3GPP TS 24.407 V8.2.0 (2009-12)

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;
Originating Identification Presentation (OIP)
and Originating Identification Restriction (OIR);
Protocol specification
(Release 8)**

**GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS**

Keywords
CLIP, CLIR, 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

3GPP

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 183 007 [14]. 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 Originating Identification Presentation (OIP) simulation service and the Originating Identification Restriction (OIR) simulation services, based on stage one and two of the ISDN CLIP [4] and CLIR [5] supplementary service. Within the TISPAN NGN Release 1 the stage 3 description is specified using the IP-Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).

NOTE: It should be noted that the behaviour described in this the present document does not take into account other behaviours that may be specified in other applications and care needs to be taken when designing the filters etc. when two or more applications are involved in a session.

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 ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

[2] ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture".

[3] ETSI ES 283 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Endorsement of "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 (Release 6)" for NGN Release 1".

[4] ETSI EN 300 089: "Integrated Services Digital Network (ISDN); Calling Line Identification Presentation (CLIP) supplementary service; Service description".

[5] ETSI EN 300 090: "Integrated Services Digital Network (ISDN); Calling Line Identification Restriction (CLIR) supplementary service; Service description".

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

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

[8] IETF RFC 2396: "Uniform Resource Identifiers (URI): Generic Syntax".

[9] IETF RFC 3966: "The tel URI for Telephone Numbers".

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

[11] ETSI ES 283 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Interworking SIP-ISUP for TISPAN-IMS".

[12] ITU-T Recommendation I.210: "Principles of telecommunication services supported by an ISDN and the means to describe them".

[13] ETSI TS 183 023: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; PSTN/ISDN simulation services; Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating NGN PSTN/ISDN Simulation Services".\

[14] ETSI TS 183 007 V1.3.0: "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"

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Breakout Gateway Control Function (BGCF): See ES 282 007 [1].

Call Session Control Function (CSCF): See ES 282 007 [1].

dialog: See RFC 3261 [10].

header: See RFC 3261 [10].

header field: See RFC 3261 [10].

identity information: all the information identifying a user, including trusted (network generated) and/or untrusted (user generated) addresses

NOTE: Identity information should take the form of either a SIP URI (see RFC 2396 [8]) or a "tel" URI (see RFC 3966 [9])

incoming initial request: all requests intended to initiate either a dialog or a standalone transaction terminated by the served user

Interconnection Border Control Function (IBCF): See ES 282 003 [2].

Interrogating-CSCF (I-CSCF): See ES 282 003 [2].

Media Gateway Control Function (MGCF): See ES 282 007 [1].

Multimedia Resource Function Controller (MRFC): See ES 282 007 [1].

Multimedia Resource Function Processor (MRFP): See ES 282 007 [1].

originating UE: sender of a SIP request intended to initiate either a dialog (e.g. INVITE, SUBSCRIBE), or a standalone transaction

> EXAMPLE: OPTIONS, MESSAGE.

outgoing (communication): communication outgoing from the user side of the interface

outgoing initial request: all requests intended to initiate either a dialog or a standalone transaction received from the served user

proxy: See RFC 3261 [10].

Proxy-CSCF (P-CSCF): See ES 282 003 [2].

public user identity: See ES 282 003 [2].

request: See RFC 3261 [10].

response: See RFC 3261 [10].

Serving-CSCF (S-CSCF): See ES 282 003 [2].

session: See RFC 3261 [10].

standalone transaction: SIP transaction that is not part of a dialog and does not initiate a dialog

> NOTE: An OPTIONS or a MESSAGE request sent outside of a SIP dialog would be considered to be part of a standalone transaction.

Subscription Locator Function (SLF): See ES 282 007 [1].

supplementary service: See ITU-T Recommendation I.210 [12], clause 2.4.

tag: See RFC 3261 [10].

terminating UE: recipient of a SIP request intended either to initiate a dialog or to initiate either a dialog or a standalone transaction

trusted identity information: network generated user public identity information

(SIP) transaction: See RFC 3261 [10].

