ETSI TS 124 607 V14.0.0 (2017-05)

**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Originating Identification Presentation (OIP)
and Originating Identification Restriction (OIR)
using IP Multimedia (IM) Core Network (CN) subsystem;
Protocol specification
(3GPP TS 24.607 version 14.0.0 Release 14)**

Reference
RTS/TSGC-0124607ve00

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

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) supplementary service and the Originating Identification Restriction (OIR) supplementary services, based on stage one and two of the ISDN CLIP [4] and CLIR [5] supplementary service. 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).

NOTE: It can be noted that the behaviour described in this the present document does not take into account other behaviours that is 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*.

[1] 3GPP TS 23.002: "Network architecture".

[2] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".

[3] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP".

[4] ETSI EN 300 089 V3.1.1: "Integrated Services Digital Network (ISDN); Calling Line Identification Presentation (CLIP) supplementary service; Service description".

[5] ETSI EN 300 090 V1.2.1: "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] Void

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

[13] 3GPP TS 24.623: "Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary 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"

[15] 3GPP TS 24.238: "Session Initiation Protocol (SIP) based user configuration; stage 3"

[16] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

[17] 3GPP TS 24.417: "Management Object (MO) for Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) using IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

3 Definitions and abbreviations

3.1 Definitions

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

Call Session Control Function (CSCF): See 3GPP TS 23.002 [1].

dialog: See IETF RFC 3261 [10].

header: See IETF RFC 3261 [10].

header field: See IETF RFC 3261 [10].

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

NOTE: Identity information takes the form of either a SIP URI (see IETF RFC 2396 [8]) or a "tel" URI (see IETF 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 3GPP TS 23.228 [2].

Media Gateway Control Function (MGCF): See 3GPP TS 23.002 [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

private information: information that according to IETF RFC 3323 [6] and IETF RFC 3325 [7] is not permitted to be delivered to the remote end.

proxy: See IETF RFC 3261 [10].

Proxy-CSCF (P-CSCF): See 3GPP TS 23.228 [2].

public user identity: See 3GPP TS 23.228 [2].

request: See IETF RFC 3261 [10].

response: See IETF RFC 3261 [10].

Serving-CSCF (S-CSCF): See 3GPP TS 23.228 [2].

session: See IETF 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.

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

tag: See IETF 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 IETF RFC 3261 [10].

3.2 Abbreviations

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

AS	Application Server
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
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
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
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 supplementary 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 (allows the UE to override the default behaviour on per call basis)
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 3GPP TS 24.229 [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:

1 The originating UE can 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.

2 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.

3 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.

The UE can include an indication that it wishes to have the presentation of its identity information to be restricted. The following cases exist:

- If the originating user has subscribed to the OIR service in the permanent mode, then the network shall 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 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 originating user has not subscribed to the OIR service but the originating UE sends a SIP request initiating a dialog or standalone transaction with Privacy header fields indicating a privacy request or a digit sequence within the Request-URI that comprise the effective dial string for restricting the presentation of identity information then, the SIP request may be rejected by operator policy.

NOTE 1AA: Only when supporting the MMTEL for the OIP/OIR Service such a procedure is possible. This requires an initial filter criterion to be setup for the user who is not subscribed to the OIR service.

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

NOTE 1A: For the network to invoke the service, the S-CSCF will forward an initial request towards the AS that hosts the OIR service. This requires an initial filter criterion to be setup for the user who is subscribed to the service. Annex B provides an example of an initial filter criterion that can be applied for the OIR service.

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.

NOTE 1: As an informative description, for OIP/OIR this means the following procedures are expected to be provided by the P-CSCF regardless of whether the originating user does or does not subscribe to the OIP service or OIR service. 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 is expected to identify the initiator of the request by that public user identity. In particular, the P-CSCF is expected to include a P-Asserted-Identity header field set to that public user identity. 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 is expected to identify the initiator of the request by a default public user identity. In particular, the P-CSCF is expected to 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 is expected to randomly select one of them.

