# 3GPP TS 24.411 V8.3.0 (2011-12)

*Technical Specification*

# 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Anonymous Communication Rejection (ACR) and Communication Barring (CB); Protocol specification (Release 8)

Keywords
ISDN, OIP, PSTN, supplementary service

***3GPP***

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

# Contents

# Foreword

This Technical Specification (TS) was been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) and originally published as ETSI TS 183 011 [19]. It was transferred to the 3rd Generation Partnership Project (3GPP) in in January 2008.

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

# 1 Scope

The present document specifies the, stage three, Protocol Description of the Anonymous Communication Rejection (ACR) and Communication Barring (CB) simulation service, based on stage one and two of the ISDN supplementary service Anonymous Call Rejection (ACR), Incoming Communication Barring (ICB) and Outgoing Communication Barring (OCB). Within the Next Generation Network (NGN) the stage 3 description is specified using the IP-Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).

# 2 References

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

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

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

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

## 2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI TS 181 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Multimedia Telephony with PSTN/ISDN simulation services".

[2] ETSI ES 283 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 (Release 7), modified]".

[3] ETSI TS 183 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); Protocol specification".

[4] ETSI TS 183 038: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Simulation Services; Extensible Markup Language (XML) Document Management; Protocol Specification (Endorsement of OMA-TS-XDM-Core-V1-0-20051103-C and OMA-TS-XDM-Shared-V1-0-20051006-C)".

[5] IETF RFC 3266: "Support for IPv6 in Session Description Protocol (SDP)".

[6] ETSI TS 183 023: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating NGN PSTN/ISDN Simulation Services".

[7] Void.

[8] Void.

[9] ETSI TS 183 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Communication Diversion (CDIV); Protocol specification".

[10] ETSI TS 183 028: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Common Basic Communication procedures Protocol specification".

[11] Void.

[12] ETSI TS 183 033: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia; Diameter based protocol for the interfaces between the Call Session Control Function and the User Profile Server Function/Subscription Locator Function; Signalling flows and protocol details [3GPP TS 29.228 V6.8.0 and 3GPP TS 29.229 V6.6.0, modified]".

[13] IETF RFC 3325: "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".

[14] IETF RFC 3323: "A privacy Mechanism for the Session Initiation Protocol (SIP)".

[15] IETF RFC 3455: "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)".

[16] IETF RFC 4745: "Common Policy: A Document Format for Expressing Privacy Preferences".

[17] OMA-TS-XDM-Core-V1-0: "XML Document Management (XDM) Specification", Version 1.0. OMA-TS-XDM-Core-V1-0-1-20061128-A.pdf.

[18] IETF RFC 5079 (December 2007): "Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)".

## 2.2 Informative references

[19] ETSI TS 183 011 V1.3.0: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Anonymous Communication Rejection (ACR) and Communication Barring (CB); Protocol specification".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 181 002 [1] apply.

## 3.2 Abbreviations

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

ACR Anonymous Communication Rejection
AS Application Server
CB Communication Barring

| | |
|---|---|
| CDIV | Communication DIVersion services |
| CONF | CONFerence calling |
| ECT | Explicit Communication Transfer |
| HOLD | communication session HOLD |
| ICB | Incoming Communication Barring |
| IFC | Initial Filter Criteria |
| I-MGCF | Incoming - Media Gateway Control Function |
| IP | Internet Protocol |
| ISUP REL | ISDN Signalling User Part |
| MCID | Malicious Call IDentification |
| MGCF | Media Gateway Control Function |
| OCB | Outgoing Communication Barring |
| OIP | Originating Identification Presentation |
| OIR | Originating Identification Restriction |
| O-MGCF | Outgoing - Media Gateway Control Function |
| P-CSCF | Proxy - Call Session Control Function |
| S-CSCF | Server - Call Session Control Function |
| TIP | Terminating Identification Presentation |
| TIR | Terminating Identification Restriction |
| UE | User Equipment |
| XCAP | eXtended Camel Application Part |
| XML | eXtensible Markup Language |