3.2 Abbreviations

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

AS	Application Server
BGCF	Breakout Gateway Control Function
CCBS	Completion of Communication to Busy Subscriber
CDIV	Communication DIVersion
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CSCF	Call Session Control Function
CW	Communication Waiting
HOLD	communication Hold
IBCF	Interconnection Border Control Function
ICB	Incoming Communication Barring
I-CSCF	Interrogating-CSCF
IFC	Initial Filter Criteria
IM	IP Multimedia
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Service Data Network
MCID	Malicious Communication IDentification
MGCF	Media Gateway Control Function

MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
NGN	Next Generation Network
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
P-CSCF	Proxy-CSCF
PSTN	Public Switched Telephone Network
S-CSCF	Serving-CSCF
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
UE	User Equipment
URI	Universal Resource Identifier

4 Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR)

4.1 Introduction

The Originating Identification Presentation (OIP) service provides the terminating user with the possibility of receiving identity information in order to identify the originating user.

The Originating Identification Restriction (OIR) service enables the originating user to prevent presentation of its identity information to the terminating user.

4.2 Description

4.2.1 General description

The OIP service provides the terminating user with the possibility of receiving trusted (i.e. network-provided) identity information in order to identify the originating user.

In addition to the trusted identity information, the identity information from the originating user can include identity information generated by the originating user and in general transparently transported by the network. In the particular case where the "no screening" special arrangement does not apply, the originating network shall verify the content of this user generated identity information. The terminating network cannot be responsible for the content of this user generated identity information.

The OIR service is a service offered to the originating user. It restricts presentation of the originating user's identity information to the terminating user.

When the OIR service is applicable and activated, the originating network provides the destination network with the indication that the originating user's identity information is not allowed to be presented to the terminating user. In this case, no originating user's identity information shall be included in the requests sent to the terminating user. The presentation restriction function shall not influence the forwarding of the originating user's identity information within the network as part of the simulation service procedures.

4.3 Operational requirements

4.3.1 Provision/withdrawal

4.3.1.1 OIP Provision/withdrawal

The OIP service may be provided after prior arrangement with the service provider or be generally available.

The OIP service shall be withdrawn at the subscriber's request or for administrative reasons.

As a general operator policy a special arrangement may exist on a per subscriber basis or on a general behaviour basis whereby the originating user's identity information intended to be transparently transported by the network is not screened by the network.

4.3.1.2 OIR Provision/withdrawal

The OIR service, temporary mode, may be provided on a subscription basis or may be generally available.

The OIR service, permanent mode, shall be provided on a subscription basis.

As a network option, the OIR service can be offered with several subscription options. A network providing the OIR service shall support temporary mode at a minimum. Subscription options are summarized in table 1.

Table 1: OIR Subscription options

Subscription option values	Values
Mode	- permanent mode (active for all requests) - temporary mode (specified by the UE per the initial outgoing request)
Temporary mode default	- presentation restricted - presentation not restricted
Restriction	- restrict the asserted identity - restrict all private information appearing in headers

4.3.2 Requirements on the originating network side

As part of the basic communication procedures specified in ES 283 003 [3], the following requirements apply at the originating network side in support of the OIP service and the OIR service. Unless noted otherwise, these requirements are meant to apply to all requests meant to initiate either a dialog or a standalone transaction. These procedures apply regardless of whether the originating or terminating parties subscribe to the OIP service or the OIR service:

- The originating UE may insert two forms of identity information that correspond to the following two purposes:

    - As a suggestion to the network as to what public user identity the network should be included in the request as network asserted identity information.

    - As a UE-provided identity to be transparently transported by the network.

- In the case where no identity information is provided by the originating UE for the purpose of suggesting a network-provided identity, the network shall include identity information based on the default public user identity associated with the originating UE.

- In the case where identity information is provided by the originating UE for the purpose of suggesting a network-provided identity, the network shall attempt to match the information provided with the set of registered public identities of the originating UE. If a match is found, the network shall include an identity based on the information provided by the originating UE.

As a network option, if the "no screening" special arrangement does not exist with the originating UE, the network may attempt to match the UE-provided identity information with the set of registered public identities of the originating user. If a match is not found, the network shall replace the UE-provided identity with one that includes the default public user identity.

For OIR subscribers:

- The UE may include an indication that it wishes to have the presentation of its identity information to be restricted.

- If the originating user has subscribed to the OIR service in the permanent mode, then the network shall automatically invoke the OIR service for each outgoing request.

- If the originating user has subscribed to the OIR service in the temporary mode with default value "presentation restricted", then the network shall automatically invoke the OIR service for each outgoing request unless the default value is overridden by subscriber request at the time of outgoing request.

