ETSI TS 124 616 V8.5.0 (2009-09)

Technical Specification

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
Malicious Communication Identification (MCID) using
IP Multimedia (IM) Core Network (CN) subsystem;
Protocol specification
(3GPP TS 24.616 version 8.5.0 Release 8)**

Reference
RTS/TSGC-0124616v850

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

ETSI

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 (http://webapp.etsi.org/IPR/home.asp).

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.

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 183 016 [12]. It was transferred to the 3rd Generation Partnership Project (3GPP) in December 2007.

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 Malicious Call Communication Identification (MCID) service based on the stage one and two of ISDN Malicious Call Identification 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). The MCID service will store session related information independent of the service requested.

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

2   References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

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

[3]   Void.

[4]   ETSI TS 181 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);Direct Communication Service in NGN; Service Description [Endorsement of OMA-ERELD-PoC-V1] NGN DC stage 1".

[5]   Void.

[6]   Void.

[7]   Void.

[8]   Void.

[9]   3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

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

[11]   IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[12]   ETSI TS 183 016 V2.5.0: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Malicious Communication Identification (MCID); Protocol specification".

[13]   ETSI TR 180 000: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TS 22.173 [1], ETSI TS 181 006 [4], ETSI TR 180 000 [13] and the following apply:

communication information: information collected and registered by the MCID service

identity information: includes all the information (IETF RFC 3966 [10] and IETF RFC 3986 [11]) identifying a user, including trusted (network generated) and/or untrusted (user generated) identities

trusted identity: network generated user address information

untrusted identity: user generated user address information

3.2 Abbreviations

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

ACR	Anonymous Communication Rejection
AS	Application Server
CB	Communication session Barring
CD	Communication Deflection
CDIV	Communication DIVersion Services
CFB	Communication Forwarding Busy
CFNL	Communication Forwarding on Not Logged-in
CFNR	Communication Forwarding No Reply
CFU	Communication Forwarding Unconditional
CONF	Conference
CW	Call Waiting
ECT	Explicit Communication Transfer
HOLD	communication Hold
IM	IP Multimedia
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Service Digital Network
MCID	Malicious Call Identification
MGCF	Media Gateway Control Function
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
PSTN	Public Switched Telephone Network
S-CSCF	Service - Call Session Control Function
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TIP	Terminating Identification Presentation
TIR	Terminating Identification Restriction
UE	User Equipment
URI	Uniform Resource Identifier

4 Malicious Communication Identification (MCID)

4.1 Introduction

The MCID service will store session related information of incoming communications independent of the service requested. The following communication information shall be registered:

-     Destination Party Identity Information;

-     originating Party Identity Information; and

-     local time and date of the invocation in the network serving the called user.

The communication information shall not be available to the terminal equipment under the control of the called user nor the originating user. The communication information shall be stored at a location(s) under the control of the network operator.

A network subscription option can be provided which allows automatic invocation of MCID service on communications to the served user which are not answered.

    NOTE: The purpose of this option is to allow for registration of communications that ring for a short time only.

A user subscription option where the MCID service can either be invoked during the active phase of the communication, or after the active phase for a limited period but never after communication termination by the served user.

4.2 Description

4.2.1 General description

The Malicious Communication Identification (MCID) service allows the service provider to trace the identity information of the source of an incoming communication on request of the destination user.

4.3 Operational requirements

4.3.1 Provision/withdrawal

This service shall be provided and withdrawn after pre-arrangement with the service provider, in accordance with national legal requirements.

This service has two modes: permanent mode and temporary mode. The permanent mode is active for all incoming communications, and the temporary mode is active only for the incoming communications declared by the served user.

As a network option, the MCID service can be offered with several subscription options. A network providing the MCID service shall support permanent mode at a minimum. Subscription options are summarized in table 4.3.1.1.

Table 4.3.1.1: Subscription options for MCID services

Subscription options	Value
Mode	Permanent Mode Temporary Mode

4.3.2 Requirements on the originating network side

No specific requirements are needed in the originating network.