# 4 Anonymous Communication Rejection (ACR) and Communication Barring (CB)

## 4.1 Introduction

The Communication Barring (CB) service offers the following services:

- The Incoming Communications Barring (ICB) is a service that rejects incoming communications that fulfil certain provisioned or configured conditions on behalf of the terminating user.
- The Anonymous Communication Rejection (ACR) is a particular case of the ICB service, that allows barring of incoming communications from an anonymous originator on behalf of the terminating user.
- The Outgoing Communication Barring (OCB) is a service that rejects outgoing communications that fulfil certain provisioned or configured conditions on behalf of the originating user.

## 4.2 Description

### 4.2.1 General description

The Incoming Communications Barring (ICB**)** service makes it possible for a user to have barring of certain categories of incoming communications according to a provisioned or user configured barring program and is valid for all incoming communications. A barring program is expressed as a set of rules in which the rules have a conditional part and an action part. Examples of conditions are whether the asserted originating public user identity matches a specific public user identity or whether the originating public user identity is restricted (anonymous). The action part could specify for a rule that contains a matching condition that the specific incoming communication shall be barred. The complete set of conditions and actions that apply to this service and their semantics is described in clause 4.9.

The Inhibition of Incoming Forwarded Calls is a special case of the ICB and allows the served user to reject incoming communications from users or subscribers who have diverted the communication towards the served user. The communication history information will be used to trigger the service as described in clause 4.9.

The Anonymous Communication Rejection (ACR) service allows the served user to reject incoming communications on which the asserted public user identity of the originating user is restricted. In case the asserted public user identity of the originating user is not provided then the communication shall be allowed by the ACR service.

An example where the originating user restricts presentation of the asserted public user identity is when he activated the OIR service TS 183 007 [3].

The originating user is given an appropriate indication that the communication has been rejected due to the application of the ACR service.

The Anonymous Communication Rejection (ACR) simulation service is a special case of the ICB service, which is highlighted here because it is a regulatory service in many countries. The ACR service can be activated for a specific subscriber by configuring an ICB service barring rule where the conditional part contains the "Condition=anonymous" and the action part "allow=false".

The Outgoing Communications Barring (OCB) service makes it possible for a user to have barring of certain categories of outgoing communications according to a provisioned or user configured barring program and is valid for all outgoing communications. A barring program is expressed as a set of rules in which the rules have a conditional part and an action part. An example condition is whether the request uri matches a specific public user identity. The action part can specify for a rule that contains a matching condition that the specific outgoing communication it to be barred. The complete set of conditions and actions that apply to this service and their semantics is described in clause 4.9.

## 4.3 Operational requirements

### 4.3.1 Provision/withdrawal

The ACR/CB service shall be provided after prior arrangement with the service provider.

The ACR/CB service shall be withdrawn at the served user's request or for administrative reasons.

### 4.3.2 Requirements on the originating network side

No specific requirements are needed in the network.

### 4.3.3 Requirements in the network

No specific requirements are needed in the network.

### 4.3.4 Requirements on the terminating network side

No specific requirements are needed in the network.

## 4.4 Coding requirements

### 4.4.1 ICB coding requirements

No specific requirements have been identified.

### 4.4.2 ACR coding requirements

The Privacy header field and the P-Asserted-Identity header fields as defined within ES 283 003 [2], are used to trigger the service. The response code 433 (Anonymity Disallowed) defined by RFC 5079 [18] is used in support of ACR service.

### 4.4.3 OCB coding requirements

No specific requirements have been identified.

# 4.5 Signalling requirements

## 4.5.0 General

For user configuration of the ACR/CB services the Ut interface should be used.

See clause 4.9 for further information about the structure of the XML document.