- If the originating user has subscribed to the OIR service in the temporary mode with default value "presentation not restricted", then the network shall only invoke the OIR service if requested by the subscriber at the time of outgoing initial request.

- If the OIR service is not invoked, the network-provided identity shall be considered to be presentation allowed.

As an originating network option, if the originating user invokes the OIR service for a particular request, the originating network may prevent any UE-provided identification information (in addition to the trusted identity information) from being displayed to the terminating user.

4.3.3   Requirements on the terminating network side

For terminating users that subscribe to the OIP service, and if network provided identity information about the originator is available, and if presentation is allowed, the network shall include that information in the requests sent to the UE.

If the presentation of the public user identity is restricted, then the terminating UE shall receive an indication that the public user identity was not sent because of restriction.

If the public user identity is not available at the terminating network (for reasons such as interworking), then the network shall indicate to the terminating user that the public user identity was not included for reasons other than that the originating user invoked the OIR service.

For terminating users that do not subscribe to the OIP service, the network shall not send the network provided identity information about the originator in the requests sent to the UE, even if that information is available, and if presentation is allowed. Additionally, the network may prevent the transmission of any UE-provided identity information.

4.4   Syntax requirements

The syntax for the relevant header fields in the SIP requests are normatively described in ES 283 003 [3]. The relevant headers are:

- The P-Preferred-Identity header field, which shall conform to the specifications in RFC 3325 [7] and RFC 3966 [9].

- The P-Asserted-Identity header field, which shall conform to the specifications in RFC 3325 [7] and RFC 3966 [9].

- The Privacy header field, which shall conform to the specifications in RFC 3323 [6] and RFC 3325 [7].

- The From header field, which shall conform to the specifications in RFC 3261 [10] and RFC 3966 [9].

4.5   Signalling procedures

4.5.0   General

For user configuration of the OIR service the Ut interface should be used.

See clause 4.10 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 this specification.

4.5.1 Activation/deactivation and registration

The OIP service is activated at provisioning and deactivated at withdrawal.

The OIR service is activated at provisioning and deactivated at withdrawal.

4.5.1A Registration/erasure

The OIP service requires no registration. Erasure is not applicable.

The OIR service requires no registration. Erasure is not applicable.

4.5.1B Interrogation

For OIP, interrogation is not applicable.

For interrogation of OIR, the Ut interface should be used.

4.5.2 Invocation and operation

4.5.2.1 Actions at the originating UE

As part of basic communication, the originating UE may insert a P-Preferred-Identity header field in any initial SIP request for a dialog or in any SIP request for a standalone transaction as a hint for creation of a public user identity as described in ES 283 003 [3].

NOTE 1: According ES 283 003 [3], the UE may include any of the following in the P-Preferred-Identity header field:

- a public user identity which has been registered by the user;

- a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implicit registration that was not subsequently deregistered or has expired; or

- any other public user identity which the user has assumed by mechanisms outside the scope of ES 283 003 [3] to have a current registration.

If the originating user wishes to override the default setting of "presentation not restricted" of the OIR service in temporary mode:

- The originating UE shall include an "anonymous" From header field. The convention for configuring an anonymous From header field described in RFC 3323 [6] and RFC 3325 [7] should be followed; i.e. From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag= xxxxxxx.

- If only the P-Asserted-Identity needs to be restricted the originating UE shall include a Privacy header field set to "id" in accordance with RFC 3323 [6], and RFC 3325 [7].

- If all headers containing private information need to be restricted the originating UE shall include a Privacy header field set to "header" in accordance with RFC 3323 [6], and RFC 3325 [7].

NOTE 2: It is assumed that all TISPAN NGN UEs will support ES 283 003 [3] or RFC 3325 [7].

If the originating user wishes to override the default setting of "presentation restricted" of the OIR service in temporary mode:

- The originating UE shall include a Privacy header field of privacy type "none" in accordance with ES 283 003 [3] (RFC 3323 [6]).

4.5.2.2 Actions at the originating P-CSCF

Procedures according to ES 283 003 [3] shall apply.

NOTE 1: As an informative description, for OIP/OIR this means the following procedures should be provided by the P-CSCF regardless of whether the originating user does or does not subscribe to the OIP service or OIR service.

NOTE 2: When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header field that matches one of the registered public user identities, the P-CSCF should identify the initiator of the request by that public user identity. In particular, the P-CSCF should include a P-Asserted-Identity header field set to that public user identity.

