ETSI TS 124 611 V14.0.0 (2017-04)

**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Anonymous Communication Rejection (ACR) and
Communication Barring (CB) using IP Multimedia (IM)
Core Network (CN) subsystem;
Protocol specification
(3GPP TS 24.611 version 14.0.0 Release 14)**

Reference
RTS/TSGC-0124611ve00

Keywords
GSM,LTE,UMTS

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

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 (https://ipr.etsi.org/).

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 Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights 2
Foreword 2
Modal verbs terminology 2
Foreword 5
1 Scope 6
2 References 6
3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 7
4 Anonymous Communication Rejection (ACR) and Communication Barring (CB) 8
4.1 Introduction 8
4.2 Description 8
4.2.1 General description 8
4.3 Operational requirements 9
4.3.1 Provision/withdrawal 9
4.3.2 Requirements on the originating network side 9
4.3.3 Requirements in the network 9
4.3.4 Requirements on the terminating network side 9
4.4 Coding requirements 9
4.4.1 ICB coding requirements 9
4.4.2 ACR coding requirements 10
4.4.3 OCB coding requirements 10
4.5 Signalling requirements 10
4.5.0 General 10
4.5.1 Activation/deactivation 10
4.5.1A Registration/erasure 11
4.5.1B Interrogation 11
4.5.2 Invocation and operation 11
4.5.2.1 Actions at the originating UE 11
4.5.2.2 Void 11
4.5.2.3 Void 11
4.5.2.4 Actions at the originating AS 11
4.5.2.4.1 Actions for OCB at the originating AS 11
4.5.2.5 Void 12
4.5.2.6 Actions at the terminating AS 12
4.5.2.6.1 Actions for ICB at the terminating AS 12
4.5.2.6.2 Action for ACR at the terminating AS 13
4.5.2.7 Void 14
4.5.2.8 Void 14
4.5.2.9 Void 14
4.5.2.10 Void 14
4.5.2.11 Void 14
4.5.2.12 Void 14
4.5.2.13 Actions at the destination UE 14
4.6 Interaction with other services 14
4.6.1 Communication HOLD (HOLD) 14
4.6.2 Terminating Identification Presentation (TIP) 14
4.6.3 Terminating Identification Restriction (TIR) 14
4.6.4 Originating Identification Presentation (OIP) 14
4.6.5 Originating Identification Restriction (OIR) 14
4.6.6 CONFerence Calling (CONF) 14
4.6.7 Communication DIVersion services (CDIV) 15
4.6.8 Malicious Communication IDentification (MCID) 15
4.6.9 Explicit Communication Transfer (ECT) 15

4.7 Interworking with other networks 15
4.7.1 Void 15
4.7.2 Void 15
4.7.3 Void 15
4.8 Parameter values (timers) 15
4.9 Service configuration 15
4.9.1 Structure of the XML Document 15
4.9.1.0 Definitions 15
4.9.1.1 General 15
4.9.1.2 Communication Barring elements 16
4.9.1.3 Communication Barring rules 16
4.9.1.4 Communication Barring rule conditions 17
4.9.1.5 Communication Barring rule actions 18
4.9.1.6 Supported Conditions for Communication Barring 18
4.9.2 XML Schema 19
4.9.3 XML schema for indication of supported conditions and actions 19

Annex A (informative): Signalling flows 21

A.1 ACR termination towards UE-B 21

A.2 Service configuration 22

Annex B (informative): Example of filter criteria 26

Annex C (informative): Change history 27

History 29

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 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) supplementary 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). It provides the protocol details in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP) and the Session Description Protocol (SDP).

The present document is applicable to User Equipment (UE) and Application Servers (AS) which are intended to support the ACR and CB supplementary services.

2 References

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

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

[1] 3GPP TS 22.173: "IP Multimedia Core Network Subsystem (IMS) Multimedia Telephony Service and supplementary services, Stage 1".

[2] 3GPP TS 24.229: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[3] 3GPP TS 24.607: "Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) using IP Multimedia (IM) Core Network (CN) subsystem; 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 4566: "SDP: Session Description Protocol".

[6] 3GPP TS 24.623: " Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services".

[7] Void.

[8] Void.

[9] 3GPP TS 24.604: "Communication Diversion (CDIV); using IP Multimedia (IM)Core Network (CN) subsystem; Protocol specification".

[10] 3GPP TS 24.628: "Common Basic Communication procedures using IP Multimedia (IM)Core Network (CN) subsystem; Protocol specification".

[11] Void.

[12] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[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 7315: "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 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 (2007): "Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)".

[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".

[20] 3GPP TS 24.238: "Session Initiation Protocol (SIP) based user configuration; stage 3".

[21] IETF RFC 7090 (April 2014): "Public Safety Answering Point (PSAP) Callback".

[22] IETF RFC 3261: "SIP: Session Initiation Protocol".

[23] IETF RFC 5031 (January 2008): "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TS 22.173 [1] apply.

3.2 Abbreviations

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

ACR	Anonymous Communication Rejection
AP	Authentication Proxy
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
IP	Internet Protocol
MCID	Malicious Call IDentification
OCB	Outgoing Communication Barring
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
PSAP	Public Safety Answering Point
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 Communication 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 Communication 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 is barred. The complete set of conditions and actions that apply to this service and their semantics is described in subclause 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 subclause 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 is 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 3GPP TS 24.607 [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) 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 Communication 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 subclause 4.9.

The configuration over the Ut interface of a barring service can be protected by a password. If the subscriber at provisioning time selects the value "by subscriber using a password" for the subscription option "control of barring services", the password is provisioned by the operator at that time. At any later time it is possible to change the password using mechanisms specified in 3GPP TS 24.623 [6].

