources) can only serve the service control/application subsystem that hosts the Application Function (AF) (e.g. an IMS-only NGN network).

5.2.3.1.9 Overload control

The SPDF provides bi-directional overload control mechanisms, which helps to limit the load on the A-RACF, SPDF, BGF or AF should any of these components experience overload. A full specification of this capability is left as an outstanding issue.

5.2.3.1.10 Discovery mechanism

The AF can obtain the RACS contact point from the NASS as a FQDN or IP address of the SPDF. Alternatively, in the absence of such a possibility, the AF may have other mechanisms, local configuration may be used.

The SPDF relies on local configuration to discover the contact points for the A-RACFs and the BGFs.

5.2.3.2 A-RACF

5.2.3.2.1 A-RACF main functions

The main functions of A-RACF are:

Admission Control (AC): The A-RACF receives requests for QoS resources from the SPDF via the Rq reference point, indicating the desired QoS characteristics (e.g. bandwidth). The A-RACF shall use the QoS information received from the SPDF to perform admission control, i.e. the A-RACF checks whether the requested QoS resources can be made available for the involved access. The A-RACF shall indicate to the SPDF whether a request for resources is granted or not via the Rq reference point.

Network Policy Assembly (NPA): Access Network Policies are a set of rules that specify what network policies should be applied to a particular access line. The A-RACF ensures that a request from the SPDF (of a particular network service provider) matches the access policies, as multiple SPDF can request resources from the A-RACF. As the Rq reference point may be an inter-domain reference point, the A-RACF shall authenticate the SPDF requesting resources via Rq. The A-RACF checks if the request matches the requestor's (operator SPDF) profile. Only validated requests for authenticated requesters shall be retained as input. The A-RACF combines the requests from the SPDFs that have requested resources and ensures that the total of the requests match the capabilities of the particular access line.

5.2.3.2.2 Reference points

The A-RACF interfaces with the NASS via e4 reference point.

The e4 reference point is used for the Customer Location Function (CLF) in the Network Attachment Subsystem (NASS) to send network attachment information and the subscriber access profile information to the A-RACF.

The A-RACF also interfaces with the SPDF via the above mentioned Rq reference point, and with the RCEF via the also above mentioned Re reference point. The Re reference point will not be standardized in Release 1.

5.2.3.2.3 Admission control process

The NASS informs the A-RACF when a subscriber attaches to the network. The subscriber access profile received from the NASS [5] consist of:

- Subscriber attachment info: Subscriber ID, Physical Access ID, Logical Access ID, Access Network Type and Globally Unique IP Address;
- QoS Profile Information (optional): Transport Service Class, UL Subscribed Bandwidth, DL Subscribed Bandwidth, Maximum Priority, Media Type and Requestor Name. The QoS Profile may contain one or more sets of information elements;
- Initial Gate Setting (optional): List of Allowed Destinations, UL Default Bandwidth, DL Default Bandwidth.

On the other hand, the SPDF provides the following information that is relevant to A-RACF procedures when it receives a request:

- Subscriber Id or IP address;
- Requestor Name/Service Class;
- Media Description;
- Service Priority.

The Physical Access ID, Logical Access ID and Access Network Type allows A-RACF to bind the Subscriber Id and/or its IP address to the topology information of the access and aggregation networks hosted in A-RACF.

The A-RACF uses the Initial Gate Setting, the capabilities of the elements in the data plane as well as access network policies, defined by the operator, to derive the initial traffic policies that must be installed in the RCEF.

When a resource request is received from the SPDF, based on the Subscriber Id and/or the IP address, the A-RACF identifies the subscriber access profile previously received from the NASS.

Local configuration shall determine the behaviour of the A-RACF if the QoS profile was not received from NASS.

The A-RACF first matches the Requestor Name in order to identify one or more QoS profile that applies to the request. In case more than one profile is identified, the A-RACF further matches the Media Type and Transport Service Class as received over Rq and in the QoS Profile.

A request over Rq may be denied if no information element set matches the request in accordance with local policies. In this process the Maximum Priority parameter (e4) is compared with the Media Priority parameter (Rq).

The A-RACF shall deny a request from the SPDF if it is not permitted by the selected QoS profile in accordance with local policies. The A-RACF only permits the request from the SPDF if all media can be accepted. In A-RACF, a request can not be partially accepted. When granting such requests the A-RACF may install a traffic policy in the RCEF.

The A-RACF returns the result of the admission control process to the SPDF, which may include a Resource Bundle-Id representing the group to which the granted resource belongs. If the A-RACF decides to associate a session with a Bundle-Id, it should provide the Bundle-Id in every reply to operations requested on the session in question, while that association exists.

NOTE: The way the Resource Bundle-Id is defined is a policy in the A-RACF. It represents a set of resources reservation sessions grouped together by A-RACF policies (e.g. represent the usage of a certain device in the transport network). The Resource Bundle-Id may represent a bundle of resources reservation session.

5.2.3.2.4 Install policies

Traffic policies installed in the RCEF may result in traffic conditioning mechanisms being applied to L2 and/or L3 in the transport data plane. The list below provides some examples of traffic conditioning mechanisms in RCEF that are installed on request from A-RACF by means of generic transport policies:

- pure L2 QoS mechanisms, e.g. VP/VC based for ATM networks, DLCI based for FR networks, or VLAN tag for Ethernet;
- intermediate L2/L3 QoS mechanisms, e.g. MPLS;
- pure L3 QoS mechanisms, e.g. DiffServ;
- L3 over L2 QoS mechanisms, e.g. DiffServ over ATM or FR;
- L3 over intermediate L2/L3, e.g. DiffServ and MPLS seamless integration.

In the context of the present document, A-RACF shall deal only with L3 policies. The use of the remaining policy types is not precluded to be applied by RCEF, which in that case would have to perform a certain policy based on its own interpretation of the L2 parameters, or of the L2 parameters combined with others, included in pre-defined/provisioned traffic policies. This can be achieved by allocating a particular Id to each policy.

As such, A-RACF shall be capable of:

- providing an explicit description of the traffic policies to be applied. This option is only applicable to L3 policies (e.g., DiffServ); and
- attaching a pre-defined traffic policy to the media flow(s). In this case the A-RACF provides a policy-id, which will be translated into specific traffic policies to be applied. This option is applicable to both L3 and L2 policies.

For guaranteed QoS, the A-RACF may enforce its admission control decision by setting L2/L3 QoS traffic policies in the RCEF via the Re reference point to police the subscriber traffic.

NOTE: The A-RACF may set QoS policies in the Access Node (AN) and/or the CPE but the mechanism to do so is outside the scope of Release 1.

For relative QoS, the A-RACF pushes, via the Re reference point, an IP QoS policy that updates dynamically the QoS differentiation parameters (e.g. DiffServ QoS parameters in the RCEF).

5.2.3.2.5 Charging

The A-RACF shall be able to provide charging information for the Request/Modify/Release/Abort commands when necessary.

5.2.3.2.6 Abnormal condition

The A-RACF informs the SPDF that the bearer previously granted is lost in case of loss of connectivity. The A-RACF relinquishes all resource related to the affected resource reservation sessions. The A-RACF may also indicate when a bundle of resources are no longer available.

5.2.3.2.7 Deployment considerations

The architecture allows multiples instances of A-RACF in the same access network. However, a particular resource shall not be controlled by more than one A-RACF at any given time (no overlapping resources).

5.2.3.2.8 Overload control

The A-RACF may provide an overload control mechanism towards the SPDF, which helps to limit the load on the A-RACF should the A-RACF components experience overload. A full specification of this capability is left as an outstanding issue.

5.2.3.3 BGF

5.2.3.3.1 BGF main functions

The BGF is a packet-to-packet gateway for user plane media traffic. The BGF performs both policy enforcement functions and NAT functions under the control of the SPDF in each of the network segments: access, aggregation and core. An overview of the services provided by BGF is given in table 1.

NOTE: Static forwarding functions may be inserted in the IP path. How many functions are inserted and whether each function is acting on user plane media traffic, signalling traffic or both is a matter for each operator to decide. These functions are not visible to the RACS and are therefore outside the scope of the present document.

The BGF has a policy enforcement function that interacts through the Ia reference point with the SPDF and is under the control of the SPDF. The BGF operates on micro-flows, i.e. on individual flows of packets belonging to a particular application session. The BGF's policy enforcement function is a dynamic gate that can block individual flows or allow authorized flows to pass. For an admitted flow the SPDF instructs the BGF to open/close its gate for the particular flow, i.e. to allow the admitted flow to pass through the BGF.

Possible resources that are managed by the BGF includes the handling of a pool of IP addresses/ports and bit rate on the BGF interfaces.