NOTE: Other possibilities for user configuration, as web-based provisioning or pre-provisioning by the operator are outside the scope of the present document.

## 4.5.1 Activation/deactivation

The services ICB, OCB and ACR are individually activated at provisioning or at the subscribers request by using e.g. the Ut interface.

The services ICB, OCB and ACR are individually deactivated at withdrawal or at the subscribers request by using e.g. the Ut interface.

### 4.5.1A Registration/erasure

For registration of information for the services ICB, OCB and ACR, the Ut interface should be used. The detailed information for the services ICB, OCB and ACR can individually be registered at the subscribers request by using the Ut interface.

For erasure of information for the services ICB, OCB and ACR, the Ut interface should be used. The detailed information for the services ICB, OCB and ACR can individually be erased at the subscribers request by using the Ut interface.

### 4.5.1B Interrogation

For interrogation of the services ICB, OCB and ACR, the Ut interface should be used.

## 4.5.2 Invocation and operation

### 4.5.2.1 Actions at the originating UE

Procedures according to ES 283 003 [2] shall apply.

### 4.5.2.2 Actions at the originating P-CSCF

Procedures according to ES 283 003 [2] shall apply.

### 4.5.2.3 Actions at the originating S-CSCF

Procedures according to ES 283 003 [2] shall apply.

NOTE: Annex B includes an example of an IFC that can be used to invoke the OCB simulation service.

#### 4.5.2.4 Actions at the originating AS

##### 4.5.2.4.1 Actions for OCB at the originating AS

Procedures according to ES 283 003 [2] shall apply.

OCB shall reject outgoing communications when the evaluation of the served users outgoing communication barring rules according to the algorithm as specified in clause 4.9.1.2 evaluates to (allow="false"), for the purpose of OCB the "cp:identity" and "ocp:external-list" conditions shall be evaluated against the called party identity which shall be taken from Request-URI and additionally may be taken from the To header field.

When the OCB service rejects a communication, it shall send an indication to the calling user by sending a 603 (Decline) response Additionally, before terminating the communication an announcement can be provided to the originating user. The procedure of invoking an announcement is described within TS 183 028 [10].

#### 4.5.2.5 Actions at the terminating S-CSCF

Procedures according to ES 283 003 [2] shall apply.

NOTE: Annex B includes an example of an IFC that can be used to invoke the ACR/ICB simulation service.

#### 4.5.2.6 Actions at the terminating AS

##### 4.5.2.6.1 Actions for ICB at the terminating AS

Procedures according to ES 283 003 [2] shall apply.

ICB shall reject incoming calls when the evaluation of the served users incoming communication barring rules according to the algorithm as specified in clause 4.9.1.2 evaluates to (allow="false"), for the purpose of ICB the "cp:identity" and "ocp:external-list" conditions shall be evaluated against the calling party identity which shall be taken from the P-Asserted-Identity header field and additionally may be taken from the From header field or the Referred-By header field.

The ACR service is a special case of the ICB service and is expressed as the following rule:

- Condition: =anonymous, Action: allow=false.

Any rule set that evaluates to (allow="false") and where one of the matching rules contained the anonymous condition shall execute the procedures as specified in clause 4.5.2.6.2.

When the ICB service rejects a communication, it shall send an indication to the calling user by sending a 603 (Decline) response Additionally, before terminating the communication an announcement can be provided to the originating user. The procedure of invoking an announcement is described within TS 183 028 [10].

##### 4.5.2.6.2 Action for ACR at the terminating AS

Procedures according to ES 283 003 [2] shall apply.

The ACR service shall reject all incoming communications where the incoming SIP request:

1) includes the P-Asserted-Identity header field AND includes the Privacy header field indicating "id" as specified in RFC 3325 [13]; or

2) includes the P-Asserted-Identity header field AND includes the Privacy header field indicating "header" as specified in RFC 3323 [14]; or

3) includes the P-Asserted-Identity header field AND includes the Privacy header field indicating "user" as specified in RFC 3323 [14].