NOTE 3: When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains as P-Preferred-Identity header field that does not match one of the registered public user identities, or does not contain a P-Preferred-Identity header field, the P-CSCF should identify the initiator of the request by a default public user identity. In particular, the P-CSCF should include a P-Asserted-Identity header field set to the default public user identity. If there is more then one default public user identity available, the P-CSCF should randomly select one of them.

4.5.2.3 Actions at the S-CSCF serving the originating UE

These procedures shall apply, whether or not the user subscribes to the OIR service, to requests originated by the served UE:

- In the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URI contained in the P-Asserted-Identity header field received in the request, the S-CSCF shall add a second P-Asserted-Identity header field containing this tel-URI.

NOTE: For the S-CSCF to forward an initial request towards the AS that hosts the OIR service, an initial filter criterion is to be setup for the user who is subscribed to the service. Annex B provides an example of an initial filter criterion that that can be applied for the OIR service.

4.5.2.4 Actions at the AS serving the originating UE

For an originating user that subscribes to the OIR service in "permanent mode", the AS shall insert a Privacy header field set to "id" or "header" based on the subscription option if the request does not include a Privacy header field that is set to the corresponding value. If the request includes a Privacy header field that is set to "none", the AS shall remove the "none" value from the Privacy header field. Additionally, based on operator policy, the AS shall either modify the From header field to remove the identification information, or add a Privacy header field set to "user".

For an originating user that subscribes to the OIR service in "temporary mode" with default "restricted", if the request does not include a Privacy header field, or the request includes a Privacy header field that is not set to "none", the AS shall insert a Privacy header field set to "id" or "header" based on the subscription option. Additionally, based on operator policy, the AS shall either modify the From header field to remove the identification information, or add a Privacy header field set to "user".

NOTE: When the OIR service is used, the originating UE is supposed to already have removed identity information. However because this UE is not trusted, this is also done by the AS to ensure that this information is removed.

For an originating user that subscribes to the OIR service in "temporary mode" with default "not restricted", if the request includes a Privacy header field is set to "id" or "header", based on operator policy, the AS shall either modify the From header field to remove the identification information, or add a Privacy header field set to "user". As an originating network option, if the "no screening" special arrangement does not exist with the originating user, the network may attempt to match the information in the From header with the set of registered public identities of the originating user. If a match is not found, the AS may set the From header to the SIP URI that includes the default public user identity.

4.5.2.5 Actions at the outgoing I-CSCF (THIG)

Procedures according to ES 283 003 [3] shall apply.

4.5.2.6 Actions at the incoming I-CSCF

Procedures according to ES 283 003 [3] shall apply.

4.5.2.7 Actions at the outgoing IBCF

Procedures according to ES 283 003 [3] shall apply.

NOTE: It is assumed that the IBCF is responsible for stripping the P-Asserted-Identity from the SIP header when interworking with untrusted networks.

4.5.2.8 Actions at the incoming IBCF

Procedures according to ES 283 003 [3] shall apply.

NOTE: It is assumed that the IBCF is responsible for stripping the P-Asserted-Identity from the SIP header when interworking with untrusted networks.

4.5.2.9 Actions at the AS serving the terminating UE

If a terminating user does not subscribe to OIP service, an AS shall remove any P-Asserted-Identity or Privacy header fields included in the request. Additionally, the Application Server may as a network option anonymize the contents of the From header by setting it to a default non significant value. As a network option, if the terminating user has an override category, the AS shall send the P-Asserted-Identity headers and remove the Privacy header fields.

When the Privacy header field is set to "id", with the exception of the cases listed above, the AS should not remove this Privacy header entry.

NOTE: The priv-value "id" in the Privacy header will be used by the terminating UE to distinguish the request of OIR by the originating user.

If the request includes the Privacy header field set to "header" the AS shall anonymize the contents of all headers containing private information in accordance with RFC 3323 [6] and RFC 3325 [7].

If the request includes the Privacy header field set to "user" the AS shall remove or anonymize the contents of all "user configurable" headers in accordance with RFC 3323 [6] and RFC 3325 [7]. In the latter case, the AS may need to act as transparent back-to-back user agent as described in RFC 3323 [6].