5.2.3.3.2 BGF parameters

Unidirectional micro-flows are specified by the SPDF towards the BGF in terms of a flow classifier including the standard 5-tuple (source IP address, destination IP address, source port, destination port, protocol). Elements of the 5-tuple that are unknown to the SPDF may be wild-carded by the SPDF in the instructions to the BGF.

Per admitted micro-flow, the SPDF may instruct the BGF to apply policies (e.g. traffic-conditioning filter) that limit the throughput of the flow to an admitted level indicated by the SPDF.

The usage of the BGF shall allow different combinations of parameters. As such:

- It must be possible to control the following services: address latching, NAT, QoS marking, bandwidth limiting and usage metering.

- It must be possible to provide media address and port information both towards and from the BGF for NAT control.

- It must be possible to provide mid-session updates related to NAT control and bandwidth policing over the reference point.
- It must be possible to indicate if RTP is used as media transport protocol, in which case the NAT must be able to establish both RTP and RTCP flows.
- It must be possible to provide an address independent media session identifier, since the address information may change during the media session.

5.2.3.3.3 Reference points

The reference point between the SPDF and the BGF is Ia.

5.2.3.3.4 Addressing latching

When a NAT device is located between a UE and the BGF, the remote media IP address/port information provided using signalling information (e.g. a SDP body in a SIP message) can not be used by the BGF to send media towards the user (instead, the media must be sent towards a specific IP address/port of the entity providing the NAT functionalities, reserved for the UE).

In the present document, address latching corresponds to determining the address on which the BGF listens for media on the local IP address/port the BGF has reserved for the remote UE as requested from SPDF. When media is received the BGF stores the IP address/port value from where the media was received (IP address/port of the entity providing the NAT functionality), and uses that information when forwarding media towards the UE. The NAT providing entity then forwards the media to the actual IP address/port of the UE.

5.2.3.3.5 Abnormal conditions

The BGF notifies the SPDF when it detects a network failure condition whereby it can no longer support the previously agreed services, and that will lead to the release of a previously allocated resources.

5.2.3.3.6 Overload control

The BGF may provide an overload control mechanism towards the SPDF, which helps to limit the load on the BGF should the BGF components experience overload. A full specification of this capability is left as an outstanding issue.

5.2.3.4 RCEF

5.2.3.4.1 RCEF main functions

The Resource Control Enforcement Function (RCEF) performs policy enforcement functions under control of the A-RACF.

The RCEF main functions are:

- Enforcement of the policies defined by the access provider:
- opening and closing of gates in order to allow only authorized traffic to flow; marks IP packets in accordance with the filtering criteria received from the A-RACF;
- policing of upstream and downstream traffic to ensure that the traffic remains within the authorized limits.

5.2.3.4.2 Reference points

The traffic policies are provided by the A-RACF to the RCEF through the Re reference point. This reference point will not be standardized in Release 1.

5.2.3.4.3 RCEF parameters

Unidirectional micro-flows are specified by the A-RACF towards the RCEF in terms of a flow classifier including the standard 5-tuple (source IP address, destination IP address, source port, destination port, protocol). Elements of the 5-tuple that are unknown to the A-RACF may be wild-carded by the A-RACF in the instructions to the SPDF.

It must be possible to provide mid-session updates over the Re reference point.

It must be possible to provide an address independent media session identifier, since the address information may change during the media session.

5.2.3.5 L2TF

The L2TF is described in ES 282 001 [2].

5.2.3.6 Application Function (AF)

5.2.3.6.1 AF main functions

This clause looks at requirements on Application Functions (AFs) related to controlling bearer resources. The AF is not a stand-alone functional entity of the NGN architecture. It is a convenient short cut to represent the functionality that exists in some Service Control Subsystems and Applications to interact with the RACS.

The AF is expected to perform the following functionalities:

- The AF shall provide information to the SPDF to identify media flows to express the service expected from RACS and the bandwidth that needs to be authorized and allocated for those flows. Bandwidth requirements shall be complemented with class based service information indicating service expectations such as QoS characteristics, which transfer layer resources that should be used, and whether service from BGF, A-RACF, or both is requested. This class-based information may also capture predefined traffic characteristics. Resource priority requirements may also be supplied.

- The AF shall indicate whether the media should be enabled (i.e. gate opened) when resources are allocated. Alternatively, the gate AF may request that the gate be opened later, after resources are committed.

- The AF shall be capable of issuing reservation modify and release messages that contain the same reservation information as provided in reservation request and commit messages together. The AF shall further be capable of updating time limited reservations through reservation modify messages and through reservation refresh messages.

- In the case where a NAT function is required, the AF shall request address-mapping information and shall do any modifications that may be required to address information within application signalling (e.g. SDP).

- In the case where support of a hosted NAT is required, the AF shall request address latching, since the remote media IP address/port information provided within application signalling (e.g. SDP) cannot be used to send media towards the UE behind the NAT.

- The AF shall provide overload control capabilities, which enable the AF to reduce its resource request rate when overload is detected within the RACS. Also, the AF may request that the RACS reduces its rate of notifications to the AF, in case of overload within the AF. A full specification is left as an outstanding issue.

- The AF may be capable of operating in a mode of operation by means of which the AF request resources for media flows belonging to a single application session per resource request.

- The AF may be capable of operating in any or all of the following modes of operation:
  - the mode where a single resource reservation request per application session is issued by the AF;
  - the mode of operation where multiple independent resource reservation requests per application session are issued either from a single or multiple AFs, where each independent request is intended to reserve a different set of resources within the network.

- The AF is entitled to use Subscriber-Id and/or an IP address to identify to RACS the resource being requested. The decision of what information is provided to RACS depends on the type of application and it is outside of the scope of the present document

5.2.3.6.2 Reference points

The Application Function (AF) interacts with the SPDF via the Gq' interface. It makes requests for bearer resources and may receive notifications when resources are reserved and released.

5.2.3.6.3 Charging

The AF shall be able to provide charging information for the Request/Modify/Release/Abort commands when necessary.

5.2.3.6.4 Abnormal conditions

Abnormal conditions are reported by the SPDF indicating that the current reservations are no long valid. The AF behaviour that follows is application dependent and the RACS does not make any assumption on that. The abnormal condition information is sent to the AF after all resource session and state information is cleared in RACS.

5.3 RACS reference points

5.3.1 Rq reference point (SPDF - A-RACF)

5.3.1.1 Functional requirements

The Rq reference point provides interaction between the SPDF and the A-RACF functional building blocks of the RACS architecture. The Rq requirements are classified in functional and non-functional elements.

The RACF provides facilities for topology-aware resource reservation, resource reservation tracking, and a resource-constraint-based admission control service that shall be addressed through the Rq reference point.

The Rq reference point is used for QoS resource reservation information exchange between the SPDF and the A-RACF. Via the Rq reference point the SPDF issues requests for resources in the access and aggregation networks, indicating IP QoS characteristics.

The Rq reference point is valid for an intra-operator and for inter-operator models.

Following functional requirements are directly derived from the role and position of the Rq reference point in the RACS.

5.3.1.1.1 Resource management mechanisms

The Rq reference point shall support a versatile set of resource management schemes, suitable for coping with all target deployment architectures, as stipulated and defined in this present document. In this context, the following resource management schemes must be supported:

- Proxies resource reservation with policy-push.
- Support for all the scenarios defined in RACS functional architecture:
  - QoS request initiated by Application Function;
  - QoS request initiated by CPE through the application layer signalling with QoS negotiation extensions.
- Flexibility for evolution in future NGN releases.

- The Rq reference point shall provide subsequent resource management models in support of these requirements:
    - Single-stage resource management model, providing resource management services in a mode where reserved resources are immediately available upon successful reservation.
    - Two-stage reserve-commit resource management model that can be leveraged in support of services that aim to support charging per service-invocation, and require as such service-theft-prevention solutions.
    - Authorize-reserve-commit resource management model, supporting service-based local policy control under coordination of a network-hosted application function.

5.3.1.1.2 Service model

The services provided for each of the resource reservation models shall offer the following capabilities:

- The service model shall allow resource reservation for an individual application session that can involve multiple media flows. A media flow may be uni-directional or bi-directional (combining in effect two uni-directional flows).
- The resource management model established through the Rq reference point shall support atomicity of resource management services at the level of an application session. This implies support for collective reservation, release, and modification of resource requirements for all the media flows that belong to the application session.
- A resource requirement budget can be established for each individual service flow of the application session.
- Mid-session modification of previously established resource reservations shall be supported for individual service sessions in an atomic manner (e.g. in support of service session modifications that have to be accommodated on behalf of SIP re-invite). Atomicity shall be guaranteed, per mid-session modification, across all changes that are in order for the individual media flows of the session, including:
    - modification (increase or reduction) of resource requirements reserved on behalf of selected individual media flows;
    - release of resources previously reserved on behalf of a selected individual media flows;
    - creation of new resource reservation on behalf of new individual media flows that are added to the service session.
- Collective release of all resources for an application session.