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.

The communication barring services can be offered with a subscription option "control of barring services". If offered, the subscriber selects one value for the "control of barring services". This subscription option is part of the communication barring profile for the served user. The subscription option is shown in table 4.3.1-1.

Table 4.3.1-1: Subscription option for barring services

Subscription option	Value
control of barring services	by subscriber using a password _____ by the service provider

If the subscriber at provisioning time for the subscription option "control of barring services" selected the value "by subscriber using a password", the service provider provisions an initial password for all communication barring services. Subsequently, the user can change the communication barring password at any time. The procedure to register a new communication barring password over the Ut interface is specified in 3GPP TS 24.623 [6]. The procedure to register a new communication barring password using the SIP based user configuration is specified in 3GPP TS 24.238 [20].

If the subscriber at provision time has selected the value "by the service provider", then an attempt to register a new communication barring password will be rejected as specified in 3GPP TS 24.623 [6] for Ut interface and 3GPP TS 24.238 [20] for SIP based user configuration.

If the service provider does not offer the subscription option "control of barring services", the subscriber can manipulate the barring settings without using a password.

The subscription option "control of barring services" described in this specification corresponds to the "control of supplementary service" option defined in 3GPP TS 24.623 [6] for Ut interface and in 3GPP TS 24.238 [20] for SIP based user configuration.

4.3.2 Requirements on the originating network side

No specific requirements are needed in the network.

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

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.

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

4.4 Coding requirements

4.4.1 ICB coding requirements

No specific requirements have been identified.

To indicate the dynamic ICB the terminating UE shall send either:

- a 603 (Decline) response including a Reason header field containing 603 Decline; or
- a BYE request including a Reason header field containing 603 Decline; or
- an initial INVITE request including a SSC command.

4.4.2 ACR coding requirements

The Privacy header field and the P-Asserted-Identity header fields as defined within 3GPP TS 24.229 [2], are used to trigger the service. The response code 433 (Anonymity Disallowed) defined by IETF 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

Configuration of supplementary services by the user should:

- take place over the Ut interface using XCAP as enabling protocol as described in 3GPP TS 24.623 [6]; or
- use SIP based user configuration as described in 3GPP TS 24.238 [20].

NOTE: Other possibilities for user configuration, such as web-based provisioning or pre-provisioning by the operator are outside the scope of the present document, but are not precluded

If the subscription option "control of barring services" is set to "by subscriber using a password", the subscriber needs to provide a password when manipulating the barring supplementary service.

If the subscription option "control of barring services" is set to "by the service provider", the barring supplementary service cannot be manipulated by the subscriber. The manipulation of the barring supplementary service has to be performed by the service provider. An attempt to manipulate the barring supplementary service over Ut interface will be rejected as specified in 3GPP TS 24.623 [6]. An attempt to manipulate the barring supplementary service using SIP based user configuration will be rejected as specified in 3GPP TS 24.238 [20].

For password handling, when the UE is using the Ut interface for service configuration, the UE shall follow the procedures specified in 3GPP TS 24.623 [6]. The UE can learn that a password is required by finding a "password-required" attribute set to "true" in both the <incoming-communication-barring> and the <outgoing-communication-barring> elements.

For password handling, when the UE is using the SIP based user configuration, the UE shall follow the procedures specified in 3GPP TS 24.238 [20].

The enhancements to the XML schema for use over the Ut interface are described in subclause 4.9.

4.5.1 Activation/deactivation

The services ICB, OCB and ACR are individually activated at provisioning or at the subscribers request by using the mechanisms specified in subclause 4.5.0.

The services ICB, OCB and ACR are individually deactivated at withdrawal or at the subscribers request by using the mechanisms specified in subclause 4.5.0.

4.5.1A Registration/erasure

For registration of information for the services ICB, OCB and ACR, the mechanisms specified in subclause 4.5.0 should be used. The detailed information for the services ICB, OCB and ACR can individually be registered at the subscribers request by using the mechanisms specified in subclause 4.5.0.

For erasure of information for the services ICB, OCB and ACR, the mechanisms specified in subclause 4.5.0 should be used. The detailed information for the services ICB, OCB and ACR can individually be erased at the subscribers request by using the mechanisms specified in subclause 4.5.0.

4.5.1B Interrogation

For interrogation of the services ICB, OCB and ACR, the mechanisms specified in subclause 4.5.0 should be used.

For interrogation of the supported conditions and actions that can be used in the network the Ut interface should be used.

4.5.2 Invocation and operation

4.5.2.1 Actions at the originating UE

Procedures according to 3GPP TS 24.229 [2] shall apply.

4.5.2.2 Void

4.5.2.3 Void

4.5.2.4 Actions at the originating AS

4.5.2.4.1 Actions for OCB at the originating AS

The AS providing the OCB service shall operate as either an AS acting as a SIP proxy as specified in subclause 5.7.4 of 3GPP TS 24.229 [2] or an AS providing 3rd party call control, and specifically as a routeing B2BUA, as specified in subclause 5.7.5 of 3GPP TS 24.229 [2]. An AS providing the OCB service and rejecting the request shall operate as a terminating UA, as specified in subclause 5.7.2 of 3GPP TS 24.229 [2].

NOTE: For the case when the session is not subject to OCB according the requirements in this document, and is the only service being applied by the AS, then the AS only needs to act as a SIP proxy. If additional services are applied, then the AS might need to act as a routeing B2BUA.

