International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3614

(01/2014)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Service and session control protocols – supplementary services

Originating identification presentation and originating identification restriction protocol specification as next-generation network supplementary service

Recommendation ITU-T Q.3614

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3999
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	**Q.3600–Q.3649**
NGN applications	Q.3700–Q.3849
Testing for next generation networks	Q.3900–Q.3999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Q.3614

Originating identification presentation and originating identification restriction protocol specification as next-generation network supplementary service

Summary

Recommendation ITU-T Q.3614 specifies the protocol for originating identification presentation and originating identification restriction (OIP/OIR) as a next-generation network (NGN) supplementary service.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3614	2014-01-13	11	11.1002/1000/12107

Keywords

Internet Protocol multimedia subsystem (IMS), next-generation network (NGN), originating identification presentation and originating identification restriction (OIP/OIR), session initiation protocol (SIP).

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Q.3614

Originating identification presentation and originating identification restriction protocol specification as next-generation network supplementary service

1 Scope

This Recommendation specifies the protocol description of the originating identification presentation (OIP) and the originating identification restriction (OIR) supplementary services, based on the requirements and architecture of the ISDN CLIP and CLIR supplementary service. This document provides the protocol details in the NGN service control based on session initiation protocol (SIP).

NOTE – It can be noted that the behaviour described in this Recommendation does not take into account other behaviours that are specified in other applications, and care needs to be taken when designing the filters (for example) when two or more applications are involved in a session.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T I.210] Recommendation ITU-T I.210 (1993), *Principles of telecommunication services supported by an ISDN and the means to describe them*.

[3GPP TS 23.228] 3rd Generation Partnership Project V12.3.0 (2013-12), *Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 12).*

[ETSI EN 300 089] ETSI EN 300 089 V3.1.1 (2000), *Integrated Services Digital Network (ISDN); Calling Line Identification Presentation (CLIP) supplementary service; Service description*.

[ETSI EN 300 090] ETSI EN 300 090 (2000), *Integrated Services Digital Network (ISDN); Calling Line Identification Restriction (CLIR) supplementary service; Service description*.

[ETSI TS 124 229] 3GPP TS 124 229 (2013), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229 version 11.9.0 Release 11).*

[ETSI TS 124.607] 3GPP TS 24.607 (2013), *Digital cellular telecommunications system (Phase 2+); 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 11.2.0 Release 11).*

[ETSI TS 183 007] ETSI TS 183 007 V2.0.0 (2008), *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.

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[IETF RFC 3323] IETF RFC 3323 (2002), *A Privacy Mechanism for the Session Initiation Protocol (SIP)*.

[IETF RFC 3325] IETF RFC 3325 (2002), *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*.

[IETF RFC 3966] IETF RFC 3966 (2004), *The tel URI for Telephone Numbers*.

[IETF RFC 3986] IETF RFC 3986 (2005), *Uniform Resource Identifier (URI): Generic Syntax*.

[IETF RFC 4825] IETF RFC 4825 (2007), *The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 dialog: See [IETF RFC 3261].

3.1.2 header: See [IETF RFC 3261].

3.1.3 header field: See [IETF RFC 3261].

3.1.4 proxy: See [IETF RFC 3261].

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

3.1.6 request: See [IETF RFC 3261].

3.1.7 response: See [IETF RFC 3261].

3.1.8 session: See [IETF RFC 3261].

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

3.1.10 tag: See [IETF RFC 3261].

3.1.11 (SIP) transaction: See [IETF RFC 3261].

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 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 an SIP URI (see [IETF RFC 3986]) or a "tel" URI (see [IETF RFC 3966]).

3.2.2 incoming initial request: All requests intended to initiate either a dialog or a stand-alone transaction terminated by the served user or the specific network entity.

3.2.3 originating UE: Sender of an SIP request intended to initiate either a dialog (e.g., INVITE, SUBSCRIBE), or a stand-alone transaction. (e.g., OPTIONS, MESSAGE).

3.2.4 outgoing (communication): Communication outgoing from the user side of the interface.

3.2.5 outgoing initial request: All requests intended to initiate either a dialog or a stand-alone transaction received from the served user or the specific network entity.