5.3.1.1.3 Duration semantics

In terms of duration semantics, the resource management model supported by the Rq reference point shall support both soft-state and hard-state resource management approaches along with the following functions:

- for both approaches Rq shall support facilities for explicit removal of previously established resource reservation;
- for both approaches Rq shall support facilities for explicit modification of previously established resource reservation;
- granularity of removal and modification facilities shall be at the level of individual flow reservations;
- Time Limited hard-state with update possibilities;
- Resource Modification Request primitive must be capable of carrying information needed to create reservation states. This means that all parameters provided in Reservation Request message must be possible to include in ReservationModify primitive. Thereby the A-RACF can rely on states kept in AF to support seamless fail over instead of replicating soft state reservations.

5.3.1.1.4 Audit and synchronization support

The only mechanism for synchronization over Rq supported in Release 1 implies the use of soft-state reservation.

The Rq does not support any audit mechanism Release 1.

5.3.1.1.5 Report facilities for unsolicited events

The Rq reference point shall support facilities for indicating, on a per request basis, relevant events such as revocation of established resource reservations.

5.3.1.2 Non-functional requirements

The Rq reference point shall support the non-functional requirements indicated in clauses 5.3.1.2.1 and 5.3.1.2.2.

5.3.1.2.1 Reliability requirements

The Rq reference point shall provide mechanisms to ensure reliability and integrity of all communication performed over the interface.

5.3.1.2.2 Security requirements

The Rq reference point shall provide mechanism to ensure:

- security to the information exchanged in the interface;
- mutual authentication and authorization of legitimate usage.

5.3.1.3 Information exchanged over the Rq Reference Point

5.3.1.3.1 Resource Reservation Request

The resource reservation request message is used to request resources from the SPDF to the A-RACF. The SPDF knows the address of the A-RACF entity based on local configuration data. The Resource Request contains the following information elements:

Table 2: Resource Reservation Request - Information Elements

<table>
<tr><th colspan="4">Resource Req (SPDF -> A-RACF)</th></tr>
<tr><td colspan="3">Application Function Identifier</td><td>Global unique Identifier for the application function instance.</td></tr>
<tr><td colspan="3">Resource Reservation Session ID</td><td>The reference is a unique resource reservation session identifier in the scope of the Application Function Identifier.</td></tr>
<tr><td colspan="3">Subscriber-ID
(optional)</td><td>It identifies the subscriber attached to the access network (see note 1).</td></tr>
<tr><td colspan="3">Globally Unique IP Address (optional)</td><td>Globally Unique address that corresponds to the UNI associated to the subscriber attached to the network (see note 10).</td></tr>
<tr><td rowspan="2"></td><td colspan="2">Assigned IP Address</td><td>The IP address [Ipv4 or Ipv6]</td></tr>
<tr><td colspan="2">Address Realm</td><td>The addressing domain in which the IP address is significant (see note 2).</td></tr>
<tr><td colspan="3">Requestor Name</td><td>Identifies the RACS client requesting the resources (e.g. name of a ASP or group of ASPs). This name corresponds to the Requestor Name in a QoS profile provided by NASS.</td></tr>
<tr><td colspan="3">Service Class</td><td>Service class requested by the SPDF. It reflects the service relationship between the A_RACF and SPDF owners. The set of Service Classes that are offered to an SPDF is an administrative matter.</td></tr>
<tr><td colspan="3">Service Priority (optional)</td><td>The priority associated to the service request that defines the handling precedence by the receiving entity.</td></tr>
<tr><td colspan="3">Charging Correlation Information (CCI) (optional)</td><td>Globally unique identifier for charging correlation purposes.</td></tr>
<tr><td colspan="3">Duration of Reservation (optional)</td><td>Duration of the reservation requested by the client.</td></tr>
<tr><td colspan="3">Media Description</td><td>The media description.</td></tr>
<tr><td rowspan="13"></td><td colspan="2">Media Type</td><td>The pre-defined type of the media for each flow (e.g. Video).</td></tr>
<tr><td colspan="2">Media Id</td><td>Identifier for the specific media.</td></tr>
<tr><td colspan="2">Media Priority (optional)</td><td>The priority associated to the media to be used in the admission control process in A-RACF.</td></tr>
<tr><td colspan="2">Traffic Flow Parameters</td><td>The traffic flow description of the media.</td></tr>
<tr><td rowspan="9"></td><td>Direction</td><td>Direction of the flow.</td></tr>
<tr><td>Flow Id</td><td>Identifier for the specific flow.</td></tr>
<tr><td>IP Addresses</td><td>Source and Destination IP addresses [Ipv4, Ipv6] and Address Realm that each address belongs to (see note 3)</td></tr>
<tr><td>Ports</td><td>Source and Destination Port Numbers (see note 4).</td></tr>
<tr><td>Protocol</td><td>Protocol Id (e.g. UDP, TCP).</td></tr>
<tr><td>Bandwidth</td><td>The maximum request bit rate.</td></tr>
<tr><td>Reservation Class (optional)</td><td>A particular index that identifies a set of traffic characteristics of the flow (e.g. burstiness and packet size).</td></tr>
<tr><td>Transport Service Class (optional)</td><td>Identifies the forwarding behaviour to be applied to the particular flow (see note 5).</td></tr>
<tr><td colspan="3">Commit Id</td><td>Identify if request is to be committed.</td></tr>
<tr><td colspan="4">NOTE 1: At least one of these two parameters - Subscriber-ID or Global Unique IP address - shall be provided.
NOTE 2: It makes the assigned IP address unique, for example it can be a VPN-id.
NOTE 3: An IP address prefix is supported.
NOTE 4: Port Ranges are supported and can be defined by specifying the minimum and maximum value or by using a wildcard.
NOTE 5: Transport Service Class is also part of QoS profile provided by NASS.</td></tr>
</table>

5.3.1.3.2 Resource Modification Request

The resource modification request message is used to modify current resource allocation from the SPDF to the A-RACF. The SPDF knows the address of the A-RACF entity based on local configuration data. The Resource Modification Request contains the following information elements:

Table 3: Resource Modification Request - Information Elements

Resource Mod (SPDF -> A-RACF) (see note)			
Application Function Identifier			Global unique Identifier for the application function instance.
Resource Reservation Session ID			The reference is a unique resource reservation session identifier in the scope of the Application Function (AF) Identifier.
Requestor Name			Identifies the RACS client requesting the resources (e.g. name of a ASP or group of ASPs). This name corresponds to the Requestor Name in a QoS profile provided by NASS.
Service Class			Service class requested by the SPDF. It reflects the service relationship between the A_RACF and SPDF owners. The set of Service Classes that are offered to an SPDF is an administrative matter.
Duration of Reservation (optional)			Duration of the reservation requested by the client.
Charging Correlation Information (optional)			Globally unique identifier for charging correlation purposes.
Service Priority (optional)			The priority associated to a service request that defines the handling precedence by the receiving entity.
Media Description			The media description.
	Media Type		The pre-defined type of the media for each flow (e.g. Video).
	Media Id		Identifier for the specific media.
	Media Priority (optional)		The priority associated to the media to be used in the admission control process in A-RACF.
	Traffic Flow Parameters		The traffic flow description of the media.
		Direction	Direction of the flow.
		Flow Id	Identifier for the specific flow.
		IP Addresses	Source and Destination IP addresses [Ipv4, Ipv6] and Address Realm that each address belongs to.
		Ports	Source and Destination Port Numbers.
		Protocol	Protocol Id (e.g. UDP, TCP).
		Bandwidth	The maximum request bit rate.
		Reservation Class (optional)	A the particular index that identifies a set of traffic characteristics of the flow (e.g. burstiness and packet size).
		Transport Service Class (optional)	Identifies the forwarding behaviour to be applied to the particular flow.
Commit Id			Identify if request is to be committed.
NOTE: Only the Bandwidth inside the Traffic Flow Parameter element can be modified.			

5.3.1.3.3 Resource Request/Modification Confirmation

The resource reservation confirmation message is used to acknowledge the resource reservation or modification by A-RACF. In case the request can not be fulfilled, the appropriate cause is returned to the SPDF.

Table 4: Resource Confirmation - Information Elements

Resource Mod/Req Cnf (A-RACF -> SPDF) (see note)	
Application Function Identifier	Global unique Identifier for the application function instance.
Resource Reservation Session ID	The reference is a unique resource reservation session identifier in the scope of the Application Function Identifier.
Resource Bundle-Id (optional)	Represents a set of resource reservation sessions grouped together by A-RACF policies. It shall be possible to represent a hierarchy of resources in the resource Bundle-Id associated to that particular RACS resource reservation session.
Duration of Reservation Granted (optional)	Duration of the reservation granted by A-RACF.
Result	The result of the request.
NOTE : The optional parameters are not present in case of an unsuccessful result.	