The AS providing the OCB service shall reject outgoing communications when the evaluation of the served users outgoing communication barring rules according to the algorithm as specified in subclause 4.9.1.2 evaluates to (allow="false"),.Outgoing communications towards emergency services are always allowed irrespective of what barring settings the user has defined. To allow emergency calls to go through, the operator creates a white list, as described in subclause 4.9.1.3, including emergency numbers in any useful format including emergency service URNs specified in RFC 5031[23]. For the purpose of OCB, the AS shall evaluate the "cp:identity" and "ocp:external-list" conditions against the called party identity taken from Request-URI or additionally taken from the To header field.

When the AS providing the OCB service rejects a communication, the AS shall send an indication to the calling user by sending a 603 (Decline) response Additionally, before terminating the communication the AS can provide an announcement to the originating user. The procedure of invoking an announcement is described within 3GPP TS 24.628 [10].

4.5.2.5 Void

4.5.2.6 Actions at the terminating AS

4.5.2.6.1 Actions for ICB at the terminating AS

The AS providing the ICB service shall operate as either an AS acting as a SIP proxy as specified in subclause 5.7.4 of 3GPP TS 24.229 [2] or an AS providing 3rd party call control, and specifically as a routeing B2BUA, as specified in subclause 5.7.5 of 3GPP TS 24.229 [2]. An AS providing the ICB service and rejecting the request shall operate as a terminating UA, as specified in subclause 5.7.2 of 3GPP TS 24.229 [2].

NOTE 1: For the case when the session is not subject to ICB according the requirements in this document, and is the only service being applied by the AS, then the AS only needs to act as a SIP proxy. If additional services are applied, then the AS might need to act as a routeing B2BUA.

The AS shall based on local policy on how to handle PSAP callbacks suppress ICB when the received initial INVITE request towards the served user is identified as a PSAP callback.

The mechanism to identify an INVITE request as a PSAP callback depends on local policy and can be based on the PSAP callback indicator specified in IETF RFC 7090 [21].

The AS providing the ICB service shall reject initial incoming requests when the evaluation of the served users incoming communication barring rules according to the algorithm as specified in subclause 4.9.1.2 evaluates to (allow="false"). For the purpose of ICB, the AS shall evaluate the "cp:identity" and "ocp:external-list" conditions against the calling party identity taken from the P-Asserted-Identity header field or additionally taken from the From header field or the Referred-By header field.

NOTE 2: The procedures give the flexibility for OPTIONS requests to be treated differently to the equivalent INVITE requests. Unless this capability is specifically required, care is needed in the design of the rules to treat these identically. Rejecting an incoming OPTIONS request can cause the originator not to attempt to place a call to the intended recipient of the OPTIONS.

The dynamic ICB is a network option to extend the ICB functionality:

To bar an incoming request, the AS providing the dynamic ICB service receives from the terminating UE:

- a 603 (Decline) response including a Reason header field containing 603 Declinefor a dialog initiating request
- a BYE request including a Reason header field containing 603 Decline or
- an initial INVITE request including a SSC command.

The AS providing the dynamic ICB service shall store the following information:

- Actual identity of caller: Network asserted identity of the calling user which is stored in the network and additionally the identity included within the From header (defined in IETF RFC 3261 [22]). If the received identity is a restricted identity (a Privacy header field with the values "user", "header" or "id") then the actual identity of the caller shall never be presented or be accessable (e.g. via the blacklist maintenance) to the served user.

NOTE 3: If the barred caller has requested privacy (e.g. by subscribing to ORI service) the served user may just see "Anonymous" or "Unknown". However the served user can invoke dynamic ICB since the network knows the true identity of the caller. To facilitate the management of the list of barred callers, the served user may use the reason field to identify the barred caller.

- Start and end date for barring: Define the duration of barring. If not provided, it implies that the caller should be barred permanently or for a maximum lifetime which is set by the network operator preferences.

Depending on operator policy, the following information may be additionally provided by the user at the time of barring and shall be associated by the AS with the actual identity:

- Reason: The reason for barring (e.g. "Telemarketer"), and

- Published identity of caller: This consists of the actual identity of the caller; "a valid SIP URI", or "private user identity", or "anonymous" if the caller has opted for privacy. This identity is conveyed by P-Asserted Identity or as an option by the From header (defined in IETF RFC 3261 [22]).

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

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

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

When the AS providing the ICB service rejects a communication, the AS shall send an indication to the calling user by sending a 603 (Decline) response Additionally, if the barred communication is a voice or video call, before terminating the communication the AS can provide an announcement to the originating user. The procedure of invoking an announcement is described within 3GPP TS 24.628 [10].

4.5.2.6.2 Action for ACR at the terminating AS

The AS providing the ACR service shall operate as either an AS acting as a SIP proxy as specified in subclause 5.7.4 of 3GPP TS 24.229 [2] or an AS providing 3rd party call control, and specifically as a routeing B2BUA, as specified in subclause 5.7.5 of 3GPP TS 24.229 [2]. An AS providing the ACR service and rejecting the request shall operate as a terminating UA, as specified in subclause 5.7.2 of 3GPP TS 24.229 [2].

NOTE: For the case when the session or transaction is not subject to ACR according the requirements in this document, and is the only service being applied by the AS, then the AS only needs to act as a SIP proxy. If additional services are applied, then the AS might need to act as a routeing B2BUA.

The AS providing 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 IETF RFC 3325 [13]; or

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

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

NOTE: In all other cases the communication proceeds normally.

When the AS providing the ACR service rejects a communication, the AS shall send an indication to the calling user by sending a 433 (Anonymity Disallowed) response. Additionally, if the barred communication is a voice or video call, before terminating the communication the AS can provide an announcement to the originating user. The procedure of invoking an announcement is described within 3GPP TS 24.628 [10].