4.3.3 Void

Void.

4.3.4 Requirements on the terminating network side

No specific requirements are needed in the terminating network.

NOTE: If the subscriber has a permanent or case by case subscription, based on Initial Filter Criteria (IFC) the INVITE request is forwarded to the AS that provides the MCID service. Annex B provides an example on how an Initial Filter Criteria (IFC) can be configured.

4.4 Coding requirements

The present clause defines the XML Schema to be used for providing the MCID Request/Response and to invoke the temporary mode of the MCID Service.

The application/vnd.etsi.mcid+xml MIME type used to provide request of a missing originating ID and the delivery of the requested originating id AS of the served user shall be coded as following described:

```xml
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/mcid"
targetNamespace="http://uri.etsi.org/ngn/params/xml/simservs/mcid" elementFormDefault="qualified">

   <xs:annotation>
      <xs:documentation>XML Schema Definition to the mcid request-response to the Malicious
Communication Identification service</xs:documentation>
   </xs:annotation>
   <!--Definition of simple types-->
   <xs:simpleType name="bitType">
      <xs:restriction base="xs:string">
        <xs:pattern value="[0-1]"/>
      </xs:restriction>
   </xs:simpleType>
   <!--Definition of complex types-->
   <xs:complexType name="requestType">
      <xs:sequence>
        <xs:element name="McidRequestIndicator" type="bitType"/>
        <xs:element name="HoldingIndicator" type="bitType"/>
      </xs:sequence>
   </xs:complexType>
   <xs:complexType name="responseType">
      <xs:sequence>
        <xs:element name="McidResponseIndicator" type="bitType"/>
        <xs:element name="HoldingProvidedIndicator" type="bitType"/>
      </xs:sequence>
   </xs:complexType>
   <!--Definition of document structure-->
   <xs:element name="mcid">
      <xs:complexType>
        <xs:choice>
           <xs:element name="request" type="requestType"/>
           <xs:element name="response" type="responseType"/>
        </xs:choice>
      </xs:complexType>
   </xs:element>
</xs:schema>
```

4.5 Signalling requirements

4.5.1 Activation/deactivation

The MCID service is provisioned only by the network operator as an automatic invocation on all calls to the served user.

NOTE: On demand invocation by the user can be available in later releases.

4.5.1a Registration/erasure

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

4.5.1b Interrogation

Interrogation of MCID is not applicable.

4.5.2 Invocation and operation

4.5.2.1 Actions at the originating UE

Basic communication procedures according to 3GPP TS 24.229 [2] shall apply.

4.5.2.2 Void

4.5.2.3 Void

4.5.2.4 Void

4.5.2.5 Actions at the AS of the terminating user

4.5.2.5.0 General

The AS shall at the minimum store the following elements of a received INVITE request:

- Destination Party Identity Information included in the Request-URI;

- Originating Party Identity Information included in the P-Asserted-Identity header field, if the P-Asserted-Identity header field is included in the request;

- local time and date of the invocation in the network serving the called user;

- call diversion information received in the History-Info header, if the History-Info header filed is included in the request (escaped Reason);

- Referred-By header field when available;

- Contact header;

- To header; and

- From header.

NOTE: The Originating Party Identity Information included in the P-Asserted-Identity header field is always present in the INVITE request if the request is originated in a trusted network.

If the INVITE request does not contain the information of the originating party, the AS shall send an INFO request including an Identification Request MIME body.

When receiving the INFO request containing identification information, the AS shall at the minimum store the following information:

- Destination Party Identity Information included in the Request-URI of the INVITE request;

- Originating Party Identity Information included in the body of the INFO request;

- local time and date of the invocation in the network serving the called user;

- call diversion information received in the History-Info header, if the History-Info header filed is included in the request (escaped Reason); and

- Contact header field.

4.5.2.5.1 Subscriber has a permanent subscription

The AS shall register stored information. The exact procedure to register the information is implementation dependent and out of scope of the present document.

