ETSI TS 124 196 V15.0.0 (2018-07)

TECHNICAL SPECIFICATION

Universal Mobile Telecommunications System (UMTS); LTE; 5G; Enhanced Calling Name (eCNAM) (3GPP TS 24.196 version 15.0.0 Release 15)

Reference

RTS/TSGC-0124196vf00

Keywords

5G,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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

ETSI

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

Trademarks

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

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 has been produced by the 3rd Generation Partnership Project (3GPP).

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 Enhanced Calling Name (eCNAM) supplementary service based on stage one description in 3GPP TS 22.173 [1]. It provides the protocol details in the IP Multimedia (IM) Core Network (CN) subsystem (see 3GPP TS 24.229 [2]) based on the Session Initiation Protocol (SIP) (see RFC 3261 [3]) where the eCNAM data is retrieved by the terminating network from trusted data sources.

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".

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

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

[4]   3GPP TS 23.003: "Numbering, addressing and identification".

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

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

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

[8]   3GPP TS 24.604: "Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem".

[9]   IETF RFC 8224: "Authenticated Identity Management in the Session Initiation Protocol (SIP)".

[10]   ITU-T Recommendation E.164 (11/2010): "The international public telecommunication numbering plan".

[11]   ITU-T Recommendation I.210 (03/1993): "Principles of telecommunication services supported by an ISDN and the means to describe them".

3 Definitions and abbreviations

For the purposes of the present document, the following definitions and abbreviations apply.

3.1 Definitions

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

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 RFC 3261 [3]) or a tel URI (see RFC 3966 [7]).

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

Private information: information that according to RFC 3323 [6] and RFC 3325 [5] is not permitted to be delivered to the remote end.

Searchkey: a user identity employed to retrieve the eCNAM data associated with that identity from the appropriate data sources.

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

For the purposes of the present document, the following definitions given in RFC 3261 [3] apply.

> **header**
> **header field**
> **request**
> **response**
> **session**
> **(SIP) transaction**

For the purposes of the present document, the following definitions given in ITU-T Recommendation I.210 [11] apply:

> **supplementary service**
> **E.164 telephone number:** telephone number formatted according to ITU-T**.**

3.2   Abbreviations

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

3GPP	3rd Generation Partnership Project
ACR	Anonymous Communication Rejection
AS	Application Server
CCBS	Completion of Communication to Busy Subscriber
CDIV	Communication DIVersion
CN	Core Network
CUG	Closed User Group
CW	Communication Waiting
eCNAM	Enhanced Calling Name
ECT	Explicit Communication Transfer
FA	Flexible Alerting
HOLD	Communication Hold
ICB	Incoming Communications Barring
IETF	Internet Engineering Task Force
IM	IP Multimedia
IMS	IP Multimedia Subsystem
IP	Internet Protocol
MCID	Malicious Communication Identification
MWI	Message Waiting Indication
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
PNM	Personal Network Management
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TIP	Terminating Identification Presentation
TIR	Terminating Identification Restriction
TN	Telephone Number
UE	User Equipment
URI	Universal Resource Identifier

4 Enhanced Calling Name (eCNAM)

4.1 Introduction

The eCNAM service provides the terminating user with the name associated with the originating user and optionally delivers metadata about that originating user. While eCNAM is a terminating service, the eCNAM operations rely on information received from the originating network, such as the originating user's E.164 telephone number (TN) to retrieve eCNAM data from trusted data sources (via methods outside the scope of this specification).

4.2 Service Description

4.2.1 General Description

The eCNAM service provides the terminating user with a name that identifies the originating user, and metadata about that originating user (e.g., address, language).

> NOTE: The terminating service provider retrieves the name and metadata from pre-selected data sources. The terminating service provider can also partner with analytics providers that offer risk indicators about the incoming call (e.g., known perpetrators of scams) as part of the metadata eCNAM delivers.

To retrieve eCNAM data, the service provider formulates queries using a searchkey to retrieve the name and metadata. The searchkey is a user identity obtained from the incoming SIP INVITE. Most commonly, the service provider uses an E.164 TN as that searchkey. Other identities could be used to retrieve the eCNAM data.