If the barred communication is a voice or video call, as a service option the AS providing the ACR service can forward the communication to a voice message service instead of rejecting the communication with a 433 (Anonymity Disallowed) final response.

4.5.2.7 Void

4.5.2.8 Void

4.5.2.9 Void

4.5.2.10 Void

4.5.2.11 Void

4.5.2.12 Void

4.5.2.13 Actions at the destination UE

Procedures according to 3GPP TS 24.229 [2] shall apply.

To indicate the barring, a destination UE which supports dynamic ICB shall send:

- a 603 (Decline) response including a Reason header field containing 603 Decline when the communication status is in early dialog; or
- a BYE request including a Reason header field containing 603 Decline when the communication status is in confirmed status; or
- an initial INVITE request including an SSC command after the session is released.

4.6 Interaction with other services

4.6.1 Communication HOLD (HOLD)

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

4.6.2 Terminating Identification Presentation (TIP)

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

4.6.3 Terminating Identification Restriction (TIR)

No impact, i.e. neither 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 3GPP TS 24.607 [3], then the AS providing ACR service shall not apply the requirements of this document.

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 -3GPP TS 24.607 [3] are rejected as a consequence of the procedure in subclause 4.5.2.6.2.

4.6.6 CONFerence Calling (CONF)

If the conference creator activated the OCB service then, the AS providing the CB service shall reject REFER requests with a refer-to target that is barred by the conference creator's Outgoing Communication Barring (OCB) rules.

If the conference creator activated the OCB service then, the AS providing the CB service 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 service shall affect the operation of the other service.

4.6.9 Explicit Communication Transfer (ECT)

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

4.7 Interworking with other networks

4.7.1 Void

4.7.2 Void

4.7.3 Void

4.8 Parameter values (timers)

No Timers for ACR/CB defined.

4.9 Service configuration

4.9.1 Structure of the XML Document

4.9.1.0 Definitions

Communication Barring documents are sub-trees of the *simservs* XML document specified in 3GPP TS 24.623 [6]. As such, Communication Barring documents use the XCAP application usage in 3GPP TS 24.623 [6].

Data semantics: The semantics of the communication barring XML configuration document is specified in subclause 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 subclause 6.3 of 3GPP TS 24.623 [6].

4.9.1.1 General

In addition to the considerations and constraints defined by the *simservs* XML document 3GPP TS 24.623 [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 services react to external stimuli.

4.9.1.2 Communication Barring elements

The communication barring configuration contains two communication barring elements, one for incoming-communication-barring and one for outgoing-communication-barring. Each barring element contains a rule set. The rule set reuses the syntax as specified by the common policy draft (see IETF RFC 4745 [16]).

Incoming-communication-barring element has the following form:

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

Outgoing-communication-barring element has the following form:

```
  <outgoing-communication-barring active="true">
    <cp:ruleset>
               rule3
               rule4
    </cp:ruleset>
  </outgoing-communication-barring>
```

For evaluating a rule set the AS shall use the algorithm as specified in common policy draft (see IETF RFC 4745 [16], subclause 10.2).

In subclause 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 3GPP TS 24.623 [6], its meaning is also specified in 3GPP TS 24.623 [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 IETF 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 AS providing the service processes a set of rules, the AS shall start executing 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 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 IETF 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.

To create a white list of identities towards which outgoing communications are always allowed, rules where the action is allow=true can be created. User or operator provided white lists may be built. Operator defined rules shall not be exposed over the Ut interface.

NOTE: Operator provided white lists are provisioned over a proprietary interface.

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 IETF 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 only evaluate to true when the conditions as set out in subclause 4.5.2.6.2 for asserted originating public user identity apply.

request-name: This condition evaluates to true when the incoming SIP request name matches whith the value of the request-name element.

NOTE 1: The absence of this condition means that the barring rules apply to all initial incoming requests.

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 IETF RFC 4566 [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 2: Diverted communication can be recognized by the presence of the History-Info header field, as specified in 3GPP TS 24.604 [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 3: 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 IETF RFC 7315 [15] and the P-Access-Network-Info header field specified in IETF RFC 7315 [15] both are provided during the registration process, see 3GPP TS 24.229 [2], subclause 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].

international: This condition evaluates to true when the request URI of the outgoing SIP request:

- corresponds to a telephone number, i.e. a SIP URI with a "user" URI parameter set to "phone" or a tel URI; and
- does not point to a destination served by a network within the country where the originating user is located when initiating the communication.

international-exHC: This condition for international barring, excluding the home country, evaluates to true when the request URI of the outgoing SIP request:

- corresponds to a telephone number, i.e. a SIP URI with a "user" URI parameter set to "phone" or a tel URI;
- does not point to a destination served by a network within the country where the originating user is located when initiating the communication; and
- does not point to a destination served within the served users home network.

NOTE 4: In case of international and international-exHC, called users subscribed to a network in the country in which the served user roams, can be called irrespective where they roam. Subscribers, subscribed to any network in another country than the one in which the served user is located cannot be called even if they roam in the same network area as the served users or in the served user's home network.

The condition elements that are not taken from the common policy draft (see IETF RFC 4745 [16]) or OMA common policy schema ETSI TS 183 038 [4] are defined in the simservs document schema specified in 3GPP TS 24.623 [6].

Information of which of the above mentioned conditions the user is allowed to use can be obtained from the network by using the schema defined in subclause 4.9.3.

The "serv-cap-media" element lists the elements that can be used in the "media" rule condition.