4.5.2.5.2 Subscriber has a temporary subscription

The AS shall store the required elements of a received INVITE request after the communication has been released for a limited period. If no MCID request is received during that period the stored elements for the last communication can be deleted.

NOTE: This version of the specification does not specify how an AS is requested to register the required information after the communication has been released. This can be an INVITE request with a service specific request URI.

A received reINVITE request of the served user as defined in subclause 4.5.2.12.1 is identified as MCID request and the AS shall register the required information.

The exact procedure to register the information is implementation dependent and out of scope of the present document.

After receiving a BYE request from the originating side the call state shall be held for a current time defined by Timer $T_{MCID-BYE}$.

With expiry of the $T_{MCID-BYE}$ the BYE request shall be forwarded to the served user and the communication shall be released according to the basic communication procedures defined in 3GPP TS 24.229 [2].

If no MCID request was received the stored elements for the last communication can be deleted.

4.5.2.5.3 Request of a missing or incomplete originating Id (network option)

The present subclause is applicable when interacting with the PSTN/ISDN.

If a received initial INVITE request does not contain an originating identification or a incomplete originating identification and only if requested by operator policy regarding the received P-Asserted-Identity header field, the AS shall send a INFO request containing a XML mcid body with MCID XML Request schema requesting the originating ID towards the originating network. If requested by operator policy and proprietary signalling, the AS shall skip sending the INFO request containing a XML mcid body with MCID XML Request schema and continue with the session setup as defined in 3GPP TS 24.229 [2].

NOTE: The received P-Asserted-Identity header field can contain a specific value indicating to skip sending INFO requests as the INFO request can indicate the request for identity towards the originating UA. The specific content of the P-Asserted-identity header field that triggers this behaviour is operator specific and is outside the scope of this specification.

After sending of the INFO request requesting the originating id, timer T_{O-ID} (as defined in subclause 4.8) is started.

When the Identification response (INFO request containing a XML mcid body with MCID XML Response schema and the originating identity) is received:

- the timer T_{O-ID} is stopped; and

- the MCID information is stored;and

- a 180 (Ringing) response is sent towards the originating user according to the basic communication procedures.

When a Identification response INFO request is received without the MCID information:

- timer T_{O-ID} is stopped; and

- a 180 (Ringing) response is sent towards the originating user according to the basic communication procedures.

When the timer T_{O-ID} expires before an Identification response INFO request is received, a 180 (Ringing) response is sent towards the originating user according to the basic communication procedures.

4.5.2.6 Void

4.5.2.7 Void

4.5.2.8 Void

4.5.2.9 Void

4.5.2.10 Void

4.5.2.11 Void

4.5.2.12 Actions at the destination UE

4.5.2.12.0 Subscriber has a permanent subscription

Basic communication procedures according to 3GPP TS 24.229 [2] shall apply.

4.5.2.12.1 Subscriber has a temporary subscription

In order to invoke the MCID service the UE shall sent a reINVITE request including a XML MIME with XML mcid body with MCID XML Request schema containing a McidRequestIndicator set to 1.

As a network operator option, the UE can skip including the XML MIME with XML mcid body in the reINVITE.

> NOTE: A reINVITE request without the XML MIME with XML mcid body can not be clearly identified as a trigger for the MCID service in an AS and therefore this reINVITE request will be sent towards the originating side. Additionally, if this network option is chosen, the AS will register MCID data for every reINVITE that the UE sends.

4.6 Interaction with other services

4.6.1 Communication Hold (HOLD)

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

4.6.2 Terminating Identification Presentation (TIP)

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

4.6.3 Terminating Identification Restriction (TIR)

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

4.6.4 Originating Identification Presentation (OIP)

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

4.6.5 Originating Identification Restriction (OIR)

Even if the originating identification is a secret (restricted) identification, MCID invocation is possible.

4.6.6 Conference (CONF)

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

4.6.7 Communication Diversion Services (CDIV)

The MCID service can be invoked for a diverted communication. In addition to the normal operation of the MCID service, the identity of the first diverting user shall be registered and, as a network option, the last diverting user can be registered.