If the terminating network determines that the telephone number's (or other identity's) presentation is restricted (i.e., not to be presented to the end user), the eCNAM data will also be restricted.

If the terminating network determines that the telephone number (or other identity's) presentation is not restricted (i.e., to be presented to the end user), the eCNAM data will also be presented to the end user with no restriction.

4.3 Operational Requirements

4.3.1 Provision/withdrawal

The eCNAM service can be provided after prior arrangement with the service provider.

The eCNAM service can be withdrawn at the subscriber's request or for administrative reasons.

4.3.2 Requirements on the Originating Network

eCNAM is a terminating service, however, the eCNAM operations rely on information received from the originating network.

If the originating user identity, such as the originating user's E.164 TN, is not delivered by the originating network to the terminating network, the terminating service provider will not be able to retrieve eCNAM data from the relevant data sources.

> NOTE: The searchkey element necessary for retrieving eCNAM data from the relevant data source is, in most cases, restricted to the originating user's E.164 TN for most databases. However, other user identities can be used as searchkey elements.

The originating network can support a verification capability, such as the number verification capability described in 3GPP TS 24.229 [2]. Without a verification capability at the originating network, the integrity of the eCNAM data retrieved could be impacted.

4.3.3 Requirements on the Terminating Network

4.3.3.1 Data Sources

The eCNAM service involves the retrieval of the name data and the additional caller information from data sources that the terminating service provider has access to, based on service provider policy.

The special arrangements and interfaces between the terminating service provider and the data sources are outside the scope of this document and are subject to operator procedures.

NOTE 1: The accuracy of the name information and the metadata about the caller varies among sources; therefore, the terminating service provider exercises a choice of which source to use. The interfaces and protocols used to retrieve the data are typically negotiated between the terminating service provider and the data source.

NOTE 2: The terminating service provider pre-determines the elements of metadata that will be delivered on each call to eCNAM subscribers. The set of metadata varies from one service provider to another.

4.4   Syntax Requirements

The syntax for the header fields are normatively described in 3GPP TS 24.229 [2]. The relevant headers are:

- The P-Asserted-Identity header field which shall conform to the specifications in RFC 3325 [5] and RFC 3966 [7].

- The Identity header field which shall conform to the specifications in draft-ietf-stir-rfc4474bis [9].

- The Call-Info header field which shall conform to the specifications in RFC 3261 [3].

- The Privacy header field which shall conform to the specifications in RFC 3323 [6] and RFC 3325 [5].

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

- The From header field which shall conform to the specifications in RFC 3261 [3] and RFC 3966 [7].

4.5   Signalling Procedures

4.5.1   General

Configuration of the eCNAM is performed by the service provider.

4.5.2   Activation/Deactivation

The service provider activates the eCNAM service at provisioning, upon the user's request.

The service provider deactivates the service at withdrawal upon the user's request.

No user configuration is defined in this release.

4.5.3   Invocation and Operation

4.5.3.1   Actions at the Originating UE

No actions at the originating UE.

4.5.3.2   Actions at the AS serving the Originating UE

No actions at the AS serving the originating UE.

4.5.3.3   Actions at the AS serving the Terminating UE

4.5.3.3.1   Identity not available

eCNAM is a terminating service; however, the eCNAM operations rely on information received from the originating network.

If the incoming INVITE does not include the user's E.164 TN in the "tel" URI or the 'user element' of the SIP URI, the terminating AS will not be able to retrieve eCNAM data from the relevant data sources. Based on service provider policy, the AS uses the E.164 TN in either the incoming From header field or the incoming P-Asserted-Identity header field to request eCNAM data from the trusted data sources.

If this information is not received in the incoming INVITE or is not available from the data sources (missing data or query timeouts) then the terminating AS shall consider the eCNAM data unavailable.

As a result, the terminating AS shall, according to local policy, populate the text string "Unavailable" in the "display-name" parameter of the outgoing From header field and/or P-Asserted-Identity header field in the SIP INVITE request that the terminating AS sends to the terminating UE.

If some elements of the eCNAM metadata are unavailable (e.g., requested data elements could not be found in the data source), the terminating AS shall deliver the available data to the terminating UE in Call-Info header fields, and shall not deliver the string "unavailable" for the missing elements.