4.9.1.5 Communication Barring rule actions

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

4.9.1.6 Supported Conditions for Communication Barring

The supported conditions for communication barring are configured with a list of condition capability elements. These capability elements are read only and indicate which capabilities related to communication barring the network has provisioned for a user. There is one rule capability element per each rule condition.

EXAMPLE: An instance of the simulation services configuration containing a service capabilities document for communication barring is shown in the following example. In this example, the same capabilities as in Call Barring in a CS network are supported.

```
<?xml version="1.0" encoding="UTF-8"?>
<simservs>
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
  <communication-barring-serv-cap active="true">
    <serv-cap-conditions>
       <serv-cap-communication-diverted provisioned="false"></serv-cap-communication-diverted>
       <serv-cap-external-list provisioned="false"></serv-cap-external-list>
       <serv-cap-identity provisioned="false"></serv-cap-identity>
       <serv-cap-media>
          <media>audio</media>
          <media>video</media>
       </serv-cap-media>
       <serv-cap-other-identity provisioned="false"></serv-cap-other-identity>
```

```
       <serv-cap-presence-status provisioned="false"></serv-cap-presence-status>
       <serv-cap-roaming provisioned="false"></serv-cap-roaming>
       <serv-cap-rule-deactivated provisioned="false"></serv-cap-rule-deactivated>
       <serv-cap-request-name provisioned="false"></serv-cap-request-name>
       <serv-cap-validity provisioned="false"></serv-cap-validity>
       <serv-cap-unconditional provisioned="true"></serv-cap-unconditional>
    </serv-cap-conditions>
</communication-barring-serv-cap>
</simservs>
```

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="xdm_commonPolicy-V1_0"/>
  <!-- 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:attribute name="password-required" type="xs:boolean" default="false" use="optional">
      </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:attribute name="password-required" type="xs:boolean" default="false" use="optional">
      </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>
```

4.9.3 XML schema for indication of supported conditions and actions

```
<?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"
```

```
targetNamespace="http://uri.etsi.org/ngn/params/xml/simservs/xcap" elementFormDefault="qualified"
attributeFormDefault="unqualified">
  <xs:annotation>
    <xs:documentation xml:lang="en">This schema defines elements that are used to inform the UE
which conditions and actions the network support.</xs:documentation>
  </xs:annotation>
  <xs:include schemaLocation="XCAP.xsd"/>
  <xs:element name="communication-barring-serv-cap" substitutionGroup="ss:absService">
    <xs:complexType>
      <xs:complexContent>
        <xs:extension base="ss:simservType">
          <xs:sequence>
            <xs:element name="serv-cap-conditions" minOccurs="0">
              <xs:complexType>
                <xs:sequence>
                  <xs:element name="serv-cap-anonymous" type="ss:provisioned-type" minOccurs="0"/>
                  <xs:element name="serv-cap-request-name" type="ss:provisioned-type"
minOccurs="0"/>
                  <xs:element name="serv-cap-communication-diverted" type="ss:provisioned-type"
minOccurs="0"/>
                  <xs:element name="serv-cap-external-list" type="ss:provisioned-type"
minOccurs="0"/>
                  <xs:element name="serv-cap-identity" type="ss:provisioned-type" minOccurs="0"/>
                  <xs:element name="serv-cap-international" type="ss:provisioned-type"
minOccurs="0"/>
                  <xs:element name="serv-cap-international-exHC" type="ss:provisioned-type"
minOccurs="0"/>
                  <xs:element name="serv-cap-media" type="ss:supported-media-type" minOccurs="0"/>
                  <xs:element name="serv-cap-other-identity" type="ss:provisioned-type"
minOccurs="0"/>
                  <xs:element name="serv-cap-presence-status" type="ss:provisioned-type"
minOccurs="0"/>
                  <xs:element name="serv-cap-roaming" type="ss:provisioned-type" minOccurs="0"/>
                  <xs:element name="serv-cap-rule-deactivated" type="ss:provisioned-type"
minOccurs="0"/>
                  <xs:element name="serv-cap-validity" type="ss:provisioned-type" minOccurs="0"/>
                  <xs:element name="serv-cap-unconditional" type="ss:provisioned-type"
minOccurs="0"/>
                </xs:sequence>
              </xs:complexType>
            </xs:element>
          </xs:sequence>
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Annex A (informative): Signalling flows

The following signalling flows show examples of the configuration and the use of the ACR and CB services. These flows are not implying that other scenarios are not valid.