NOTE: In all other cases the communication proceeds normally.

When the ACR service rejects a communication, the ACR service shall send an indication to the calling user by sending a 433 (Anonymity Disallowed) response. Additionally, before terminating the communication an announcement can be provided to the originating user. The procedure of invoking an announcement is described within TS 183 028 [10].

As a service option the ACR service may forward the communication to a voice message service instead of rejecting the communication with a 433 (Anonymity Disallowed) final response.

#### 4.5.2.7 Actions at the incoming I-CSCF

Procedures according to ES 283 003 [2] shall apply.

#### 4.5.2.8 Actions at the outgoing IBCF

Procedures according to ES 283 003 [2] shall apply.

NOTE: The interworking with other NGN is described in clauses 4.7.

#### 4.5.2.9 Actions at the incoming IBCF

Procedures according to ES 283 003 [2] shall apply.

#### 4.5.2.10 Actions at the BGCF

Procedures according to ES 283 003 [2] shall apply.

NOTE: The interworking with other NGN is described in clauses 4.7.3.

#### 4.5.2.11 Actions at the MGCF

Procedures according to ES 283 003 [2] shall apply.

NOTE: The interworking is described in clause 4.7.1.

#### 4.5.2.12 Actions at the destination P-CSCF

Procedures according to ES 283 003 [2] shall apply.

#### 4.5.2.13 Actions at the destination UE

Procedures according to ES 283 003 [2] shall apply.

## 4.6 Interaction with other services

### 4.6.1 Communication HOLD (HOLD)

No impact, i.e. neither simulation service shall affect the operation of the other service.

### 4.6.2 Terminating Identification Presentation (TIP)

No impact, i.e. neither simulation service shall affect the operation of the other service.

### 4.6.3 Terminating Identification Restriction (TIR)

No impact, i.e. neither simulation service shall affect the operation of the other service.

### 4.6.4 Originating Identification Presentation (OIP)

If the called user has subscribed to the override category according to the OIP service TS 183 007 [3], then the ACR service shall not apply.

Within the network execution of ICB and ACR services shall precede the OIP service.

### 4.6.5 Originating Identification Restriction (OIR)

If the called user has activated the ACR service, then incoming communications of originating user that have activated the OIR service -TS 183 007 [3] are rejected as a consequence of the procedure in clause 4.5.2.6.2.

### 4.6.6 CONFerence Calling (CONF)

If the conference creator activated the OCB service then, REFER request with a refer-to target that is barred by the conference creator's Outgoing Communication Barring (OCB) rules shall not be accepted.

If the conference creator activated the OCB service then, the AS shall remove the URI that is barred by the conference creator's Outgoing Communication Barring (OCB) rules from the list of URIs in the "recipient-list" body of INVITE request.

### 4.6.7 Communication DIVersion services (CDIV)

If the served user has activated the ACR or ICB service, then the ACR or ICB service shall take precedence over the Communication Diversion service for the served user.

If the served user activated the OCB service then, the OCB service shall take precedence on the outgoing communication towards the targeted-to user.

### 4.6.8 Malicious Communication IDentification (MCID)

No impact, i.e. neither simulation service shall affect the operation of the other service.

### 4.6.9 Explicit Communication Transfer (ECT)

No impact, i.e. neither simulation service shall affect the operation of the other service.

## 4.7 Interworking with other networks

### 4.7.1 Interworking with PSTN/ISDN

#### 4.7.1.1 General

Clause 4.7.1 deals with the interworking of:

1) the ACR Supplementary Service executed within the PSTN/ISDN interworking with the NGN; and

2) the ACR service executed within the NGN interworking with the PSTN/ISDN.

The 433 (Anonymity Disallowed) response shall be mapped to the Cause Value Field. Procedures described within the following clauses shall apply.