3.2.6 stand-alone 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 an SIP dialog would be considered to be part of a stand-alone transaction.

3.2.7 terminating UE: Recipient of an SIP request intended either to initiate a dialog or to initiate either a dialog or a stand-alone transaction.

3.2.8 trusted identity information: Network generated user public identity information.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

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 Services Digital Network
MCID	Malicious Communication Identification
MGCF	Media Gateway Control Function
NGN	Next Generation Network
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
PSTN	Public Switched Telephone Network
SC	Service Control
SDP	Session Description Protocol
SIP	Session Initiation Protocol
UE	User Equipment
URI	Universal Resource Identifier

5 Originating identification presentation (OIP) and originating identification restriction (OIR)

5.1 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.

5.2 Description

5.2.1 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 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.

5.3 Operational requirements

5.3.1 Provision/withdrawal

5.3.1.1 OIP provision/withdrawal

The OIP service may be provided after some prior arrangement has been made with the service provider or it may be generally available.

The OIP service shall be withdrawn at the subscriber's request or by the administrator of this service.

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, which is intended to be transparently transported by the network, is not screened by the network.

5.3.1.2 OIR provision/withdrawal

The OIR service, temporary mode, may be provided on a subscription basis or it 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 as 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

5.3.2 Requirements on the originating network side

As part of the basic communication procedures, 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 stand-alone 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 include 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 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 the subscriber’s request at the time of the 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 the outgoing initial request.

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

NOTE 1 – For the network to invoke the service, the service control 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. Appendix II 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 2 – As an informative description, for OIP/OIR this means the following procedures are expected to be provided by the service control regardless of whether the originating user subscribes to the OIP service or OIR service. When the service control receives an initial request for a dialog or a request for a stand-alone transaction, and the request contains a P-Preferred-Identity header field that matches one of the registered public user identities, the service control is expected to identify the initiator of the request by that public user identity. In particular, the service control is expected to include a P-Asserted-Identity header field set to that public user identity. When the service control receives an initial request for a dialog or a request for a stand-alone transaction, and the request contains a 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 service control is expected to identify the initiator of the request by a default public user identity. In particular, the service control is expected to include a P-Asserted-Identity header field set to the default public user identity. If there is more than one default public user identity available, the service control is expected to randomly select one of them.

NOTE 3 – In the case where the service control has knowledge of an associated TEL-URI for an SIP URI contained in the P-Asserted-Identity header field received in the request, the service control adds a second P-Asserted-Identity header field containing this TEL-URI.

NOTE 4 – For the service control 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. Appendix II provides an example of an initial filter criterion that can be applied for the OIR service.

NOTE 5 – It is assumed that the IBCF is responsible for stripping the P-Asserted-Identity from the SIP header when interworking with untrusted networks.

5.3.3 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 the 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 the originating user invoking 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 CSCF applies any privacy required by [IETF RFC 3325] to the P-Asserted-Identity. In particular, if the Privacy header field is included and set to "id", the service control removes any P-Asserted-Identity header fields from the request.

NOTE 2 – The priv-value "id" in the Privacy header is not expected to be removed when removing any P-Asserted-Identity header.

If the request contains the Privacy header fields "header" or "user", the service control forwards the request to the AS.

NOTE 3 – For the service control to forward an initial request or stand-alone request to an AS, an initial filter criterion is to be set up for the user who is subscribed to the service. Appendix II provides an example of an initial filter criterion that can be applied for the OIP service.

NOTE 4 – When removing the P-Asserted-Identity, any following services in the chain could be affected. Therefore, services based on the originating identity (such as ICB and ACR), are expected to precede the OIP service in the chain.

NOTE 5 – It is assumed that the IBCF is responsible for stripping the P-Asserted-Identity from the SIP header when interworking with untrusted networks.

5.4 Syntax requirements

The relevant headers are:

- The P-Preferred-Identity header field, which shall conform to the specifications in [IETF RFC 3325] and [IETF RFC 3966].
- The P-Asserted-Identity header field, which shall conform to the specifications in [IETF RFC 3325] and [IETF RFC 3966].
- The Privacy header field, which shall conform to the specifications in [IETF RFC 3323] and [IETF RFC 3325].
- The From header field, which shall conform to the specifications in [IETF RFC 3261] and [IETF RFC 3966].