A.1 ACR termination towards UE-B

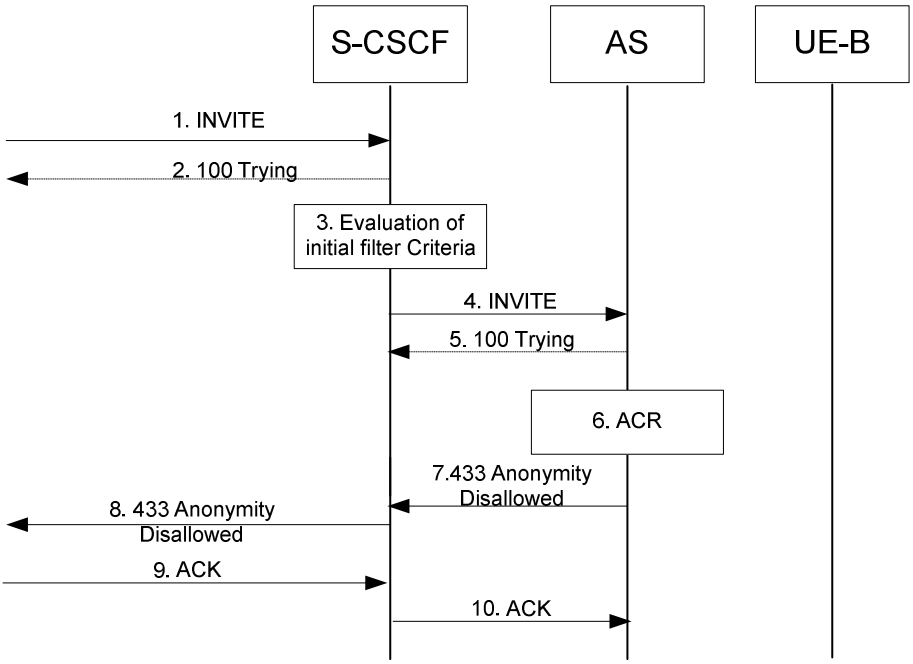

Figure A.1.1: ACR termination towards UE-B

1 to 2. INVITE request (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 request 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 request to the ACR AS.

4 to 5. INVITE request (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.

A.2 Service configuration

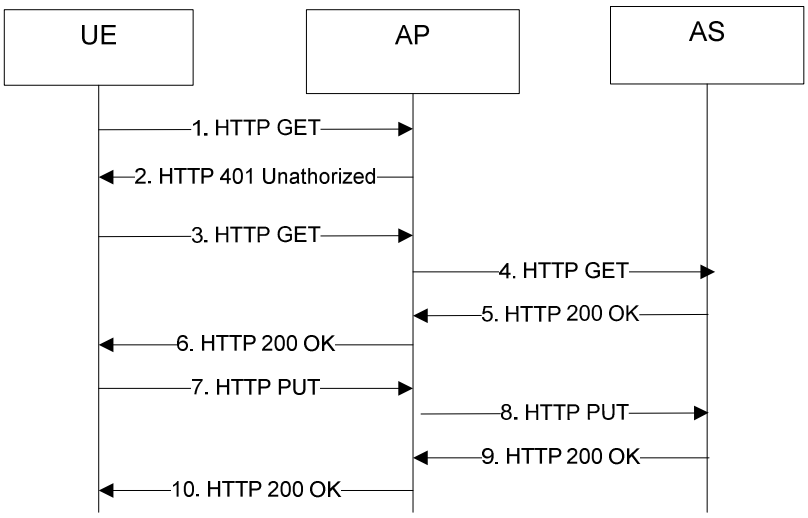

Figure A.2.1: Service configuration example

1. HTTP GET request (UE to AP) - see example in table A.2-1

The UE wants to retrieve the supported conditions for communication barring from the AS.

Table A.2-1: HTTP GET request (UE to AP)

```
GET /simservs.ngn.etsi.org/users/sip:user1@home1.net/simservs.xml/~~/simservs/communication-
   barring-serv-cap HTTP/1.1
Host: xcap.mnc012.mcc345.ipxuni.3gppnetwork.org
Date: Thu, 16 Jun 2011 10:50:33 GMT
X-3GPP-Intended-Identity: "sip:user1@home1.net"
```

2. HTTP 401 (Unathorized) response (AP to UE) - see example in table A.2-2

Upon receiving an unauthorized HTTP GET request the AP authenticates the UE.

Table A.2-2: HTTP 401 (Unathorized) request (AP to UE)

```
HTTP/1.1 401 Unauthorized
Date: Thu, 16 Jun 2011 10:50:34 GMT
WWW-Authenticate: Digest realm="xcap.mnc012.mcc345.ipxuni.3gppnetwork.org",
   nonce="47364c23432d2e131a5fb210812c", qop=auth-int
Content-Length: 0
```

3. HTTP GET request (UE to AP) - see example in table A.2-3

The UE repeats the HTTP GET request including the Authorization header.

Table A.2-3: HTTP GET request (UE to AP)

```
GET /simservs.ngn.etsi.org/users/sip:user1@home1.net/simservs.xml/~~/simservs/communication-
   barring-serv-cap HTTP/1.1
Host: xcap.mnc012.mcc345.ipxuni.3gppnetwork.org
Date: Thu, 16 Jun 2011 10:50:36 GMT
Authorization: Digest realm="xcap.mnc012.mcc345.ipxuni.3gppnetwork.org",
   nonce="47364c23432d2e131a5fb210812c", username="sip:user1@home1.net", qop=auth-int,
   uri="/simservs.ngn.etsi.org/users/sip:user1@home1.net/simservs.xml/~~/simservs/communicatio
   n-barring-serv-cap", response="2c8ee200cec7f6e966c932a9242554e4",
   cnonce="dcd99agsfgfsa8b7102dd2f0e8b1", nc=00000001
X-3GPP-Intended-Identity: "sip:user1@home1.net"
```

4. HTTP GET request (AP to AS) - see example in table A.2-4

The AP forwards the HTTP GET request to the AS.

Table A.2-4: HTTP GET request (AP to AS)

```
GET /simservs.ngn.etsi.org/users/sip:user1@home1.net/simservs.xml/~~/simservs/communication-
   barring-serv-cap HTTP/1.1
Host: xcap.mnc012.mcc345.ipxuni.3gppnetwork.org
Via: HTTP/1.1 ap.home1.net
Date: Thu, 16 Jun 2011 10:50:38 GMT
X-3GPP-Asserted-Identity: "sip:user1@home1.net"
```

5. HTTP 200 (OK) response (AS to AP) - see example in table A.2-5

The AS returns the supported conditions for communication barring. The <serv-cap-media> child element of the <serv-cap-conditions> element describes that audio and video media are allowed to be used as Communication Barring rule conditions. The other child elements of the <serv-cap-conditions> element list the conditions that are not provisioned for the user. If a service capability for a condition is not listed from the list of conditions specified in subclause 4.9.1.4 then the condition is provisioned for the user. The following conditions are provisioned: roaming, international, international-exHC.