5.3.1.3.4 Resource Release Request

The resource reservation release message is used by the SPDF to relinquish the resource reservation in A-RACF.

Table 5: Resource Release - Information Elements

Resource Rel (SPDF-> A-RACF)	
Application Function Identifier	Global unique Identifier for the application function instance.
Resource Reservation Session ID	The reference is a unique session identifier in the scope of the Application Function Identifier (see note).
NOTE: The presence of a wildcard in the session part of the reference indicates that all resources identified associated to the Application Function Identifier shall be released, otherwise only the specific session is released (it implies all media in the session).	

5.3.1.3.5 Abort Resource Reservation

The abort reservation message is used by the A_RACF to indicate to the SPDF that the resource previously reserved is lost. The message may transport an indication for more than one reservation. The message contains the following elements:

Table 6: Abort Reservation- Information Elements

Abort Res (A-RACF -> SPDF) (see note)	
Application Function Identifier	Global unique Identifier for the application function instance.
Resource Reservation Session ID	The reference is a unique Resource Reservation session identifier in the scope of the Application Function Identifier (see note).
Resource Bundle-Id (optional)	It represents a set of resource reservation sessions grouped together by A-RACF policies. It shall be possible to represent a hierarchy of resources in the resource Bundle-Id associated to that particular RACS resource reservation session.
Time Stamp	The time when the resources were lost.
Cause	The cause that lead to the loss of the reservation.
NOTE: A single message shall be able to carry multiples blocks.	

5.3.2 e4 reference point (A-RACF - NASS)

This is the reference point between the A-RACF and the Customer Location Function (CLF) of the network attachment subsystem (NASS). The reference point e4 is described in ES 282 004 [5].

5.3.3 Ia Reference Point (SPDF -BGF)

This is the reference point between the SPDF and the BGF. This reference point is internal to the administrative domain. The following requirements apply to the reference point.

5.3.3.1 Functional Requirements

5.3.3.1.1 Control of NAT, Hosted NAT traversal and Gating

1) Request of the NAT binding (two terminations, each containing an IP address, port and IP version) to receive and transmit the media flows; information about the allocated bindings must be returned to the requestor.

2) Indicate, in the NAT binding request, the remote source and destination media parameters for each media flow, including possible wildcarding of specific media parameters (in case the information is not known by the controlling node).

3) Indicate, in the NAT binding request, the IP address/port latching for specific terminations (if the information cannot be retrieved from signalling data, the data is known to be incorrect etc).

4) Indicate, in the NAT binding request, the media transport protocol (RTP, T.38, MSRP etc) for each media flow in order for the BGF to be able to perform protocol specific functions (e.g. dual-port reservation for RTP/RTCP, proper statistics collection etc).

5) Indicate, in the NAT binding request, if the media flow is uni- or bi-directional (in case of uni-directional, also indicate the specific direction).

6) Request mid-session modification of media parameters, including a possible request for new IP address/port latching.

5.3.3.1.2 Bandwidth control

1) Request allocation of bandwidth resources needed for a specific media flow.

2) Indicate, in the bandwidth allocation request, the bandwidth policing information.

3) Request mid-session bandwidth modification.

5.3.3.1.3 QoS marking

1) Indicate QoS marking values (e.g. DiffServ/DSCP) for each egress media flow.

5.3.3.1.4 Usage metering and statistics reporting

Report media flow specific usage metering information (octets of sent data etc), when flow is released and during mid-session, if requested.

5.3.3.1.5 Resource state synchronization

Given that resource state synchronization is a required function in order to recover from different failure scenarios, the reference point shall allow:

1) Reporting of BGF state change (due to rebooting, network failure, HW failure etc).

2) Requesting and Reporting of the current BGF resource state

5.3.3.2 Non-Functional Requirements

The Ia reference point shall support the following non-functional requirements.

5.3.3.2.1 Reliability requirements

The Ia reference point shall provide a mechanism to guarantee reliability and integrity of all communication performed over the interface.

5.3.3.2.2 Security requirements

The Ia reference point shall provide a mechanism to guarantee security of the information exchanged in the interface.

5.3.3.3 Information exchanged over the Ia Reference Point

The information elements for the Ia reference point are not described in the present document. Further information is available in the Stage 3 documentation.

5.3.4 Gq' Reference Point (AF - SPDF)

5.3.4.1 Functional Requirements

The Gq' reference point allows the AF to request resources from the RACS. Since the SPDF functional entity can only request policy enforcement from other elements in the RAC subsystem, this implies that the resource reservations performed over Gq' will result, if authorized by the SPDF, in derivative resource reservations and/or service requests over Rq and/or Ia.

Functional requirements over Gq' are therefore a combination of the requirements over Rq and Ia, described in later clauses. However, it should be noted that the Gq' reference point is not a simple aggregation of functions resulting in two separate information flows for Rq-related and Ia-related requests; the Gq' interface also allows for reservations relevant to Rq and Ia to be requested by AFs as a single atomic request, which the SPDF can then split into separate requests and coordinate accordingly depending on the service requested (see clause 5.2.3.1.6 on the SPDF coordination).

5.3.4.2 Non-Functional Requirements

Non-functional requirements for the Gq' reference point on reliability and security are the same as those defined for the Rq reference point in clause 5.3.1.2.

5.3.4.3 Information exchanged over the Gq' Reference Point

Resource reservation requests over Gq' shall be expressed using the same information elements as those over the Rq and Ia (see clauses 5.3.1 and 5.3.3 above), with the exceptions listed in table 7.

Table 7: Information Elements with specific meaning in Gq'

Service Class	Service class requested by the AF. It reflects the service relationship between the AF and SPDF owners. The set of Service Classes that are offered to an AF is an administrative matter.
Resource Bundle-Id	Not transported over Gq'.

NOTE: Information elements exchanged over Gq' are described here as equivalent to those over Rq and Ia. However, the actual values given to these parameters at service execution may be different across each of these interfaces, depending on mappings performed by the SPDF to requests coming from Application Functions according to the operator's local policies.

5.3.5 Re Reference Point (A-RACF - RCEF)

5.3.5.1 Functional Requirements

The RCEF entity ensures facilities for the enforcement of L2/L3 traffic policies defined by the access network provider that are communicated by the A-RACF through the Re reference point.

The Re reference point is used for controlling the L2/L3 traffic policies performed in the transport plane, as requested by the resource management mechanisms, i.e. gating, packet marking, traffic policing and mid-session updates functionalities.

According to the common approach adopted, the RACS interfaces present functional and non-functional requirements.

In clauses 5.3.5.1.1 to 5.3.5.1.1.4, the functional requirements for the Re interface will be described.

5.3.5.1.1 Policy Enforcement Management

5.3.5.1.1.1 Install Policies

After successful authorization of QoS resources, the Re reference point shall allow the A-RACF to install traffic policies in RCEF, in order to enable traffic conditioning in the transport plane.

The installation of a new policy to a particular flow or a group of flows may or may not result in the replacement of a policy previously installed. A confirmation for this request is also required.

In the context of the present document, A-RACF shall deal only with L3 policies. However, the use of the remaining policy types is not precluded to be applied by RCEF, which in that case would have to perform a certain policy based on its own interpretation of the L2 parameters, or of the L2 parameters combined with others, included in pre-defined/provisioned traffic policies. This can be achieved by allocating a particular Id to each policy.

As such, A-RACF shall be capable of:

- providing an explicit description of the traffic policies to be applied. This option is only applicable to L3 policies (e.g., DiffServ); and
- attaching a pre-defined traffic policy to the media flow(s). In this case the A-RACF provides a policy-id, which will be translated into specific traffic policies to be applied. This option is applicable to both L3 and L2 policies.

In addition, the A-RACF shall be capable either:

- to provide an explicit description of the policies to be applied;
- attach a pre-defined policy of RCEF to the media flow(s). In this case the A-RACF provides a policy-id to the RCEF, which is capable of translating the policy-id into specific policies to be applied.

The specific controls that may be requested are indicated in clauses 5.3.5.1.1.1.1 to 5.3.5.1.1.1.3

5.3.5.1.1.1.1 Gating

This functionality is performed by the RCEF in the transport plane. The decision of applying Gate Control is dependent on the request that indicates if the associated gate should be opened or closed, as well as on local policies stored in the A-RACF. This command allows the A-RACF to enable or disable IP flows.

5.3.5.1.1.1.2 Packet marking

This functionality is usually associated with the appliance of QoS differentiation mechanisms involving the DiffServ Edge Function.

Where the associated parameters for the DiffServ Edge Function, i.e., classifiers, meters, packet handling actions, may be statically or dynamically configured on the RCEF.