4.6.7.1 Communication Forwarding Unconditional (CFU)

If the served user has activated CFU service, once forwarding has taken place, the forwarding user cannot invoke the MCID service.

4.6.7.2 Communication Forwarding Busy (CFB)

If the served user has activated CFB, once forwarding has taken place, the forwarding user cannot invoke the MCID service.

4.6.7.3 Communication Forwarding No Reply (CFNR)

If the served user has activated CFNR, once forwarding has taken place, the forwarding user (served user) cannot invoke the MCID service.

The MCID service shall not be automatically invoked when an alerting communication is terminated due to the invocation of the communication forwarding no reply service.

4.6.7.4 Communication Forwarding on Not Logged-In (CFNL)

If the served user has activated CFNL, once forwarding has taken place, the forwarding user (served user) cannot invoke the MCID service even after a log-in procedure.

The MCID service shall not be automatically invoked when an alerting communication is terminated due to the invocation of the communication forwarding not logged in service.

4.6.7.5 Communication Deflection (CD)

If the served user has activated communication deflection, once deflection has taken place, the deflecting user cannot invoke the MCID service.

The MCID service shall not be automatically invoked when an alerting communication is terminated due to the invocation of the communication deflection service.

4.6.8 Call Waiting (CW)

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

4.6.9 Anonymous Communication Rejection and Communication session Barring (ACR/CB)

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

4.6.10 Explicit Communication Transfer (ECT)

If the transferor invokes the malicious communication identification service on an initial communication after that communication has been successfully transferred then the AS will reject the request.

4.7 Interactions with other networks

4.7.1 Void

4.7.2 Void

4.7.3 Void

4.8 Parameter values (timers)

A new timer is identified in the destination exchange:

Timer T_{O-ID}: 4-15 seconds.

Timer T_{O-ID} is initiated only at the AS of the served user after sending an MCID request in an INFO request and is stopped at the receipt of an INFO request containing a XML mcid body with MCID XML Response schema.

At expiry of the timer, the communication continues according to the basic communication procedures.

A new timer is identified in the AS to count the post time for invoking the MCID temporary mode.

Timer $T_{MCID-BYE}$: recommended 0-120 seconds. The timer value is defined by the Operator.

Timer $T_{MCID-BYE}$ initiated only at the AS of the served user after receiving a CANCEL request or BYE request.
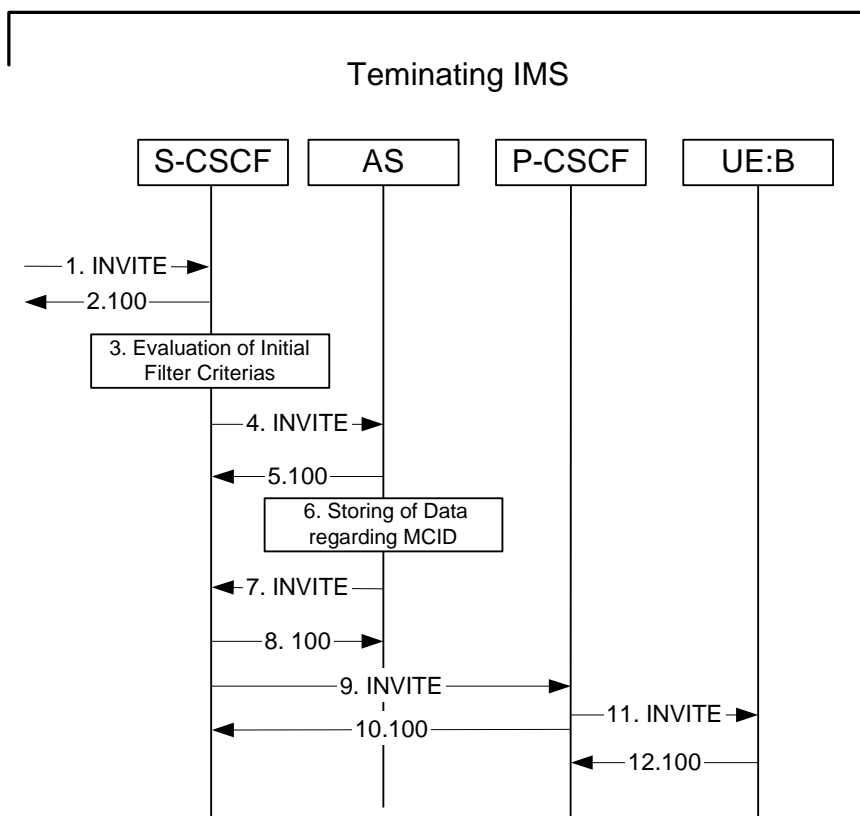
At expiry of the timer, the communication continues shall be released according to the basic communication procedures defined in 3GPP TS 24.229 [2].