5.5 Signalling procedures

Configuration of supplementary services by the user should:

- use SIP-based user configuration.

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.

5.5.1 Activation/deactivation

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

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

5.5.1.1 Registration/erasure

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

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

5.5.1.2 Interrogation

For interrogation of OIP and OIR, the mechanisms specified in clause 5.5 should be used.

5.5.2 Invocation and operation

5.5.2.1 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 stand-alone transaction as a trigger for the creation of a public user identity.

NOTE 1 – 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 having 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] and [IETF RFC 3325] 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 [IETF RFC 3323] and [IETF RFC 3325].

– 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 [IETF RFC 3323] and [IETF RFC 3325].

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 [ETSI TS 124 229].

5.5.2.2 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 the 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 have already 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 the default "not restricted", if the request includes a Privacy header field which 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.

5.5.2.3 Actions at the AS serving the terminating UE

If the 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 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:

a) anonymize the contents of all headers containing private information in accordance with [IETF RFC 3323] and [IETF RFC 3325]; and

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

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

5.5.2.4 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 stand-alone 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 has previously been present, then 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 can lack availability (due to, for example, interworking with other networks), or the user can be without a subscription to the OIP service.

NOTE 3 – A user-provided identity can also be available, within the From header field of the request.

5.5.2.5 Actions at the P-CSCF serving the terminating UE

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

5.6 Interaction with other services

5.6.1 Communication hold (HOLD)

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

5.6.2 Terminating identity presentation (TIP)

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

5.6.3 Terminating identity restriction (TIR)

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

5.6.4 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 this Recommendation.

5.6.5 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 this Recommendation.

5.6.6 Conference calling (CONF)

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

5.6.7 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.

5.6.8 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.

5.6.9 Incoming communication barring (ICB)

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

5.6.10 Explicit communication transfer (ECT)

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

5.7 Signalling flows

No OIP or OIR service-specific signalling flow is necessary in addition to the basic communication control.

5.8 Parameter values (timers)

No specific timers are required.

Appendix I

Signalling flows

(This appendix does not form an integral part of this Recommendation.)

No signalling flows are provided.

Appendix II

Example of filter criteria

(This appendix does not form an integral part of this Recommendation.)

This appendix provides an example of a filter criterion that triggers SIP requests that are subject to initial filter criteria (IFC) evaluation.

II.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.

II.2 Terminating filter criteria for OIP service

All incoming SIP requests are forwarded to an application server providing the OIP service.

Appendix III

The reference information for OIP/OIR supplementary service interoperability based on NGN

Calling line identification presentation and related headers[1]

(This appendix does not form an integral part of this Recommendation.)

This appendix describes the reference information for OIP/OIR supplementary service interoperability based on NGN. For interoperability testing, a concrete and detailed protocol specification is necessary.

This appendix provides such reference information for interoperability testing specifications. As this appendix refers to domestic and national information, this content should not reflect upon the main body of this Recommendation. Therefore, although the content of this appendix includes national specifications, it is still valuable information which can be used as a reference for more concrete implementation information.

III.1 Overview

This appendix clarifies procedures for calling line identification presentation and notification of "cause of no ID", SIP headers used for them (*P-Preferred-Identity*, *P-Asserted-Identity*, *Privacy* and *From*) and *Request-URI,* the SIP header used for relevant network-asserted user identity (*P-Associated-URI*) and the SIP header used for terminating UE notification (*P-Called-Party-ID*).

III.2 References

References used in this appendix are as follows.

[TS-1008] "Technical Specification on ISDN Called Party Subaddress Information Transferring through Provider's SIP Networks". TTC standard TS-1008, version 1, The Telecommunication Technology Committee, Jun, 2004.