5.3.5.1.1.1.3 Traffic policing

This functionality shall consist of the inspection of each packet performed by the RCEF in order to enforce the decision of the A-RACF. This inspection shall lead to a packet handling action, in terms of packets matching or not the classification, which will result in packets being forwarded or silently discarded.

5.3.5.1.1.2 Removal of Policies

This mechanism shall be initiated by the A-RACF. Upon reception of this message, the RCEF shall release all the resources associated with an existing traffic policy.

5.3.5.1.1.3 Revoke of policies indication

This mechanism shall be initiated by the RCEF every time an external event occurs denoting that the access information is no longer valid. The RCEF shall notify the A-RACF accordingly, and shall release all the resources associated with an existing reservation.

5.3.5.1.1.4 Audit and synchronization support

Not provided in the present document.

5.3.5.2 Non-functional requirements

5.3.5.2.1 Reliability requirements

Not provided in the present document.

5.3.5.2.2 Security requirements

Not provided in the present document.

5.3.5.3 Information exchanged over the Re Reference Point

The information elements for the Re reference point are not described in the present document.

5.4 RACS Flows: Interaction Procedures

This clause describes the RACS interactions involved within the sub-procedure blocks for Authorize QoS Resources, Resource Reservation with Service-based Policy, Resource Modification, Resource Commit, Resource Release, Report Event and Abort Reservation indicated by the BGF and the A-RACF, Indication of Bearer Release, Resource Reservation Modification. These procedures are utilized to provide Service based Policy for session-based services and Border Gate Function (BGF).

NOTE: In the following scenarios, the sequence used by SPDF to access the A-RACF and BGF is a local decision in the SPDF meaning that the SPDF is able to decide whether to access A-RACF and then BGF, or vice versa, or both in parallel (depending on the input from the AF). This is valid for request, modification and release flows.

5.4.1 Subscriber Attaches to the Access Network

The NASS is responsible for notifying the A-RACF when a subscriber attaches to the network. The NASS provides to A-RACF an association between Subscriber ID/IP address, the bearer used in the access network and additional subscriber access information.

Figure 3 presents the associated procedure:

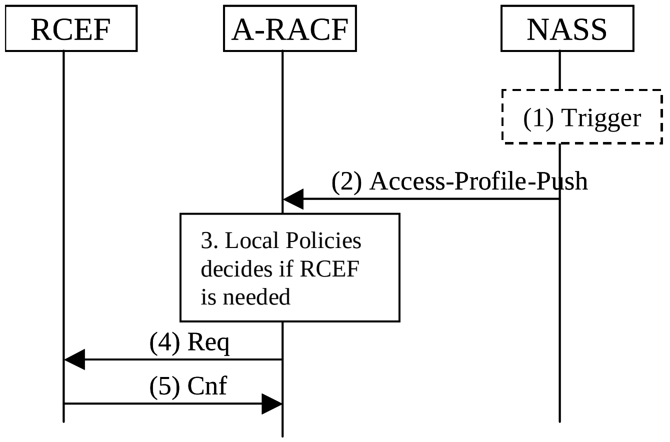


Figure 3

1) The NASS accepts a request from a customer equipment device to obtain bearer resources to attach to the access network or a modification on a subscriber's access profile that has been previously pushed to the RACS by NASS occurs.

2) The NASS sends Access-Profile-Push to inform A-RACF.

3) Based on Local Policies in the A-RACF and the information received from the NASS, the A-RACF decides if any traffic policy need to be installed, changed or removed. The application of the new local policies will apply to new SPDF requests whereas the current reservations are optionally handled according to previous local policies.

4) The A-RACF requests the RCEF to install traffic policies (depending on step 3).

5) The RCEF confirms the installation of the traffic policies (depending on step 4).

5.4.2 Request Resource

This clause provides the flows for resource reservation request from the AF towards the SPDF. Based on SPDF policies, the SPDF decides to contact the A_RACF, BGF or both.

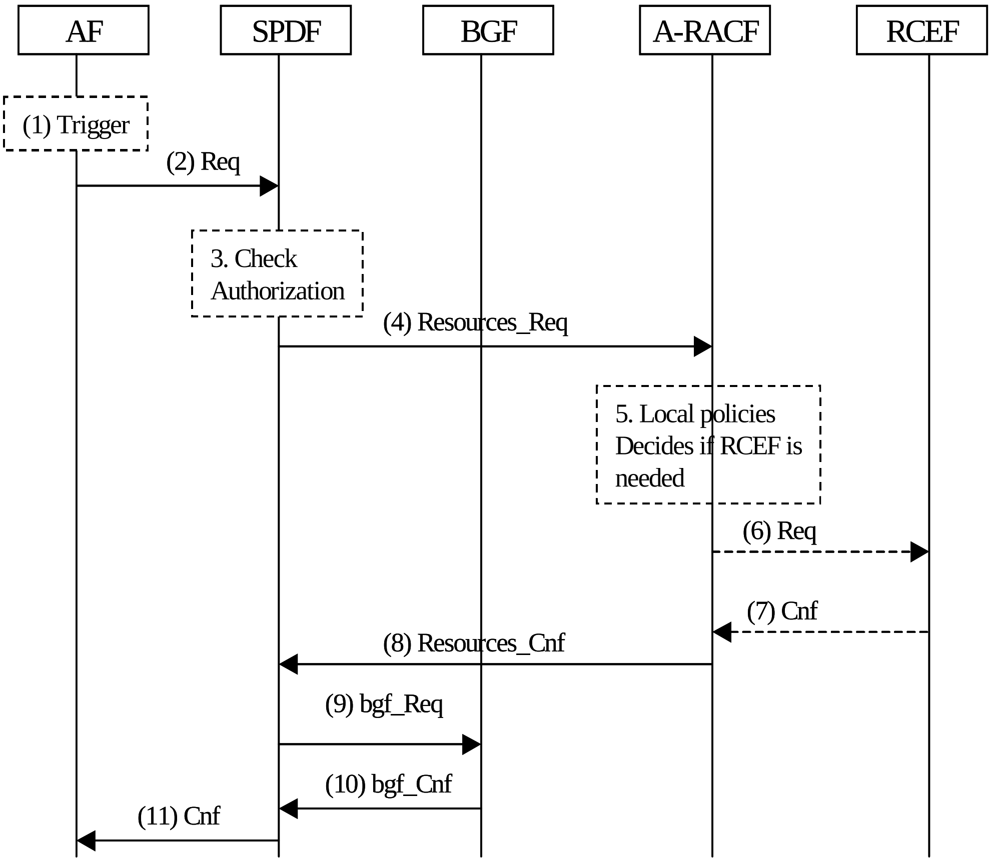


Figure 4

1) An AF session initiation message is received or generated in AF. The AF identifies that this session requires resources in the transport network in order to support the associated media flows.

2) The AF sends a service request information to the SPDF.

3) The SPDF authorizes the request. This process consists of verifying if the required resources for the AF session, present in the service request, are consistent with operator policy rules defined in the SPDF for that particular AF.

4) In case the service is authorized, the SPDF determines how to serve the request. It may be required to send Resources-Req to allocated resources of the A-RACF and/or bgf-Req request to BGF. The SPDF uses the local policies and the parameters in the request in order to take the decision. Therefore, steps 5 to 8 and/or 9 and 10 may not be performed depending on the SPDF decision.

5) The A-RACF maps the request from SPDF into the internal network topology. The A-RACF performs authorization and admission control based on access network policies. The A-RACF also decides if there are traffic policies to be installed in the RCEF.

6) The A-RACF requests the RCEF to install the traffic policies to be applied to the associated flows (depending on step 5).

7) The RCEF confirms the installation of the traffic policies (depending on step 6).

8) The A-RACF sends Resource-Cnf to inform the SPDF if the resources are reserved.

9) The SPDF has determined that serving this request requires sending a request to the appropriate BGF and therefore the SPDF sends bgf_Req to the BGF.

10) The BGF performs the requested service (e.g. allocates the necessary resources to insert a RTP relay function) and confirms the operation to the SPDF.

11) The SPDF forwards the result to the AF.

5.4.3 Release Resource

This clause provides the flows for resource release in A-RACF as well as a service termination in the Border Gateway Function (BGF).