4.5.2.10 Actions at the S-CSCF serving the terminating UE

The CSCF shall apply any privacy required by RFC 3325 [7] to the P-Asserted-Identity. In particular, if the Privacy header field is included and set to "id", the S-CSCF shall remove any P-Asserted-Identity header fields from the request.

NOTE 1: For the S-CSCF to forward an initial request or standalone request, an initial filter criterion is to be setup for the user who is subscribed to the service. Annex B provides an example of an initial filter criterion that that can be applied for the OIP service.

NOTE 1a: The priv-value "id" in the Privacy header should not be removed when removing any P-Asserted-Identity header as described in ES 283 003 [3] clause 5.4.3.3.

If the request contains the Privacy header field "header" and/or "user" the S-CSCF shall forward the request to the AS.

NOTE 2: When removing the P-Asserted-identity any following service in the chain could be affected. Therefore service based on the originating identity (such as ICB and ACR), should precede the OIP service in the chain.

4.5.2.11 Actions at the destination P-CSCF

The basic communication procedures according to ES 283 003 [3] shall apply.

4.5.2.12 Actions at the terminating UE

A terminating UE shall support the receipt of one or more P-Asserted-Identity header fields in SIP requests initiating a dialog or standalone transactions, each one containing a public user identity of the originating user. The UE may present the information to the user.

> NOTE 1: If no P-Asserted-Identity header fields are present, but a Privacy header field was present, then the one or more identities may have been withheld due to presentation restriction.

> NOTE 2: If neither P-Asserted-Identity header fields nor a Privacy header field are present, then the network-provided identities may not have been available (due to, for example, interworking with other networks), or the user may not hold a subscription to the OIP service.

> NOTE 3: A user-provided identity may also be available, within the From header field of the request. The TISPAN NGN network can not take any responsibility for the content of the From header field.

4.6 Interaction with other simulation services

4.6.1 Communication Hold (HOLD)

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

4.6.2 Terminating Identity Presentation (TIP)

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

4.6.3 Terminating Identity Restriction (TIR)

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

4.6.4 Originating Identity Presentation (OIP)

The OIR service shall normally take precedence over the OIP service.

The OIP service can take precedence over the OIR service when the destination subscriber has an override category. This is a national matter, and is outside the scope of the present document.

4.6.5 Originating Identity Restriction (OIR)

The OIR service shall normally take precedence over the OIP service.

The OIP service can take precedence over the OIR service when the destination user has an override category. This is a national matter, and is outside the scope of the present document.

4.6.6 Conference calling (CONF)

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

4.6.7 Communication diversion services (CDIV)

When a request has been diverted and the diverted-to user has been provided with the OIP service, the diverted-to UE shall receive the identity information of the original originating user. When the OIR service has been invoked, the originating user's identity information shall not be presented to the diverted-to user unless the diverted-to user has an override category.

4.6.8 Malicious Communication IDentification (MCID)

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

NOTE: When the MCID service is invoked, the identity of an incoming communication is registered in the network whether or not the originating user has activated the OIR service.

4.6.9 Incoming Communication Barring (ICB)

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

4.6.10 Explicit Communication Transfer (ECT)

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

4.7 Interactions with other networks

4.7.1 Interaction with PSTN/ISDN networks

The interworking described in ES 283 027 [11], clause 7.4.1 shall apply.

NOTE: The mapping of parameters for the regarding supplementary service is the same as for the OIP/OIR simulation service.

4.7.2 Interworking with PSTN/ISDN emulation

When interworking with the PSTN/ISDN domain, the following header fields, shall be passed without changes:

- the P-Asserted-Identity header field; and
- the Privacy header field.

NOTE: The SIP header fields are transcoded by the MGCF from and to an ISUP MIME body.

If the network is not trusted the P-Asserted-Identity shall be removed from SIP requests and SIP responses.

4.7.3 Interaction with other IP networks

If the other IP based network is a trusted network and the RFC 3323 [6] and RFC 3325 [7] are supported the following header fields shall be forwarded without changes:

- the P-Asserted-Identity header field; and
- the Privacy header field.

If the other IP network is not trusted the P-Asserted-Identity header fields shall be removed from SIP requests and SIP responses.

4.8 Signalling flows

No OIP or OIR service specific signalling flow is necessary in addition to the basic communication control according to ES 283 003 [3].

4.9 Parameter values (timers)

No specific timers are required.