III.3 Network-asserted user identity

The network-asserted user identity is the identity of a user that is asserted by the network through authentication or other means (verified by the network if provided by the terminal), and it is used for originating-UE identity, etc. An example of network-asserted user identity information is a SIP-URI composed of an E.164 number reachable to the terminal. As described in clause III.7, subaddress information may be provided by the originating UE.

Clause III.6 indicates a specific URI format for network-asserted user identity.

III.3.1 Notification when the terminal registers

In the case of using a *REGISTER* request for registration, the network may set a *P-Associated-URI* header [b-IETF RFC 3455] in its *200 OK* response in order to notify a network-asserted user identity to the terminal.

A *P-Associated-URI* header lists one or more URIs which indicate network-asserted user identities allocated to the terminal. In the case that multiple network-asserted user identities are listed, the terminal recognizes the first URI as the default network-asserted user identity.

[1] Clauses III.1 to III.7.1.2 of this appendix are from Annex b of [b-TTC Diff. JT-Q3402 & Q.3402]. Copyright 2011, Telecommunication Technology Committee.

III.4 Originating UE numbers

Originating UE number (hereinafter referred to as originating-UE identity) presentation should be realized based on [IETF RFC 3323], [b-IETF RFC 3324] and [IETF RFC 3325] by notifying network-asserted user identity and presentation/restriction information. Originating UE identity presentation/restriction are applied to requests outside existing dialogs except for *REGISTER* which can be sent and received over the UNI.

Originating UE identity information presentation is mainly performed by four steps as follows.

– An originating UE transmits the selected originating-UE identity information (*P-Preferred-Identity*) and preference of presentation/restriction (*Privacy*) to a network, instructs a destination (*Request-URI*), and calls.

– The network which has the originating-UE verifies and normalizes an originating-UE identity that a terminal selected, takes into consideration the default presentation/restriction setting, etc. regarding the subscriber, and determines an originating-UE identity information transmitted in the network and through the NNI.

– The network which has the terminating UE takes into consideration the preference of presentation/restriction and the terminating UE's subscription for originating-UE identity presentation service, and determines an originating-UE identity information to be notified to the terminating UE.

– The terminating UE is notified of originating-UE identity information from the network when receiving a call.

III.4.1 Procedures on originating a call

III.4.1.1 Selecting an originating-UE identity

In the case that a terminal desires to explicitly select an originating-UE identity among the network-asserted identities, the terminal populates the selected network-asserted user identity in *P-Preferred-Identity* header in requests outside existing dialogs. If network-asserted user identities are notified, the terminal selects one of the URIs listed in a *P-Associated-URI* header and populates it in the *P-Preferred-Identity* header.

The network handles a SIP-URI set in the *P-Preferred-Identity* header as originating-UE identity. Note that in the case the *P-Preferred-Identity* header is not set, or a URI set in the *P-Preferred-Identity* header is not a network-asserted user identity allocated to the originating UE, it is to be the same as when the default network-asserted user identity is set in the *P-Preferred-Identity* header.

III.4.1.2 Setting for presentation/restriction of originating-UE identity

When a terminal sends requests outside existing dialogs, originating-UE identity presentation/restriction is requested using two kinds of procedures, namely, *Privacy* header [IETF RFC 3325] and 186/184 prefixes.

- Originating UE identity presentation can be requested by setting "*none*" in *Privacy* header, and restricted by setting "*id*". The *Privacy* header is set only when the terminal has the user configuration option of originating-UE identity presentation/restriction, and the user completes the setting.
- In the case that the *Request-URI* is a URI composed of a national telephone number, originating-UE identity presentation is specified when the 186 prefix is set, and restriction is specified when the 184 prefix is set. Whether to set the 186/184 prefix must be left to the decision of a dialling user, and a terminal must not act on its own, such as automatically putting the prefix.

The settings of the *Privacy* header and those of the 186/184 prefix are independent of each other.

In the case that the terminal sets "*id*" in a *Privacy* header, *<sip:anonymous@anonymous.invalid>* is set to the SIP-URI of a *From* header. In other cases, a URI identical to that of a *P-Preferred-Identity* header is set.

Table III.1 describes the contents set in the headers above.