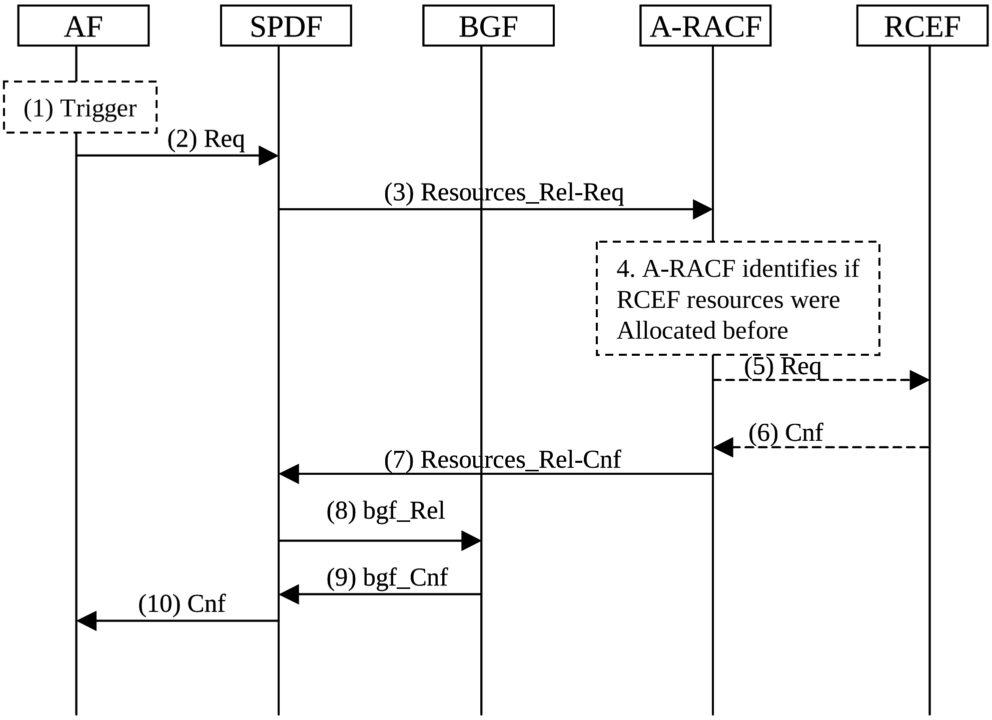


Figure 5

1) An AF session release message is received or generated in AF. The AF identifies that the associated resources shall be released.

2) The AF sends a request to the SPDF to relinquish the resources previously allocated.

3) The SPDF determines that serving this request requires sending a Resources-Rel to A-RACF and/or to request the termination of the BGF service (s). Steps 4 to 7 and/or 8-9 may not be performed.

4) The A-RACF releases all associated resources. The A_RACF checks if there are traffic policies to be removed from the RCEF.

5) The A-RACF requests the RCEF to remove the associated traffic policies (depending on 4).

6) The RCEF confirms the removal of the traffic policies (depending on 5).

7) The A-RACF informs the SPDF that the resources were relinquished.

8) The SPDF determines that a release request is to be sent to the appropriate BGF.

9) The BGF terminates the service (s) and confirms the operation to the SPDF.

10) The SPDF forwards the result to the AF.

5.4.4 Commit Resources procedure: A-RACF

This procedure is triggered by an AF session signalling message received at the AF, or an internal action at the AF. The "Commit Resources" procedure is optional and is only needed if the AF had previously ordered the SPDF to reserve resources without a commit.

The decision where the commit is ultimately performed is based on the SPDF policies.

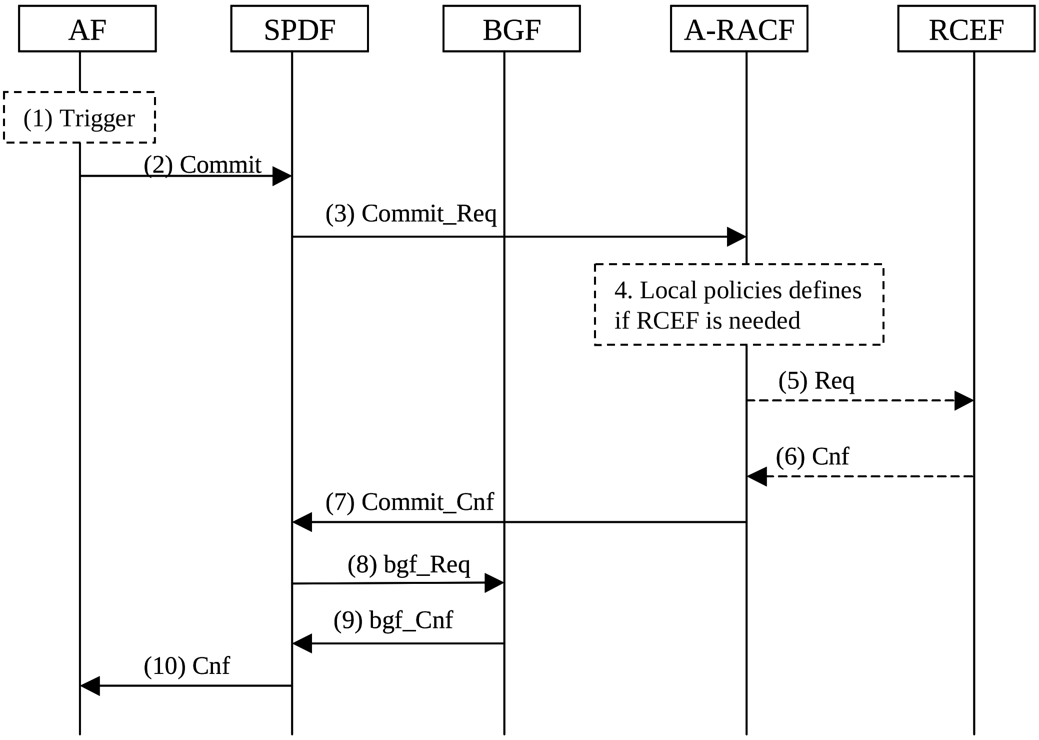


Figure 6

1. An AF session signalling message is received at the AF, or an internal action at the AF triggers the need to enable the transport of the media flow in the access network associated with the application.
2. The Application Function (AF) sends a Commit request to the SPDF.
3. The SPDF sends a Commit-Req message to the A-RACF and/or to the BGF to open the "gate". The decision is based on local policies. Whether steps (4 to 7) and (8 and 9) are executed is dependent on this decision.
4. The A-RACF receives the Commit-Req message. One possible decision of A-RACF is to explicitly open the "gate" in the transport network. This corresponds to the installation of a particular traffic policy in the RCEF.
5. The A-RACF sends a request to install the traffic policies in the RCEF (depending on 4).
6. The RCEF reports to the A-RACF the installation of the traffic policies (depending on 5).
7. The A-RACF reports to the SPDF that the Commit-Req was successfully performed.
8. The SPDF may also (or alternatively) need to perform gate control at the BGF. In such a case the BGF sends a bgf_Req to the BGF.
9. The BGF reports to the SPDF that the action was performed.
10. The SPDF reports to the AF that the Commit was performed.

5.4.5 Resource Modification Request

This procedure is used when the AF session signalling decides to modify the AF session. An update of a previous reservation is requested from the SPDF.

The following figure is applicable to both access sides of a session establishment.

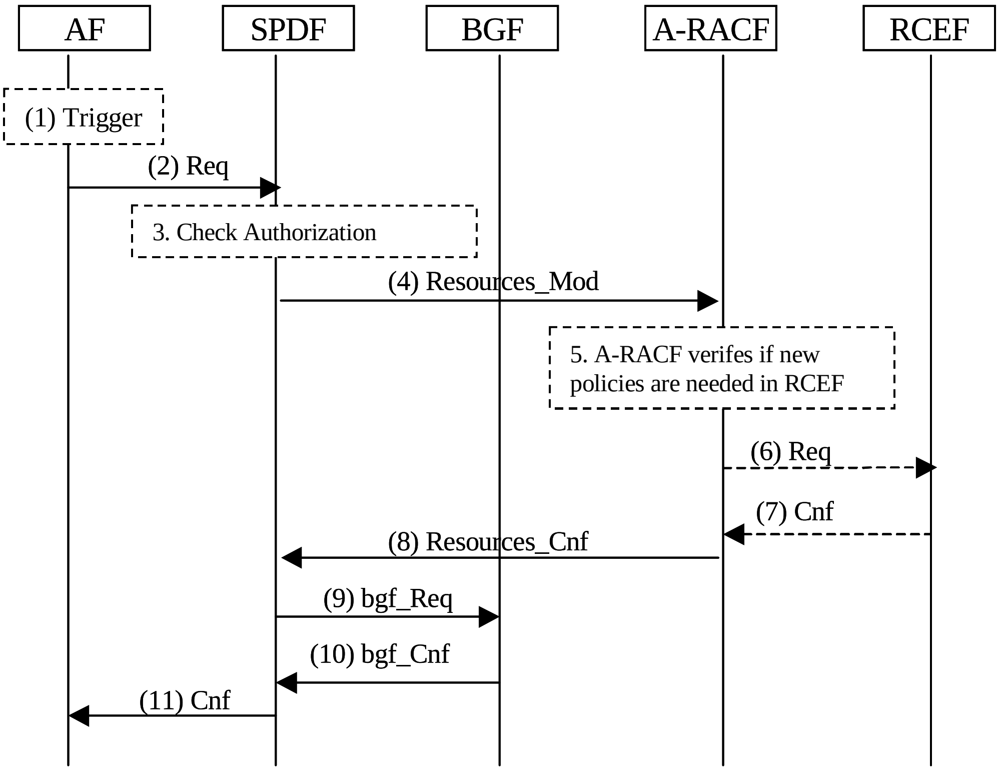


Figure 7

1. An AF session modification results in the need to change the existing resource reservation.

2. The AF sends the service request information to the SPDF.

3. The SPDF shall authorize the request with the modified parameters. This authorization consists of verifying if the modified QoS resources for the AF session, present in the session description, are consistent with the operator policy rules defined in the SPDF. The SPDF determines if serving this request requires sending a Resources-Req to A-RACF and/or bgf-Req request for BGF service(s). Whether steps 4 to 8 and/or 9 and 10 are executed is dependent on this decision.