NOTE: When interworking with existing implementations, the cause value 24 *"call rejected due to ACR supplementary service"* indicating that the call was rejected due to the ACR service, may be lost.

#### 4.7.1.2 SIP-ISUP protocol interworking at the I-MGCF

##### 4.7.1.2.1 Coding of the mapping of REL to 433 (anonymity disallowed) response

If ISUP Cause Value field in the ISUP REL includes Cause Value 24 *"call rejected due to ACR supplementary service"* the I-MGCF maps this to a 433 (Anonymity Disallowed) response.

#### 4.7.1.3 SIP-ISUP protocol interworking at the O-MGCF

##### 4.7.1.3.1 Receipt of the 433 (Anonymity Disallowed) response

If the response is a 433 (Anonymity Disallowed) response, then this response shall be mapped to the ISUP Cause Value field 24 *"call rejected due to ACR supplementary service"* in the ISUP REL.

### 4.7.2 Interworking with PSTN/ISDN Emulation

The interworking with PSTN/ISDN Emulation is for further study.

### 4.7.3 Interworking with external IP networks

The procedures of ES 283 003 [2] shall apply in addition 433 (Anonymity Disallowed) responses are forwarded to other SIP-based networks.

The interworking with non SIP networks is for further study.

## 4.8 Parameter values (timers)

No Timers for ACR/CB defined.

## 4.9 Service configuration

### 4.9.1 Structure of the XML Document

Communication Barring documents are sub-trees of the *simservs* XML document specified in TS 183 023 [6]. As such, Communication Barring documents use the XCAP application usage in TS 183 023 [6].

**Data semantics:** The semantics of the communication barring XML configuration document is specified in clause 4.9.1. "*Structure of the XML Document*".

**XML schema:** Implementations in compliance with the present document shall implement the XML schema that minimally includes the XML Schema defined in clause 4.9.2 "*Communication Barring Rules*" and the *simservs* XML schema specified in clause 6.3 of TS 183 023 [6].

#### 4.9.1.1 General

In addition to the considerations and constraints defined by the *simservs* XML document TS 183 023 [6], the following additional constraints and considerations for the Communication Barring sub-tree are defined.

An instance of the simulation services configuration containing a communication barring configuration document.

```
<?xml version="1.0" encoding="UTF-8"?>
<simservs
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
xmlns:cp="urn:ietf:params:xml:ns:common-policy"
xmlns:ocp="urn:oma:params:xml:ns:common-policy">
  <incoming-communication-barring active="true">
            rule set
  </incoming-communication-barring >
  <outgoing-communication-barring active="true">
            rule set
```

```
  </outgoing-communication-barring >
</simservs>
```

The communication barring service contains a rule set, which specifies how the communication barring service shall react to external stimuli.

### 4.9.1.2 Communication Barring elements

The communication barring configuration is contains a rule set. The rule set reuses the syntax as specified by the common policy draft (see RFC 4745 [16]).

```
<incoming-communication-barring active="true">
  <cp:ruleset>
              rule1
              rule2
  </cp:ruleset>
</ incoming-communication-barring >
```

For evaluating a rule set the algorithm as specified in common policy draft (see RFC 4745 [16], clause 10.2) shall be used.

In clause 4.9.1.3 all allowed conditions are specified, communication barring rules are always evaluated at communication setup time.

The shown "active" attribute is inherited from the simservType from TS 183 023 [6], its meaning is also specified in TS 183 023 [6].

### 4.9.1.3 Communication Barring rules

The Communication Barring service is configured with an ordered set of forwarding rules. The XML Schema reuses the rule syntax as specified by common policy draft (see RFC 4745 [16]). The rules take the following form:

```
<cp:rule id="rule66">
  <cp:conditions>
                    condition1
                    condition2
  </cp:conditions>
  <cp:actions>
    <allow>false</allow>
  </cp:actions>
</cp:rule>
```

When the service processes a set of rules it shall startexecuting the first rule. If:

- the rule has no <conditions> element;
- the rule has an empty <conditions> element; or
- conditions are present and they all evaluate to true;

then the rule matches and the specified action is executed.