Table A.2-5: HTTP 200 (OK) response (AS to AP)

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2011 10:50:40 GMT
Etag: "eti87"
Content-Type: application/xcap-el+xml; charset="utf-8"
Content-Length: (...)

  <communication-barring-serv-cap active="true">
    <serv-cap-conditions>
       <serv-cap-anonymous provisioned="false"></serv-cap-anonymous>
       <serv-cap-communication-diverted provisioned="false"></serv-cap-communication-diverted>
       <serv-cap-external-list provisioned="false"></serv-cap-external-list>
       <serv-cap-identity provisioned="false"></serv-cap-identity>
       <serv-cap-media>
          <media>audio</media>
          <media>video</media>
       </serv-cap-media>
       <serv-cap-other-identity provisioned="false"></serv-cap-other-identity>
       <serv-cap-presence-status provisioned="false"></serv-cap-presence-status>
       <serv-cap-rule-deactivated provisioned="false"></serv-cap-rule-deactivated>
       <serv-cap-validity provisioned="false"></serv-cap-validity>
    </serv-cap-conditions>
</communication-barring-serv-cap>
```

6. HTTP 200 (OK) response (AP to UE) - see example in table A.2-6

The AP routes the HTTP 200 (OK) response to the UE.

Table A.2-6: HTTP 200 (OK) response (AP to UE)

```
HTTP/1.1 200 OK
Via: HTTP/1.1 ap.home1.net
Date: Thu, 16 Jun 2011 10:50:42 GMT
Authentication-Info: nextnonce="e966c32a924255e42c8ee20ce7f6"
Etag: "eti87"
Content-Type: application/simservs+xml; charset="utf-8"
Content-Length: (...)

(...)
```

7. HTTP PUT request (UE to AP) - see example in table A.2-7

The UE creates a new rule to activate the ICB service without conditions. If a rule with id="rule1" previously existed then the new rule replaces that rule. The rule has an empty <conditions> element.

Table A.2-7: HTTP PUT request (UE to AP)

```
PUT /simservs.ngn.etsi.org/users/sip:user1@home1.net/simservs.xml/~~/simservs/incoming-
   communication-barring/ruleset/rule%5b@id=%22rule1%22%5d HTTP/1.1
Host: xcap.mnc012.mcc345.ipxuni.3gppnetwork.org
Date: Thu, 16 Jun 2011 10:52:33 GMT
Authorization: Digest realm="xcap.mnc012.mcc345.ipxuni.3gppnetwork.org",
   nonce="e966c32a924255e42c8ee20ce7f6", username="sip:user1@home1.net", qop=auth-int,
   uri="/simservs.ngn.etsi.org/users/sip:user1@home1.net/simservs.xml/~~/simservs/incoming-
   communication-barring/ruleset", response="adq3283hww88whhjw98822333ddd32",
   cnonce="wqesatt874873j3gg3kk39944hhhee", nc=00000001
X-3GPP-Intended-Identity: sip:user1@home1.net
Content-Type: application/xcap-el+xml; charset="utf-8"
Content-Length: (...)

      <cp:rule id="rule1">
        <cp:conditions>
        </cp:conditions>
        <cp:actions>
          <allow>false</allow>
        </cp:actions>
      </cp:rule>
```

8. HTTP PUT request (AP to AS) - see example in table A.2-8

The AP forwards the HTTP PUT request to the AS.

Table A.2-8: HTTP PUT request (AP to AS)

```
PUT /simservs.ngn.etsi.org/users/sip:user1@home1.net/simservs.xml/~~/simservs/incoming-
   communication-barring/ruleset/rule%5b@id=%22rule1%22%5d HTTP/1.1
Host: xcap.mnc012.mcc345.ipxuni.3gppnetwork.org
Via: HTTP/1.1 ap.home1.net
Date: Thu, 16 Jun 2011 10:52:35 GMT
X-3GPP-Asserted-Identity: sip:user1@home1.net
Content-Type: application/xcap-el+xml; charset="utf-8"
Content-Length: (...)

(...)
```

9. HTTP 200 (OK) response (AS to AP) - see example in table A.2-9

The AS acknowledges the addition of the new ICB rule with a HTTP 200 (OK) response.

Table A.2-9: HTTP 200 (OK) response (AS to AP)

```
HTTP/1.1 200 OK
Date: Thu, 16 Jun 2011 10:52:37 GMT
Etag: "efefefef"
Content-Length: 0
```

10. HTTP 200 (OK) response (AP to UE) - see example in table A.2-10

The AP routes the HTTP 200 (OK) response to the UE.

Table A.2-10: HTTP 200 (OK) response (AS to AP)