Table III.1 – Settings of headers for calling line identification presentation

Field	**Privacy header**		
	None	**id**	**No header**
The *user* part or *telephone-subscriber* part of a *Request-URI*	Number that a user dialled (includes 186/184 prefix if dialled)		
P-Preferred-Identity header	Originating UE's network-asserted user identity		
URI in *To* header	Same value as *Request-URI*		
name-addr in *From* header	Same value as the URI set in a *P-Preferred-Identity* header, if the header is set	<sip:anonymous@anonymous.invalid>	Same value as the URI set in a *P-Preferred-Identity* header, if the header is set

A network selects originating-UE identity presentation/restriction, based on the *Privacy* header and 186/184 prefix setting, and the default originating-UE identity presentation/restriction setting of a subscriber who originates a call.

- In the case that a 186/184 prefix is set at the beginning of the telephone number in the *Request-URI*, the call is treated to be originating-UE identity presentation when 186 is set, and originating-UE identity restriction when 184 is set, regardless of a *Privacy* header setting content.
- The default originating-UE identity presentation setting of the subscriber who originates the call is applied when neither the *Privacy* header setting nor a 186/184 prefix setting exists.
- In the case that the 184 prefix is not set, it is treated to be originating-UE identity presentation, regardless of a Privacy header setting content, at the time of emergency call.

Tables III.2 and III.3 describe the order of priority among the *Privacy* header settings, 186/184 prefix settings, and the default originating-UE identity presentation/restriction setting above.

Table III.2 – Originating-UE identity presentation/restriction selection conditions for normal call

		Prefix of destination number		
		186	**184**	**No prefix**
Privacy	*none*	Originating-UE identity presentation	Originating-UE identity restriction	Originating-UE identity presentation
	id			Originating-UE identity restriction
	No header			Follow the default value of the network managed for each calling user

Table III.3 – Network selected conditions of presentation/restriction of originating-UE identity for emergency call

		Prefix of a destination number		
		186	**184**	**No prefix**
Privacy	*none*	Originating-UE identity presentation	Originating-UE identity restriction	Originating-UE identity presentation
	id			
	No header			

In the case that the originating-UE identity is restricted, "*Anonymous*" (No caller ID: rejected by user) is selected as cause of no ID out of causes described in Table III.4.

III.4.2 Procedures on receiving a call

The SIP headers on the terminating side are populated according to the terminating-UE's subscription of originating-UE identity presentation/restriction.

III.4.2.1 In the case that originating-UE identity, cause of no ID, etc. are notified

The originating-UE identity and cause of no ID, etc. are notified by setting a *Privacy* header in requests outside existing dialogs received from a network.

In the case that "*none*" is set in the *Privacy* header, originating-UE identity is notified by a *P-Asserted-Identity* header. In the *P-Asserted-Identity* header, only a SIP-URI is set or both a SIP-URI and a TEL-URI are set.

In the case that "*id*" is set in the *Privacy* header, originating-UE identity is not notified by the *P-Asserted-Identity* header. Instead, cause of no ID is set in *display-name* in a *From* header. In the case that originating-UE identity is not notified, a displayed content (meaning) may be provided as cause of no ID in the form indicated in Table III.4. Note that the cause of no ID is not provided in the case that a format is not as shown in Table III.4.

Table III.4 – Cause of no ID

Received content (Notes 1 and 2)	**Display content (meaning)**
Anonymous	No caller ID: rejected by user
Coin line/payphone	No caller ID: call from public telephone
Interaction with other service	No caller ID: service conflict
Unavailable	No caller ID: service unavailable
NOTE 1 – It may be enclosed with a pair of double quotation marks. NOTE 2 – A character string listed in this table may be followed by a given character string.	

III.4.2.1.1 Displaying originating-UE identity

A terminal displays originating-UE identity notified by a *P-Asserted-Identity* header according to the order of priority described below.

– In the case that both a SIP-URI and a TEL-URI are set in a *P-Asserted-Identity* header, the TEL-URI is preferred for display.

– In the case that display-name is set in the URI of a *P-Asserted-Identity* header, *display-name* is preferred for display rather than *addr-spec*.