NOTE 2: 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 adds a second P-Asserted-Identity header field containing this tel-URI.

NOTE 3: 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.

NOTE 4: It is assumed that the IBCF is responsible for stripping the P-Asserted-Identity from the SIP header when interworking with untrusted networks.

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.

NOTE 1: The priv-value "id" in the Privacy header is not expected be removed when removing any P-Asserted-Identity header as described in 3GPP TS 24.229 [3] subclauses 4.4.2 and 5.4.3.3.

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), are expected to precede the OIP service in the chain.

NOTE 3: It is assumed that the IBCF is responsible for stripping the P-Asserted-Identity from the SIP header when interworking with untrusted networks.

4.4 Syntax requirements

The syntax for the relevant header fields in the SIP requests are normatively described in 3GPP TS 24.229 [3]. The relevant headers are:

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

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

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

NOTE: The privacy level "session" and "critical" are not used in this specification.

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

4.5 Signalling procedures

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 [13]; or
- use SIP based user configuration as described in 3GPP TS 24.238 [15];

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.

The enhancements to the XML schema for use over the Ut interface are described in subclause 4.10.

4.5.1 Activation/deactivation

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 interrogation of OIP and OIR, the mechanisms specified in subclause 4.5.0 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 3GPP TS 24.229 [3].

NOTE 1: According 3GPP TS 24.229 [3], the UE can 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 3GPP TS 24.229 [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 IETF RFC 3323 [6] 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 [6] set to "id" in accordance with IETF RFC 3325 [7].

- If all headers containing private information that the UE cannot anonymize itself need to be restricted, the originating UE shall include a Privacy header field set to "header" in accordance with IETF RFC 3323 [6].

NOTE 2: The Privacy header field value "header" does not apply to the identity in the From header field.

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 3GPP TS 24.229 [3] (IETF RFC 3323 [6]).

4.5.2.2 Void

4.5.2.3 Void

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:

1) insert a Privacy header field set to:

   a) "id" if only the P-Asserted-Identity header field needs to be restricted as described in RFC 3325 [7]; or

   b) "header" if all the header fields, containing private information that the UE cannot anonymize need to be restricted as described in RFC 3323 [6]. This choice is based on the subscription option.

NOTE 1: The Privacy header field value "header" does not apply to the identity in the From header field.

2) If the request includes a Privacy header field that is set to "none", remove the "none" value from the Privacy header field; and

3) based on operator policy, 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 "presentation-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:

1) insert a Privacy header field set to:

   a) "id" if only the P-Asserted-Identity header field needs to be restricted as described in RFC 3325 [7]; or

   b) "header" if all the header fields, containing private information that the UE cannot anonymize need to be restricted as described in RFC 3323 [6]. This choice is based on the subscription option.

NOTE 2: The Privacy header field value "header" does not apply to the identity in the From header field.

2) based on operator policy, either modify the From header field to remove the identification information, or add a Privacy header field set to "user".

NOTE 3: When the OIR service is used, the originating UE is supposed to already have removed identity information from the From header field. 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 "presentation-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 AS 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.

For an originating user who has not subscribed to the OIR service but requests the restriction of its identity information by sending Privacy header fields requesting privacy as defined in subclause 4.5.2.1, then the SIP request for initiating a dialog or standalone transaction may be rejected by operator policy with a 403(Forbidden) response including a warning header field 399 "OIR not subscribed".

NOTE 4: Only when supporting the MMTEL for the OIP/OIR Service such a procedure is possible. This requires an initial filter criterion to be setup for the user who is not subscribed to the OIR service.

4.5.2.5 Void

4.5.2.6 Void

4.5.2.7 Void

4.5.2.8 Void

4.5.2.9 Actions at the AS serving the terminating UE

If OIP service of the terminating user is not activated, then the 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 field 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 header fields and remove the Privacy header fields.

Based on local policy, if a P-Asserted-Identity header field and a From header field exist and carry different user identities, the AS may remove the P-Asserted-Identity header fields. As part of this policy, this removal can be limited to scenarios where the From header field fulfils some operator specific prerequisites (e.g. specific national number ranges).