4. The SPDF has determined that serving this request requires sending a Resources-Mod message to the A-RACF.

5. The A-RACF performs admission control based on access network policies with the new QoS parameters.

6. The A-RACF may request the RCEF to modify the installed traffic policies that are applied to the associated resource reservation session flows.

7. The RCEF confirms the modification of the traffic policies (depending on 6).

8. The A-RACF informs the SPDF that the resources requested are reserved.

9. The SPDF checks if there are also service (s) to be modified in BGF. If yes, a bgf-req is sent to the BGF.

10. The BGF modifies the service (s) and confirms the operation to the SPDF.

11. The SPDF sends the confirmation to the AF.

5.4.6 RACS Retrieves Access Profile from NASS

When A-RACF processes a resource reservation request received from the SPDF, the user's access profile may not be available.

Depending on Local Policies, the A-RACF may pull the Access-Profile from the NASS. This procedure is also applicable to the A-RACF recovery via data synchronization with NASS.

Figure 8 presents the associated procedure:

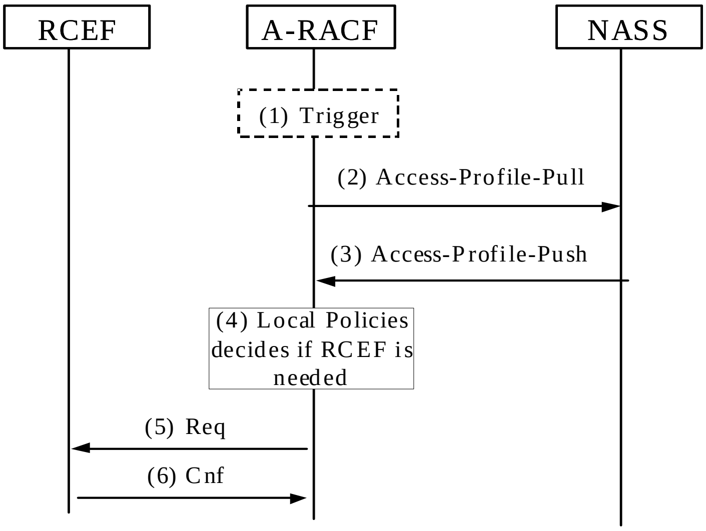


Figure 8

1. This trigger represents the situations where the A-RACF needs the subscriber's access profile and this information is not locally available.
2. The A-RACF sends Access-Profile-Pull message to the NASS for retrieving Access Profile Information.
3. The NASS sends the subscriber associated access profile to the A-RACF using Access-Profile-Push message.
4. Based on the local policies of A-RACF and the information received from the NASS, the A-RACF decides if any traffic policy needs to be installed in the RCEF.
5. The A-RACF requests the RCEF to install the appropriate traffic policies to be applied (depending on step 4).
6. The RCEF confirms the installation of the traffic policies.

5.4.7 Subscriber Detaches from the access network

This procedure presents the flows for the case where the NASS notifies the A-RACF that a certain binding (see scenario in clause 5.4.1) is no longer valid.

NOTE: A similar flow can also represent an internal event in the A-RACF, for example a management decision. In this case the message from the NASS to the A-RACF is not present.

The A-RACF sends a notification towards the AF that the resource reservation is revoked and all associated resources are released.

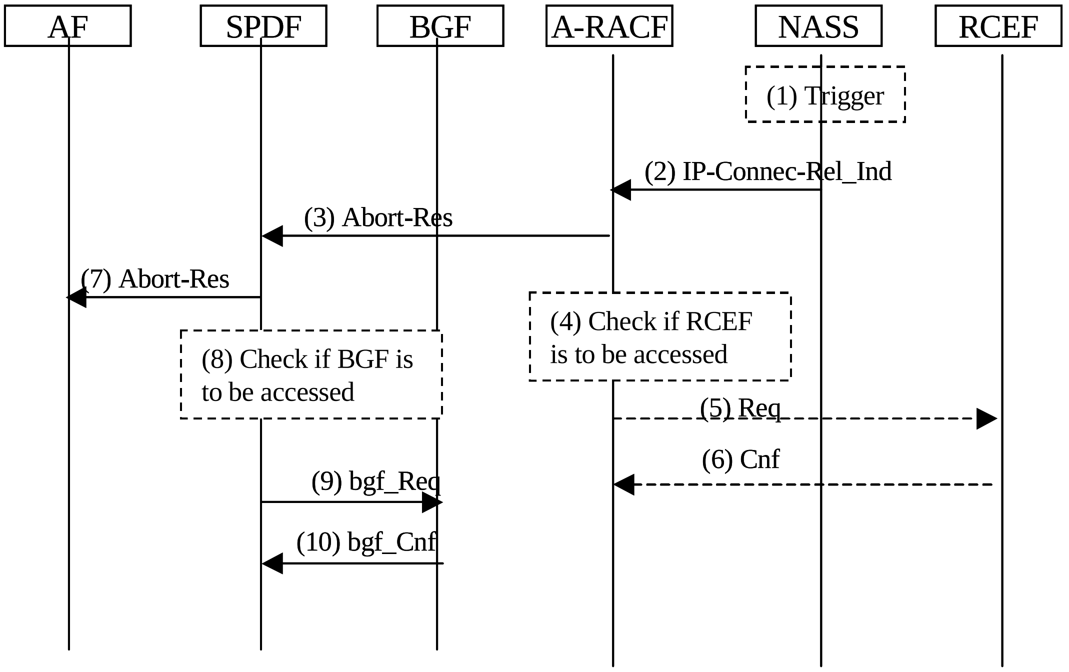


Figure 9

1. The NASS decides that a bearer path is to be released (e.g. the end user equipment sends a release request for the bearer path to NASS).
2. The NASS informs the A-RACF that the access information is no longer valid by sending an IP-Connectivity-Release-Indication.
3. The A-RACF needs to relinquish all resources associated to the IP address/Subscriber-Id. In case there are still outstanding reservations, the A-RACF also notifies the SPDF.
4. The A-RACF checks if there are resources to be released in the RCEF. Whether steps (5) and (6) are executed is dependent on this decision.
5. The A-RACF sends a request to the RCEF for the removal of existing policies.
6. The RCEF confirms the removal of existing policies.
7. The SPDF reports to the AF that the existing reservation was revoked.
8. The SPDF checks if there are resources to be released in the BGF. The execution of steps (9) and (10) are depending on this decision.
9. The SPDF sends a request to the BGF for the removal of allocated resources.
10. The BGF confirms the removal of allocated resources.

5.4.8 Abnormal event from the RCEF

This procedure is used when the A-RACF receives an indication from the RCEF that a certain traffic policy can no longer be sustained. The A-RACF sends a notification towards the AF that the resource reservation was revoked and all associated resources are released.