Annex A (informative): Signalling Flows

A.1　　MCID invocation

The MCID invokes, in the destination, the storage of data.

Figure A.1 shows an example signalling flow for the scenario.

Figure A.1: MCID Permanent and triggered by the B user

The steps of the flow are as follows:

1) INVITE request (to S-CSCF).

   The INVITE request is sent from the UE to S-CSCF. The INVITE request includes P-Asserted-Identity header fields as follows:

   - P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>;

   - Privacy header field: id or Privacy header or Privacy user; and

   - P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>.

2) 100 (Trying) response (from S-CSCF).

3) Evaluation of initial filter criteria.

The initial Filter criteria identifies that the requested URI is subscribed to the MCID service. Therefore the S-CSCF forwards the INVITE request to the MCID AS.

4) INVITE request (S-CSCF to AS).

   INVITE request is send to the AS.

5) 100 (Trying) response from S-CSCF.

6) AS stores Data.

   AS stores:

   - Request URI.

   - To header field.

   - P-Asserted-Identity header fields.

   - From header field.

   - Contact header field.

   - Time and date field.

7-12) INVITE request (S-CSCF to AS).

INVITE request is send towards the UE:B.

A.2 Identity information not present in the initial request

Hereby, we show a PSTN to IMS scenario, but notice that any call, originated in the PSTN domain and being diverted before reaching the served user AS, must be treated in the same manner. The terminating AS sends a 18x provisional response previous to sending a SIP INFO request, which requests the information from the originating network. It can then route the call while waiting for an answer to the INFO request. Note that the 18x response is sent reliably, this is not intended to indicate ringing (not be a 180 (Ringing) response), and contains no SDP. This 18x response establishes a early dialog, which is needed before the INFO request can be sent.
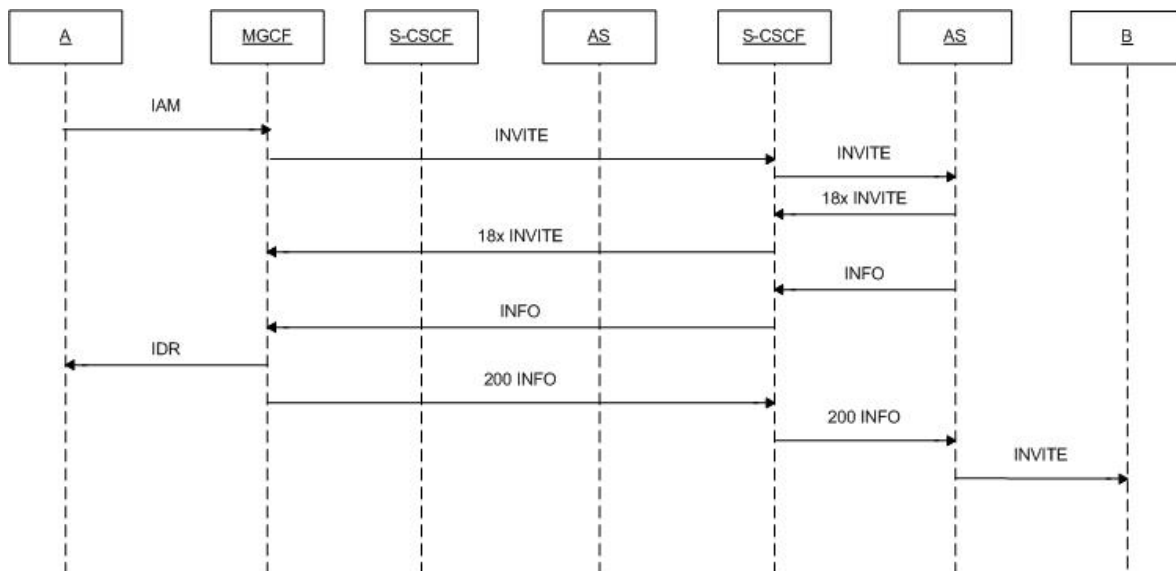
Figure A.2.1:MCID with Information Request towards the ISDN/PSTN