NOTE 1: This option is used to achieve an identical behaviour for different access types where just one identity is provided to the UE.

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 2: 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:

a) anonymize the contents of all header fields containing private information that are not "user configurable" in accordance with IETF RFC 3323 [6];

b) add a Privacy header field with the priv-value set to "id" if not already present in the request; and

c) remove the priv-value "header" from the Privacy header field in accordance with IETF RFC 3323 [6].

NOTE 3: The Privacy header field value "header" does not apply to the identity in the From header field.

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

4.5.2.10 Void

4.5.2.11 Void

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.

The UE may support the operator's originating party identity determination policy.

The UE may support being configured with the operator's originating party identity determination policy in the "FromPreferred" leaf node of 3GPP TS 24.417 [17].

Editor's note [CR#0055, IOC_UE_conf]: Handling of any configuration on UICC related to the operator's originating party identity determination policy is FFS.

If the UE supports the operator's originating party identity determination policy:

1) if the operator's originating party identity determination policy indicates that the From header field is not used for determination of the originating party identity in OIP service, the UE shall determine that the identity(ies) in the P-Asserted-Identity header field(s) is(are) the originating user identity. If the P-Asserted-Identity header field is absent and the Privacy header field is set to "id", the UE shall determine the originating party identity is anonymized. If the P-Asserted-Identity header field is absent and the Privacy header field is set to "none" or absent, the UE shall determine the originating party identity is unavailable; and

2) if the operator's originating party identity determination policy indicates that the identity provided within the From header field is used for determination of the originating party identity in OIP service, then regardless of the presence or absence of the P-Asserted-Identity header field, the UE shall determine that the identity in the From header field is the originating user identity.

NOTE 1: The UE finds the network-asserted identity(ies) of the originating user in the P-Asserted-Identity header field(s). The UE finds the additional identity in the From header field.

NOTE 2: If the UE does not support the operator's originating party identity determination policy, it is dependent on the UE implementation whether the additional identity, the network-asserted identity(ies), all or none are presented to the user.

NOTE 3: It is not guaranteed that the additional identity is trusted.

NOTE 4: If no P-Asserted-Identity header fields are present, but a Privacy header field was present, then the one or more network-asserted identities of the originating user can have been withheld due to presentation restriction.

NOTE 5: If neither P-Asserted-Identity header fields nor a Privacy header field are present, then the network-asserted identities of the originating user can lack availability (due to, for example, interworking with other networks), or the user can be without a subscription to the OIP service.

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 Identity Presentation (TIP)

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

4.6.3 Terminating Identity Restriction (TIR)

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

4.7 Interactions with other networks

4.7.1 Void

4.7.2 Void

4.7.3 Void

4.8 Signalling flows

No OIP or OIR service specific signalling flow is necessary in addition to the basic communication control according to 3GPP TS 24.229 [3].

4.9 Parameter values (timers)

No specific timers are required.

4.10 Service configuration

4.10.0 General

Originating Identity documents are sub-trees of the *simservs* XML document specified in 3GPP TS 24.623 [13]. As such, Originating Identity documents use the XCAP application usage in 3GPP TS 24.623 [13].

Data semantics: The semantics of the Originating Identity XML configuration document is specified in subclause 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 subclause 4.10.2 and the *simservs* XML schema specified in subclause 6.3 of 3GPP TS 24.623 [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 subclause 4.5.2.4 for the case OIR service in "temporary mode" with default "presentation-restricted".

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

Manipulation of the active attribute of the <originating-identity-presentation> service element and of the <originating-identity-presentation-restriction> service element is subject to authorization via local policy. Unauthorized manipulation attempts are rejected with an HTTP 409 (Conflict) response as defined in IETF RFC 4825 [16].