Figure 10 presents the associated procedure:

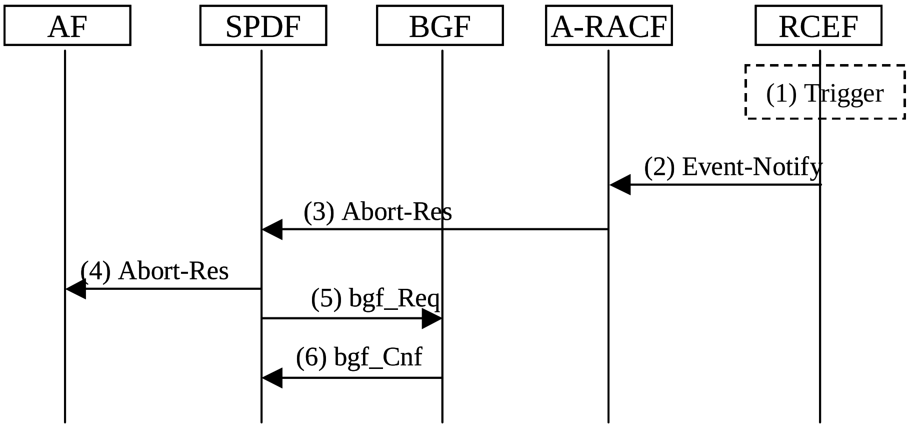


Figure 10

1. The RCEF decides that it can no longer support the previously installed traffic policies (e.g. problem in the interface).
2. The RCEF informs A-RACF that the traffic policies can no longer be applied via an Event-Notify.
3. The A-RACF needs to relinquish all associated resources . In case there are outstanding reservations, the A-RACF notifies the SPDF by sending Abort-Res.
4. The SPDF reports to the AF that the resources were lost by sending Abort-Res.
5. The SPDF checks if there are resources to be released in the BGF. If yes, the SPDF sends a request to the BGF for the removal of allocated resources.
6. The BGF confirms the removal of allocated resources.

5.4.9 Report of BGF Events

The BGF is capable of providing dynamic information about the traffic associated to certain media. As such, applications can request RACS to be notified about certain events, for example the level of traffic usage or media activity.

In the scenario the event is reported to the AF as previously requested.

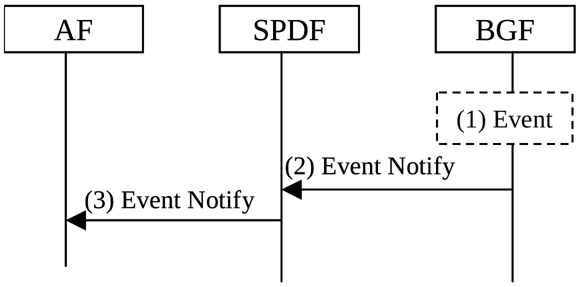


Figure 11

1. The BGF identifies a certain traffic condition needs to be reported in accordance with a service previously requested by the SPDF.

2. The BGF sends the event notification to the SPDF.

3. The SPDF forwards the event notification to the respective AF.

5.4.10 Indication of a BGF Service Failure (Autonomous Release of BGF)

The BGF notifies the SPDF when it detects a condition that leads to the release of previously allocated resources.

Figure 12 presents the particular case where the A-RACF is accessed.

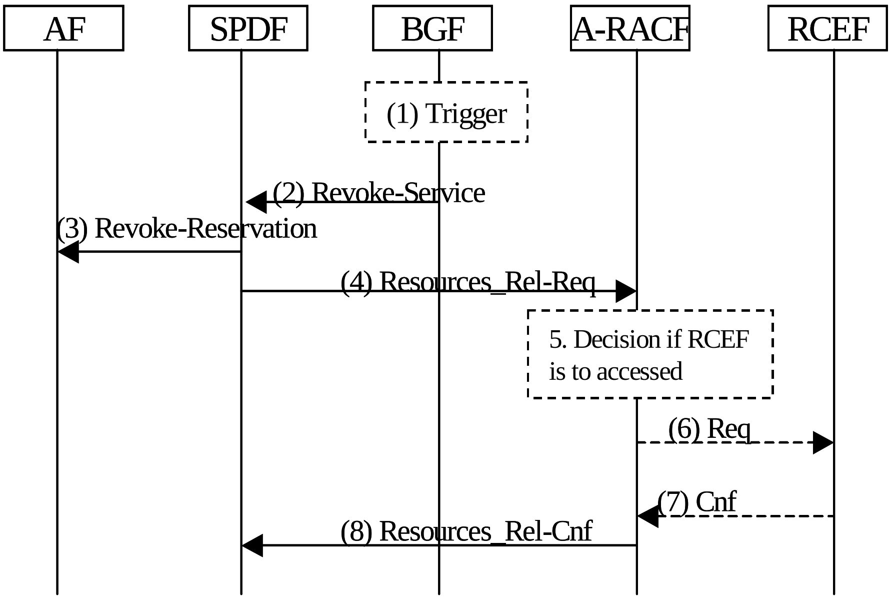


Figure 12

1. The BGF detects a failure that affects an existing service (e.g. interface failure).

2. The BGF informs the SPDF that the policies can no longer be applied via Revoke-Service. The SPDF verifies that there are resources to be released in A-RACF. Whether steps 4-7 are executed is dependent on this decision.

3. The SPDF reports to the AF that the resources of the resource reservation were revoked.

4. The SPDF requests the A-RACF to release the associated resources (depending on step 2).

5. The A-RACF needs to relinquish all resources associated to the associated resource reservation session. The A-RACF checks if there are traffic policies to be removed in the RCEF.

6. The A-RACF contacts the RCEF(depending on step 5).

7. The RCEF replies to the A-RACF.

8. The A-RACF replies to the SPDF with information that the resources are released.

Annex A (informative): Binding Information in RACS, NASS and AF

The example here described uses a xDSL access line to illustrate the use of Subscriber-Id and @IP as binding information. The PPP and DCHP methods are used in a multi-VC environment to illustrate some capabilities offered by the NGN access. It is not the purpose of this annex to limit any other deployment. The same example could also illustrate the Ethernet case by replacing VCs by VLANs.

In this example, " Customer C" has a contract with Access Service Provider S to provide a broadband service.

Figure A.1 gives an example of the usage of the NASS/RACS/AF binding identities. This is a particular implementation that does not preclude other mappings.

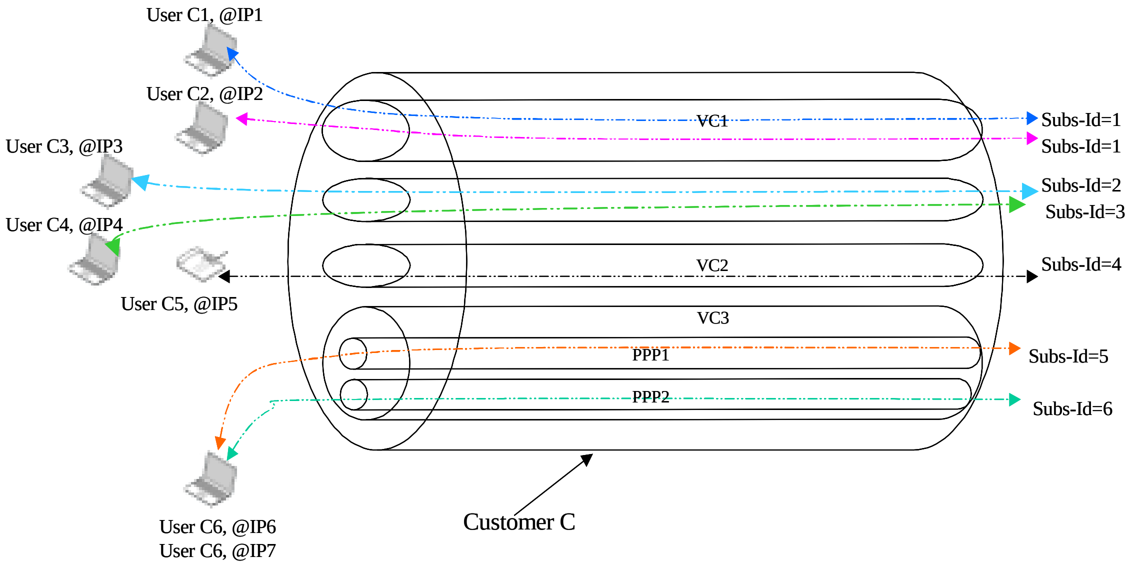


Figure A.1: Example of use of NASS/RACS/AF binding identities

The following consideration applies to the architecture model applied in the access network. It is a particular implementation to illustrate the possibilities of address mapping in NASS.

- Subscriber-ID and or @IP identifies the service bearer resource granted by the network to UE. In the case of PPP, it may identify the bearer (PPP tunnel) that is granted to the end user when the attachment procedure is finished. In case of DHCP, it is expected that Subscriber-ID is derived from the identity of the Client C.

- When an UE attaches to the network , NASS sends to the A-RACF the Subscriber-ID associated to this bearer together with the respective @IP. Different PPP sessions can share the same VC which results that every PPP session may have a different Subscriber-ID, even though those PPP session are over the same VC in the last mile (it does not precludes that the same Subscriber-Id is used). The model allows to the same UE to start multiple PPP sessions.

- When the AF queries the Location of the user to NASS, the AF obtains the same Subscriber-ID as the one sent before by NASS to A-RACF.

- The AF can use the @IP and/or Subscriber-ID to reserve resources from RACS. The SPDF does not modify these parameter.

History

Document history			
V1.1.1	March 2006	Membership Approval Procedure	MV 20060505: 2006-03-07 to 2006-05-05
V1.1.1	June 2006	Publication	