Applied to the fragment above which shows the case where conditions are present this means that only if the expression (*condition1* AND *condition2*) evaluates to true that then the *rule66* matches call is executed, if there are more matching rules then the resulting actions shall be combined according to the procedure specified in the common policy draft (see RFC 4745 [16]). If one of the matching rules evaluates to allow=true then the resulting value shall be allow=true and the call continues normally, otherwise the result shall be allow=false and the call will be barred. If there are no matching rules then the result shall be allow=true.

The "id" attribute value of a rule shall uniquely identify the rule within a rule set. This can be used in XCAP usage to address one specific rule.

### 4.9.1.4 Communication Barring rule conditions

The following conditions are allowed by the XML Schema for the communication barring service.

**presence-status:** This condition evaluates to true when the called user's current presence activity status is equal to the value set for this condition. In all other cases the condition evaluates to false.

**cp:identity:** This condition evaluates to true when a provided user's identity matches with the value of the identity element. The interpretation of all the elements of this condition is described in the common policy draft (see RFC 4745 [16]). In all other cases the condition evaluates to false.

**anonymous:** To comply with the requirements as set for simulation of the ACR service, the *anonymous* element shall only evaluate to true when the conditions as set out in clause 4.5.2.6.2 for asserted originating public user identity apply.

**cp:sphere:** Not applicable in the context of the Communication Barring service.

**cp:validity:** Specifies a period. The condition evaluates to true when the current time is within the validity period expressed by the value of this condition. In all other cases the condition evaluates to false.

**media:** This condition evaluates to true when the value of this condition matches the media field in one of the "m=" lines in RFC 3266 [5] offered in an INVITE request. It allows for barring of specific media.

**communication-diverted:** This condition evaluates to true when the incoming communication has been previously diverted.

NOTE: Diverted communication can be recognized by the presence of the History header field, as specified in TS 183 004 [9].

**roaming:** This condition evaluates to true when the served user is registered from an access network other then the served users home network.

NOTE: Whether the served user is registered from another network then the served users home network can be determined from the P-Visited-Network-ID header field specified in RFC 3455 [15] and the P-Access-Network-Info header field specified in RFC 3455 [15] both are provided during the registration process, see ES 283 003 [2], clause 5.7.1.3.

**rule-deactivated:** This condition always evaluates to false. This can be used to deactivate a rule, without loosing information. By removing this condition the rule can be activated again.

**ocp:external-list:** This condition evaluates to true when a provided users identity is contained in an external URI list stored in a OMA-TS-XDM_Shared [17] to which the value of external-list refers. The exact interpretation of this element is specified in OMA-TS-XDM_Core [17].

**ocp:other-identity:** If present in any rule, the "other-identity" element, which is empty, matches all identities that are not referenced in any rule. It allows for specifying a default policy. The exact interpretation of this condition is specified in OMA-TS-XDM_Core [17].

The condition elements that are not taken from the common policy draft (see RFC 4745 [16]) or OMA common policy schema TS 183 038 [4] are defined in the simservs document schema specified in TS 183 023 [6].

#### 4.9.1.5 Communication Barring rule actions

The action supported by the communication barring service is (un)conditional barring of calls. For this the allow action has been defined. The allow action takes a Boolean argument when the value is true calls are allowed to continue, when it is false the call shall be barred.

