ETSI TS 124 611 V17.0.0 (2022-05)

TECHNICAL SPECIFICATION

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 17.0.0 Release 17)

Reference
RTS/TSGC-0124611vh00

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 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

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".

[24] 3GPP TS 24.196: "Technical Specification Group Core Network and Terminals; Enhanced Calling Name".

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
MiD Multi-iDentity
MuD Multi-Device
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 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 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 clause 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 clause 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 clause 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 clause 4.5.0.

4.5.1A Registration/erasure

For registration of information for the services ICB, OCB and ACR, the mechanisms specified in clause 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 clause 4.5.0.

For erasure of information for the services ICB, OCB and ACR, the mechanisms specified in clause 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 clause 4.5.0.

4.5.1B Interrogation

For interrogation of the services ICB, OCB and ACR, the mechanisms specified in clause 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 clause 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 clause 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 clause 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 clause 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 an allow list, as described in clause 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].