The Terminating AS will then wait for an INFO request containing the response to the information query in the previous INFO request. This request provides the requested identity. If such a request is not received within a period of time, the service cannot be provided.

Figure A.2.2: MCID with Information Response towards the ISDN/PSTN

A.3 MCID invocation in temporary mode

The MCID invokes, in the destination, the storage of data.

Figure A.3.1 shows an example signalling flow for the scenario.

Figure A.3.1: MCID Permanent and triggered by the B user

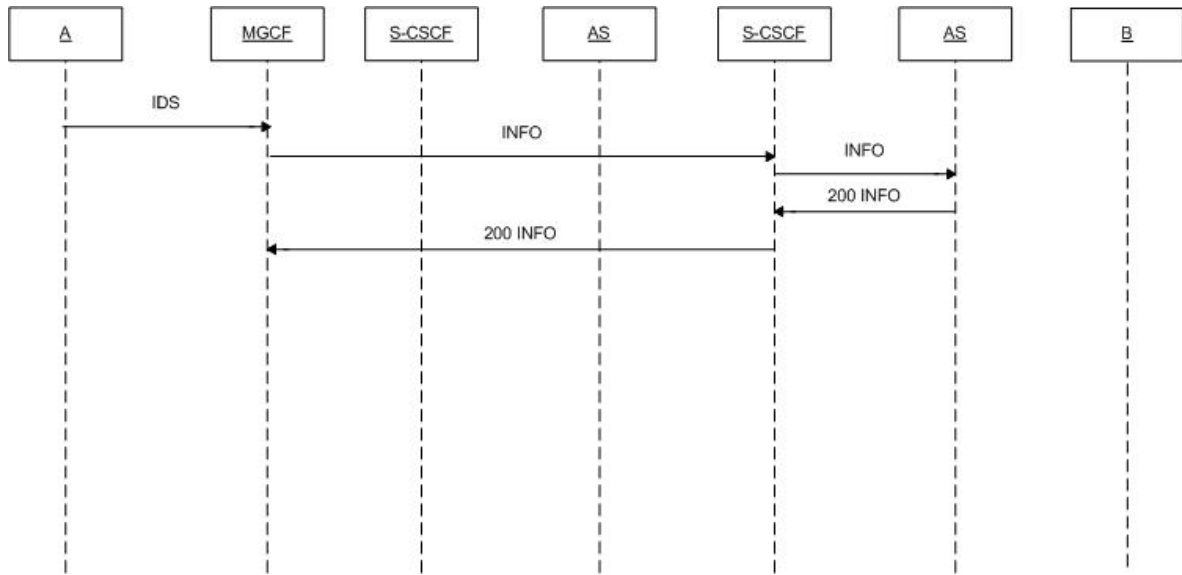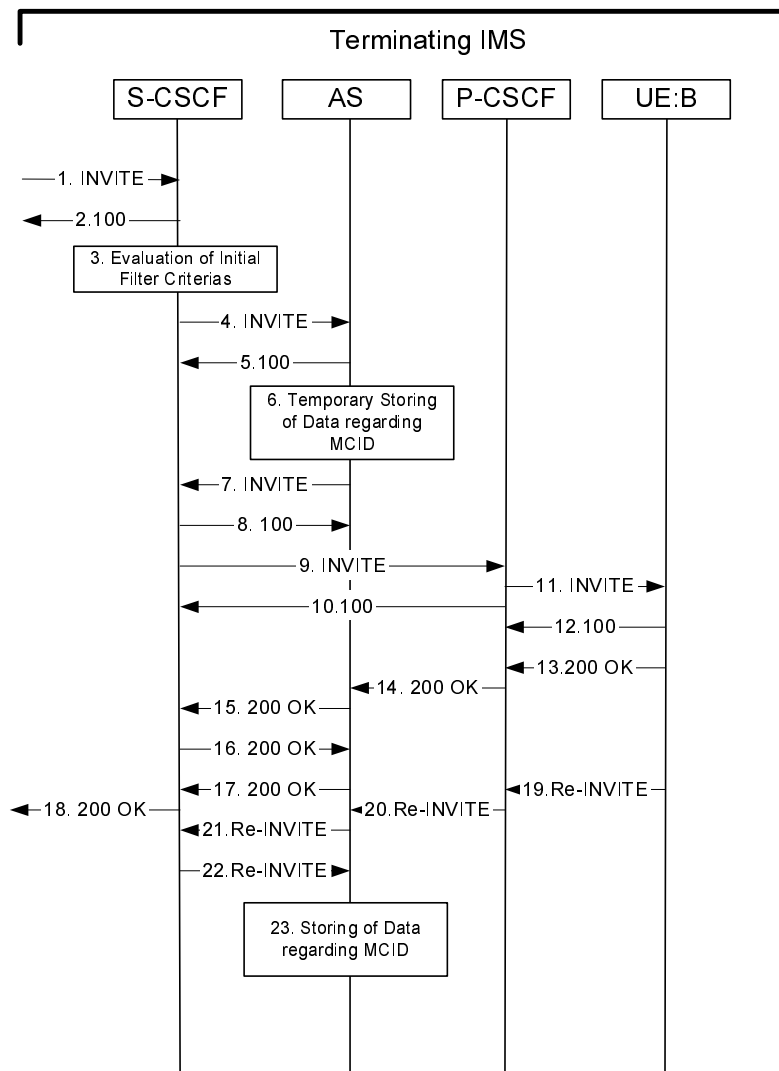The steps of the flow are as follows:

1) INVITE request (to S-CSCF).

   The INVITE request is sent from the UE to S-CSCF The INVITE request includes a P-Asserted-Identity header fields as follows:

   - P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>, "John Doe" <sip:user1_public1@home1.net>;

   - Privacy header field: id or Privacy header or Privacy user.

2) 100 (Trying) response (from S-CSCF).

3) Evaluation of initial filter criteria.

   The initial Filter criteria identifies that the requested URI is subscribed to the MCID service. Therefore the S-CSCF forwards the INVITE request to the MCID AS.

4) INVITE request (S-CSCF to AS).

   INVITE request is send to the AS.

5) 100 (Trying) response from S-CSCF.

6) Temporarily AS stores Data.

AS stores:

- Request URI.

- To header field.

- P-Asserted-Identity header fields.

- From header field.

- Contact header field.

- Time and date field.

7-12) INVITE request (S-CSCF to AS).

INVITE request is send towards the UE:B.

NOTE: 180 (Ringing) response is not shown.

13-18) UE-B takes the communication. A 200 (OK) response is sent towards UE-A.

19) UE-B initiates the temporary mode with sending a reINVITE request - see example in table A.3-19.