### 4.9.2 XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ss="http://uri.etsi.org/ngn/params/xml/simservs/xcap" xmlns:cp="urn:ietf:params:xml:ns:common-
policy"
xmlns:ocp="urn:oma:xml:xdm:common-policy"
targetNamespace="http://uri.etsi.org/ngn/params/xml/simservs/xcap" elementFormDefault="qualified"
attributeFormDefault="unqualified">
  <!-- import common policy definitions -->
  <xs:import namespace="urn:ietf:params:xml:ns:common-policy" schemaLocation="common-policy.xsd"/>
  <!-- import OMA common policy extensions -->
```

```
    <xs:import namespace="urn:oma:xml:xdm:common-policy" schemaLocation="OMA-SUP-
    XSD_xdm_commonPolicy-V1_0_2-20070830-A"/>
  <!-- incoming communication barring rule set based on the common policy rule set.-->
  <xs:element name="incoming-communication-barring" substitutionGroup="ss:absService">
    <xs:annotation>
      <xs:documentation>This is the incoming communication barring configuration
       document.</xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:complexContent>
        <xs:extension base="ss:simservType">
          <xs:sequence>
            <!-- add service specific elements here-->
            <xs:element ref="cp:ruleset" minOccurs="0"/>
          </xs:sequence>
        </xs:extension>
        <!-- service specific attributes can be defined here -->
      </xs:complexContent>
    </xs:complexType>
  </xs:element>
  <!-- outgoing communication barring rule set based on the common policy rule set.-->
  <xs:element name="outgoing-communication-barring" substitutionGroup="ss:absService">
    <xs:annotation>
      <xs:documentation>This is the outgoing communication barring configuration
       document.</xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:complexContent>
        <xs:extension base="ss:simservType">
          <xs:sequence>
            <!-- add service specific elements here-->
            <xs:element ref="cp:ruleset" minOccurs="0"/>
          </xs:sequence>
        </xs:extension>
        <!-- service specific attributes can be defined here -->
      </xs:complexContent>
    </xs:complexType>
  </xs:element>
  <!-- communication barring specific extensions to IETF common policy actions-->
  <xs:element name="allow" type="ss:allow-action-type"/>
  <!-- communication barring specific type declarations -->
  <xs:simpleType name="allow-action-type" final="list restriction">
    <xs:restriction base="xs:boolean"/>
  </xs:simpleType>
</xs:schema>
```

# Annex A (informative): Signalling flows

The following signalling flows shows examples showing the use of the ACR service. These flows are not implying that other call scenarios are not valid.

## A.1 ACR termination towards UE-B

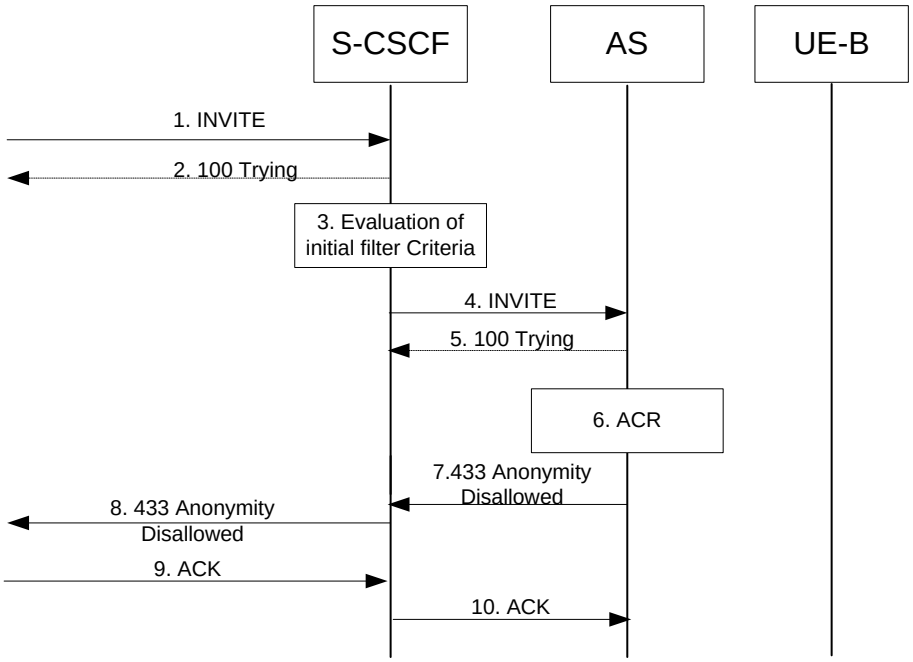


**Figure A.1.1: ACR termination towards UE-B**

**1 to 2. INVITE (UE to S-CSCF) - see example in figure A.1.1.**

The incoming INVITE request is sent to the S-CSCF serving UE-B. The INVITE includes a Privacy header field set to one of the following values: "id" or "header" or "user".