4.10.2 XML schema

```
<?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

No signalling flows are provided.

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.

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
2008-01					Technically identical copy as **3GPP TS 24.607** as basis for further development.		1.3.2
2008-02					Implemented C1-080099		1.4.0
2008-04					The following CR's were incorporated and the editor adopted their content / structure to the structure of the TS C1-080883 C1-081004 C1-081086 C1-081412 C1-081434	1.4.0	1.5.0
2008-05					The following CR's were incorporated and the editor adopted their content / structure to the structure of the TS C1-081553 C1-081614 C1-081829 C1-081911	1.5.0	1.6.0
2008-05					Editorial changes done by MCC	1.6.0	1.6.1
2008-06					CP-080328 was approved by CT#40 and version 8.0.0 is created by MCC	1.6.1	8.0.0
2008-06					Version 8.0.1 created to include attachments (.xml and .xsd files)	8.0.0	8.0.1
2008-09	CT#41	CP-080533	0001		Removal of normative statements in NOTEs	8.0.1	8.1.0
2008-09	CT#41	CP-080533	0002	1	Network requirements for OIP and OIR	8.0.1	8.1.0
2008-09	CT#41	CP-080539	0003	1	Allow SIP based user configuration mechanism for configuring supplementary services	8.0.1	8.1.0
2008-12	CT#42	CP-080864	0004	2	Interaction between SIP and Ut based service configuration	8.1.0	8.2.0
2008-12	CT#42				Editorial clean up by MCC	8.1.0	8.2.0
2009-06	CT#44	CP-090407	0006	1	Invalid XML schema bug fix	8.2.0	8.3.0
2009-12	CT#46	CP-090905	0009	1	Action on the originating network to apply privacy	8.3.0	8.4.0
2009-12	CT#46	CP-090923	0008		Ut applicability for OIP	8.4.0	9.0.0
2010-03	CT#47	CP-100141	0013	1	Error in XCAP for OIP/OIR	9.0.0	9.1.0
2010-03	CT#47	CP-100135	0014	1	Header privacy correction	9.0.0	9.1.0
2010-03	CT#47	CP-100141	0015	1	OIP activation/deactivation	9.0.0	9.1.0
2010-06	CT#48	CP-100371	0019	1	Conflicting normative statement	9.1.0	10.0.0
2012-06	CT#56	CP-120307	0022	1	Cleanup of privacy requirements	10.0.0	11.0.0
2012-09	CT#57	CP-120676	0027	2	Reference corrections	11.0.0	11.1.0
2012-12	CT#58	CP-120793	0028	6	Application of privacy correction and clarification	11.1.0	11.2.0
2014-03	CT#63	CP-140116	0029	3	Inclusion of definition for private information	11.2.0	11.3.0
2014-03	CT#63	CP-140143	0033	1	Correction of Notes regarding P-Asserted-Identity header removal for OIP / OIR	11.3.0	12.0.0
2014-09	CT#65	CP-140666	0046	2	Procedures for OIR not subscribed	12.0.0	12.1.0
2014-09	CT#65	CP-140665	0048		Privacy - wrong reference to 24.229	12.0.0	12.1.0
2014-12	CT#66	CP-140837	0044	5	Presentation of Calling Identity in Terminating UE	12.1.0	12.2.0
2015-03	CT#67	CP-150082	0049	3	Introduction of Network Option for removal of P-Asserted-Identity header field	12.2.0	13.0.0
2015-06	CT#68	CP-150328	0051	4	Clarification on removal of priv-value at the terminating AS	13.0.0	13.1.0
2015-06	CT#68	CP-150328	0052	2	Clarification on procedure for priv-value "session" and "critical"	13.0.0	13.1.0
2015-09	CT#69	CP-150530	0053	1	Reconstructing subclause 4.5.2.4	13.1.0	13.2.0
2015-12	CT#70	CP-150709	0054	3	OIR configuration clarification	13.2.0	13.3.0

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2016-09	CT#73	CP-160515	0055	2	B	Adding reference to TS 24.417 for OIP-OIR MO	14.0.0

History

Document history		
V14.0.0	May 2017	Publication