```
HTTP/1.1 200 OK
Via: HTTP/1.1 ap.home1.net
Date: Thu, 16 Jun 2011 10:52:38 GMT
Authentication-Info: nextnonce="737jkjssj733hjjk3hjk3999ss3kj"
Etag: "efefefef"
Content-Length: 0
```

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 3GPP TS 29.228 [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 subclause 4.5.2.6.1 "Action for ACR at the terminating AS".

NOTE 3: In practice it is more likely that all INVITE requests 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.

If the AS cannot suppress ICB for for a call identified as a PSAP callback, an IFC bypassing the ICB AS can be used. An example IFC using the PSAP callback indicator specified in IETF RFC 7090 [21] is:

- Method: "INVITE" and not Priority header field with a "psap-callback" header field value.

Annex C (informative): Change history

TISPAN #	TISPAN Doc.	CR	Subject/Comment
11	11TD157	001	"ICB identity rules should be matched against the Referred-By header"
11	11TD157	002	"To avoid the effects between OIP and ACR service"
12	12TD062	003	Correct User Configuration XML Schema errors
12	12TD062	004	Change simservs XCAP namespace
12	12TD062	005	Corrections to ACR call flow
12	12TD062	006	wrong reference
13	SS-060040	007r1	ETSI TS 183 011 (CB) - Incorporation of 3GPP requirements
13	12bTD326r2	008	Communication Barring on roaming
13	12tTD104r1	009	Rule conditions correction
14bis	14bTD413r4	010	CR to TS 183 011
14ter	14tTD416r1	011	Correction of XML
15bis	15bTD336r3	012	Correction of XML Schema and misalignment
15bis	15bTD441r1	013	Correction of the use of the terms Interaction and Interworking in the ACR-CB Simulation Service description
15bis	15b350	014	Add interaction between ACR&CB and CONF (Corresponding CR 15bTD352)

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
2008-01					Technically identical copy as **3GPP TS 24.611** as basis for further development.		1.3.2
2008-02					Implemented C1-080102		1.4.0
2008-04					Implemented C1-081237, C1-080875, C1-080888, C1-080889, C1-081092, C1-081093, C1-081182		1.5.0
2008-05					Implemented C1-81832, C1-81914 Editorial: Cover page change to Release 8, correction of Key words Incorporation of comments from ETSI Edit help		1.6.0
2008-05					Editorial changes done by MCC	1.6.0	1.6.1
2008-06	CT#40	CP-080331			CP-080331 was approved by CP-080331 and version 8.0.0 is created by MCC for publishing	1.6.1	8.0.0
2008-06					Verson 8.0.1 created to include attachments (.xml and .xsd files)	8.0.0	8.0.1
2008-09	CT#41	CP-080539	0001	1	Allow SIP based user configuration mechanism for configuring supplementary services	8.0.1	8.1.0
2008-09	CT#41	CP-080533	0002		Applicability statement in scope	8.0.1	8.1.0
2008-09	CT#41	CP-080533	0003		Identification of AS procedures	8.0.1	8.1.0
2008-12	CT#42	CP-080865	0004	1	Clarification of B2BUA and proxy roles for AS	8.1.0	8.2.0
2008-12	CT#42	CP-080864	0005	2	Interaction between SIP and Ut based service configuration	8.1.0	8.2.0
2008-12	CT#42				Editorial cleanup by MCC	8.1.0	8.2.0
2009-06	CT#44	CP-090432	0009	2	Service capability indication for CB	8.2.0	9.0.0
2009-06	CT#44	CP-090432	0010	2	Addition of international-communications to barring conditions	8.2.0	9.0.0
2009-09	CT#45	CP-090687	0012		Media capabilities for Call Barring	9.0.0	9.1.0
2009-09	CT#45	CP-090682	0014	4	Dynamic barring of users for ICB	9.0.0	9.1.0
2009-09	CT#45	CP-090687	0016	1	Example doc for CB	9.0.0	9.1.0
2009-12	CT#46	CP-090928	0017	2	CB serv-cap corrections	9.1.0	9.2.0
2009-12	CT#46	CP-090928	0018	1	Corrections to EXAMPLE	9.1.0	9.2.0
2010-03	CT#47	CP-100141	0019		Cleanup EN	9.2.0	9.3.0
2011-03	CT#51				Upgrade to Rel-10	9.3.0	10.0.0
2011-09	CT#53	CP-110657	0021	2	<conditions> element values	10.0.0	10.1.0
2011-09	CT#53	CP-110695	0022	1	Service configuration signalling flow	10.1.0	11.0.0
2011-12	CT#54	CP-110857	0027	2	Use of "Critical"	11.0.0	11.1.0
2012-09	CT#57	CP-120583	0031		Incorrect reference to OMA Common Policy Schema	11.1.0	11.2.0
2013-06	CT#60	CP-130415	0032	5	PSAP callback ICB suppression	11.2.0	12.0.0
2013-06	CT#60	CP-130265	0033	3	Barring of incoming OPTIONS requests	11.2.0	12.0.0
2013-09	CT#61	CP-130507	0035		draft-ietf-ecrit-psap-callback reference update	12.0.0	12.1.0
2013-12	CT#62	CP-130758	0036	2	Reference update: draft-ietf-ecrit-psap-callback	12.1.0	12.2.0
2014-03	CT#63	CP-140143	0037	1	Correction of history related header field name	12.2.0	12.3.0
2014-12	CT#66	CP-140833	0040	1	Reference update: RFC 7090 (draft-ietf-ecrit-psap-callback)	12.3.0	12.4.0
2014-12	CT#66	CP-140826	0042		Reference Update: RFC7315	12.3.0	12.4.0
2014-12	CT#66	CP-140837	0043	1	simservs filename correction	12.3.0	12.4.0
2015-06	CT#68	CP-150328	0046	2	White lists and barring	12.4.0	13.0.0
2015-12	CT#70	CP-150709	0047	1	Service capability unconditional for barring	13.0.0	13.1.0

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-03	CT#75	CP-170131	0048	6	B	Password handling for communication barring	14.0.0
2017-03	CT#75	CP-170131	0049	4	B	Password option for barring service	14.0.0

History

Document history		
V14.0.0	April 2017	Publication