In the case that *display-name* is not set, *user* part of a SIP-URI, *local-number-digits* part or *global-number-digits* part of a TEL-URI is displayed, and this part is a character string indicated in the display content in Table III.5, a display content (meaning) corresponding to each case is indicated.

Table III.5 – Content of caller number display

Received content (Note)	Display content (meaning)
Only numbers	Received numeric string
Starting with +81, and the part after + is composed of only numbers	Numeric string that omits +81 and starts with 0
Starting with +, the part after + is all composed of numbers, and the part next to + is not 81.	Numeric string that omits + and starts with 010
NOTE – When used as *display-name*, it may be enclosed with a pair of double quotation marks.	

III.4.2.2 In the case that originating-UE identity, cause of no ID, etc. are not notified

A *Privacy* header and a *P-Asserted-Identity* header are not set, and a character string which indicates cause of no ID is not set in *display-name* in a *From* header.

III.5 Destination notification

A network may populate a *P-Called-Party-ID* header [b-IETF RFC 3455] in requests outside existing dialogs to a terminating UE, and may set a URI which indicates a network-asserted user identity of the destination.

In the case that multiple network-asserted user identities are allocated, a terminal uses a *P-Called-Party-ID* header in order to identity towards which network-asserted user identity a call is directed. In the case that the *P-Called-Party-ID* header is not set, it should be recognized that the call is directed to the default network-asserted user identity.

III.6 URI format in the case that a national number is used

This clause describes a URI format for the case using a national number as network-asserted user identity and *Request-URI*. Other URI formats may be used.

A SIP-URI or a TEL-URI is used for network-asserted user identity. Either one or multiple SIP-URIs are allocated as network-asserted user identity for each user. A SIP-URI or a TEL-URI is used for *Request-URI*.

III.6.1 user part and local-number-digits part

In a SIP-URI, a numeric string of national number is described in *user* part, and in a TEL-URI, a numeric string of national number is described in *local-number-digits* part. Note that letters equivalent to *visual-separator* are not to be used in either *user* part or *local-number-digits* part.
In the case of *Request-URI*, a numeric string that a user dialled is set as it is in the *user* part or in the *local-number-digits* part. In the case of network-asserted user identity, all digits of a telephone number starting with a national prefix (i.e., "0") are set.

III.6.2 hostport part and descriptor part of context

The *hostport* part of a SIP-URI and the *descriptor* part of TEL-URI *context* are to be set as domain name or host name (including IP address) that a network specifies.

III.7 Sub-address

A network may provide services that are equivalent to services realized by the transfer of sub-address information that can be provided in the ISUP network through the interconnection interface.

This appendix shows the usage of sub-address information in SIP messages and complements the standard. The network and terminals, which handle sub-address information, are required to follow this clause and its subclauses.

III.7.1 Subaddress information

III.7.1.1 Contents of subaddress information

The subaddress is a numeric string of 19 digits or less using numbers 0 to 9. The details are based on [b-IETF RFC 4715].

III.7.1.2 Formats of subaddress information

Subaddress information is applied to all the requests and responses of SIP messages and may be set in the headers that show the originating UE (*From*, *P-Preferred-Identity*, *P-Asserted-Identity*), headers that show the terminating UE (*To*, *P-Called-Party-ID*), and *Request-URI*. Subaddress is expressed as a numeric string following a semicolon (;) and "isub=" in the *user* part of SIP URI or TEL URI.

Bibliography

[b-IETF RFC 3324] IETF RFC 3324 (2002), *Short Term Requiremens for Network Asserted Identity*.

[b-IETF RFC 3455] IETF RFC 3455 (2003), *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP).*

[b-IETF RFC 4715] IETF RFC 4715 (2006), *The Integrated Services Digital Network (ISDN) Subaddress Encoding Type for tel URI*.

[b-TTC Diff. JT-Q3402 & Q.3402] TTC Diff. JT-Q3402 & Q.3402 (2011), *The difference between TTC JT-Q3402 and ITU-T Q.3402*.

[TTC TS-1008] TTC TS 1008 (2004), *Technical specification on ISDN Called Party Subaddress Information Transferring through Provider's SIP Networks*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014