4.10   Service configuration

Originating Identity documents are sub-trees of the *simservs* XML document specified in TS 183 023 [13]. As such, Originating Identity documents use the XCAP application usage in TS 183 023 [13].

Data semantics: The semantics of the Originating Identity XML configuration document is specified in clause 4.10.1.

XML schema: Implementations in compliance with the present document shall implement the XML schema that minimally includes the XML Schema defined in clause 4.10.2 and the *simservs* XML schema specified in clause 6.3 of TS 183 023 [13].

An instance of an Originating Identity document is shown:

```
<?xml version="1.0" encoding="UTF-8"?>
<simservs xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
xmlns:xsi="http://www.w3.org/2001/XMLSchema--instance" >

    <originating-identity-presentation active="true"/>

    <originating-identity-presentation-restriction active="true">
        <default-behaviour>presentation-restricted</default-behaviour>
    </originating-identity-presentation-restriction>

</simservs>
```

4.10.1   Data semantics

The OIP service can be activated/deactivated using the active attribute of the <originating-identity-presentation> service element.

The OIR service can be activated/deactivated using the active attribute of the <originating-identity-presentation-restriction> service element. Activating the OIR service this way activates the temporary mode OIR service. When deactivated and not overruled by operator settings, basic communication procedures apply.

The behaviour of the temporary mode OIR is configured with the optional <default-behaviour> element. There are two values that this element can take:

- **Presentation-restricted**: This configures the service to behave as specified in clause 4.5.2.4 for the case OIR service in "temporary mode" with default "restricted".

- **Presentation-not-restricted**: This configures the service to behave as specified in clause 4.5.2.4 for the case OIR service in "temporary mode" with default "not restricted".

4.10.2 XML schema

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:ss="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://uri.etsi.org/ngn/params/xml/simservs/xcap" elementFormDefault="qualified"
attributeFormDefault="unqualified">
   <xs:element name="originating-identity-presentation-restriction"
substitutionGroup="ss:absService">
      <xs:annotation>
         <xs:documentation>Originating Identity presentation Restriction
          </xs:documentation>
      </xs:annotation>
      <xs:complexType>
         <xs:complexContent>
            <xs:extension base="ss:simservType">
               <xs:sequence>
                  <xs:element name="default-behaviour" default="presentation-restricted"
                   minOccurs="0">
                     <xs:simpleType>
                        <xs:restriction base="xs:string">
                           <xs:enumeration value="presentation-restricted"/>
                           <xs:enumeration value="presentation-not-restricted"/>
                        </xs:restriction>
                     </xs:simpleType>
                  </xs:element>
               </xs:sequence>
            </xs:extension>
         </xs:complexContent>
      </xs:complexType>
   </xs:element>
   <xs:element name="originating-identity-presentation" type="ss:simservType"
   substitutionGroup="ss:absService">
      <xs:annotation>
         <xs:documentation>Originating Identity Presentation
          </xs:documentation>
      </xs:annotation>
   </xs:element>
</xs:schema>
```

Annex A (informative):
Signalling flows

The signalling flow for the OIR service and the OIP service is the same as the signalling flow for basic communication described in ES 283 003 [3].

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 (IFC) evaluation.

B.1 Originating filter criteria for OIR service

All outgoing SIP requests are forwarded to an Application Server providing the OIR service under the following conditions:

- the user is subscribed to the OIR service in permanent mode; or

- the request does not include a Privacy header field.

B.2 Terminating filter criteria for OIP service

All incoming SIP requests are forwarded to an Application Server providing the OIP service under the following conditions:

- The terminating user does not subscribe to the OIP service and the AS acts according to clause 4.5.2.9.

Annex C (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2006-03					Publication as **ETSI TS 183 007**		1.1.1
2007-03					Publication as ETSI TS 183 007		1.2.1
2008-01					Publication as ETSI TS 183 007		1.3.0
2008-01					Conversion to **3GPP TS 24.407**		1.3.1
2008-03	CT#39	CP-080079			Version 1.2.2 approved in CP#39 and version 7.0.0 created by MCC	1.3.1	7.0.0
2008-03					Based on the decision in CT#39 version 8.0.0 was created by MCC	7.0.0	8.0.0
2009-06	CT#44	CP-090407	0001	1	Invalid XML schema bug fix	8.0.0	8.1.0
2009-12	CT#46	CP-090905	0004		Action on the originating network to apply privacy	8.1.0	8.2.0