**3. Evaluation of initial filter criteria.**

The initial Filter criteria indicates that the called user is subscribed to the ACR service. Therefore the S-CSCF forwards the INVITE to the ACR AS.

**4 to 5. INVITE (S-CSCF to AS) - see example in figure A.1.1.**

INVITE is sent to the AS.

**6 to 8. 433 (Anonymity Disallowed) response. (AS to UE) - see example in figure A.1.1.**

AS has identified that the call is anonymous and answers with a 433 (Anonymity Disallowed) response.

**9 to 10. The originating party acknowledges the final response with ACK.**

# Annex B (informative): Example of filter criteria

This annex provides an example of a filter criterion that triggers SIP requests that are subject to initial filter criteria evaluation.

When the initial request matches the conditions of the next unexecuted IFC rule for the served user which points to the ACR service and the P-Asserted-Identity header is set to "id", "header" or "user" or "critical", the communication is forwarded to the AS.

An example of an Initial Filter Criteria (IFC) Trigger Point configurations under the assumption that the ACR service is a standalone service that can be invoked by a very specific triggerpoint active at the destination S-CSCF:

- (Method="INVITE" AND [Header="P-Asserted-Identity"] AND [Header="Privacy", Content="id"]); or
- (Method="INVITE" AND [Header="P-Asserted-Identity"] AND [Header="Privacy", Content="header"]); or
- (Method="INVITE" AND [Header="P-Asserted-Identity"] AND [Header="Privacy", Content="user"]); or
- (Method="INVITE" AND [Header="P-Asserted-Identity"] AND [Header="Privacy", Content="critical"]).

NOTE 1: The coding of the Initial Filter Criteria is described in TS 183 033 [12].

NOTE 2: In this case there is a one to one relationship with the conditions that express the rejection cases for the ACR service as specified in clause 4.5.2.6.1 "Action for ACR at the terminating AS".

NOTE 3: In practice it is more likely that all Invite's are forwarded to the AS, because there is more services to execute then ACR alone. This is already apparent when the combined service ACR/ICB is deployed.

# Annex C (informative): Change history

| Change history | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** |
| 2006-03 | | | | | Publication as **ETSI TS 183 011** | | 1.1.1 |
| 2007-03 | | | | | Publication as ETSI TS 183 011 | | 1.2.1 |
| 2008-01 | | | | | Publication as ETSI TS 183 011 | | 1.3.0 |
| 2008-01 | | | | | Convertsion to **3GPP TS 24.411** | | 1.3.1 |
| 2008-03 | CT#39 | CP-080088 | | | Version 1.3.1 approved as CP-080088 and version 7.0.0 created by MCC for publication | 1.3.1 | 7.0.0 |
| 2008-03 | | | | | Based on the decision in CT#39, version 8.0.0 created by MCC | 7.0.0 | 8.0.0 |
| 2008-06 | CT#40 | CP-080350 | 0002 | | Revision of references to documents from IETF SIP working group | 8.0.0 | 8.1.0 |
| 2011-09 | CT#53 | CP-110657 | 0005 | | <conditions> element values | 8.1.0 | 8.2.0 |
| 2011-12 | CT#54 | CP-110857 | 0007 | 2 | Use of "Critical" | 8.2.0 | 8.3.0 |