Table A.3-19: re-INVITE request (UE-B to P-CSCF)

```
INVITE sip:user1_public1@home1.net; gr=urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6
   ;comp=sigcomp
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:orig@scscf1.home1.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>; tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: sec-agree
Proxy-Require: sec-agree
Supported: precondition, 100rel, gruu, 199
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
   port-c=8642; port-s=7531
Contact: <user2_public1@home2.net;gr=urn:uuid:2ad8950e-48a5-4a74-8d99-ad76cc7fc74
   ;comp=sigcomp SIP/2.0>;+g.3gpp.icsi-ref="urn%3Aurn-7%3gpp-service.ims.icsi.mmtel"
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE, SUBSCRIBE, NOTIFY
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVPF 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendonly
a=des:qos none remote sendonly
a=inactive
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99:MPVMP4V-ES
m=audio 3456 RTP/AVPF 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendonly
a=des:qos none remote sendonly
a=inactive
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=rtpmap:96 telephone-event
```

20-22) network routes the reINVITE request.

23)   The AS finally stores the regarding MCID data cached at step 6).

Annex B (informative):
Example of filter criteria

This annex provides an example of a filter criterion that triggers SIP requests that are subject to initial filter criteria evaluation.

The coding of the Initial Filter Criteria is described in 3GPP TS 29.228 [9].

B.1   Terminating S-CSCF

If a user identified by the Request-URI is provided with the MCID service the IFC can be:

The S-CSCF forwards all INVITE requests to the AS providing the MCID service.

Annex C:
(void)

Annex D (informative):
Void

Annex E (informative): Change history

					Change history		
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2006-03					ETSI TISPAN: 1st Draft forR2.		0.0.1
2006-05					output TISPAN 10bis		0.0.2
2006-06					output TISPAN 10ter		0.0.3
2006-08					input TISPAN#10bis, Inclusion of CR1 to aling with MCID R1 Maintanance		0.0.4
2006-09					output TISPAN#11bis		0.0.5
2006-10					output TISPAN#11ter		0.0.6
2007-02					output TISPAN#12ter including 12tTD163r1 (addition of temporary mode)		2.1.0
2007-03					clean input for TISPAN#13bis		2.1.1
2007-03					agreed output TISPAN#13bis inclusion of 13bTD358 and 13bTD308		2.2.0
2007-05					INPUT version for TISPAN#13ter with editorial changes		2.3.0
2007-05					OUTPUT version for TISPAN#13ter		2.4.0
2007-07					Published as **ETSI TS 183 016** Note: History table of ETSI publication shows v2.4.0.		2.5.0
2007-12					Converted to **3GPP TS 24.516**		2.5.1
2007-12					Technically identical copy as **3GPP TS 24.616** as basis for further development.		2.5.2
2008-02					Implemented C1-080095		2.6.0
2008-04					Implemented C1-081238, C1-080890, C1-081094, C1-081095		2.7.0
2008-04					Corrected version from rapporteur		2.7.1
2008-05					Implemented C1-81559, C1-81834 Incorporation of comments from ETSI Edit help		2.8.0
2008-05					Editorial changes done by MCC	2.8.0	2.8.1
2008-06	CT#40	CP-080332			CP-080332 was approved by CT#40 and version 8.0.0 is created by MCC for publishing	2.8.1	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 text from voided subclause	8.0.1	8.1.0
2008-09	CT#41	CP-080533	0002		Applicability statement in scope	8.0.1	8.1.0
2008-12	CT#42	CP-080865	0003	2	Fixed the flows	8.1.0	8.2.0
2008-12	CT#42				Editorial cleanup by MCC	8.1.0	8.2.0
2009-03	CT#43	CP-090121	0004		Correction of URN-value for Service Identifiers	8.2.0	8.3.0
2009-06	CT#44	CP-090416	0005	2	MCID with temporary subscription	8.3.0	8.4.0
2009-09	CT#45	CP-090665	0006		AS behaviour in case no P-Asserted-Identity	8.4.0	8.5.0

History

Document history		
V8.2.0	January 2009	Publication
V8.3.0	March 2009	Publication
V8.4.0	June 2009	Publication
V8.5.0	September 2009	Publication