4.5.3.3.2 Identity available, presentation not allowed

If the terminating AS receives a Privacy header field set to any of the priv-values "id", "user" or "header" (i.e., presentation is not allowed), then the terminating AS shall populate the text string "Anonymous" in the "display-name" parameter of the From header field in the SIP INVITE request that the AS sends to the terminating UE. The full SIP URI for Anonymous User Identity is described in 3GPP TS 23.003 [4].

The metadata may be sent to the terminating UE, based on service provider policy.

NOTE: The service provider may allow delivery of only the metadata (such as analytics), if allowed by local and national policies to caution users against fraudsters disguised with anonymous identities.

4.5.3.3.3 Identity available, originating user identity verified and passed, presentation allowed

The terminating AS shall consider that the user identity presentation is allowed when there is no Privacy header field in the received INVITE or a Privacy header field set to priv-value "none".

If the identity presentation is allowed and the result of the originating user identity verification performed (such as the verification resulting in the "verstat" tel URI parameter described in 3GPP TS 24.229 [2]) shows the verification passed, the AS shall proceed to retrieve eCNAM data from the trusted sources.

The AS shall extract the originating identity from the incoming INVITE in order to formulate the query to the trusted data sources. It is based on service provider policy to decide whether the identity retrieved from the P-Asserted-Identity header field, the From header field or both with a priority order.

If the chosen identity is the E.164 TN, the following procedures shall apply:

1 The terminating AS shall extract the TN from the username portion of the incoming SIP URI request of the incoming From header field or P-Asserted-Identity header field, if user=phone parameter is present.

2 If user=phone is not present in the SIP URI, the terminating AS shall extract the TN from the tel URI of the incoming From header field or P-Asserted-Identity header field.

3 If both a SIP URI with user=phone present, and a tel URI are available, the terminating AS shall extract the TN from the tel URI of the incoming From header field or P-Asserted-Identity header field.

4 The terminating AS will query the appropriate data source(s) using the extracted TN.

NOTE 1: The labels/titles of the data elements are known to the terminating service provider based on their arrangements with the data sources.

NOTE 2: Semantic translation is outside the scope of the present document.

NOTE 3: In addition to plain text, the Call-Info header field supports the delivery of icons, which may be needed if analytics results include symbols to be displayed on the UE.

The terminating AS shall populate the received name (retrieved from data sources) in the "display-name" parameter of the From header field or the P-Asserted-Identity header field in the INVITE request being sent to the UE.

The terminating AS shall populate the received metadata elements in one or more Call-Info header fields.

NOTE 4: The eCNAM metadata elements can include information about the caller's language, address, email, or type of business and more. The metadata can also include the results of analytics that the service provider makes available to the user directly or through third party affiliations. The analytics can contain text and icons about the originating user.

If other name information is received in the INVITE request , the terminating service provider local policy shall apply. The AS may discard the received name data.

4.5.3.3.4 Identity available, verification failed

If the originating user identity verification performed (such as the verification resulting in the "verstat" tel URI parameter described in 3GPP TS 24.229 [2]) shows that verification failed, the terminating AS may deliver partial or no eCNAM information to the subscriber's UE.

As a result, and based on terminating service provider policy, the terminating AS may perform one or more of the following actions:

a) The AS may remove the display-name of the From header field or the P-Asserted-Identity header field in the INVITE request being sent to the UE;

b) The AS may populate a text string of the terminating service provider's choice in the display-name of the From header field or the P-Asserted-Identity header field in the INVITE request being sent to the UE. Examples of such strings include "Suspected Spam" or "Fake Number";

c) The AS may populate graphical symbols of the service provider's choice in one or more Call-Info header field(s) to the terminating UE. Examples include warning symbols and text.

4.5.3.4 Actions at the Terminating UE

The terminating UE shall support the receipt of one or more P-Asserted Identity header fields.

The terminating UE shall retrieve the originating user's name from the "display-name" parameter of the P-Asserted Identity header field or the "display-name" parameter of the From header field depending on the header used for determining the originating party identity.

NOTE 1: The data sources queried for metadata are typically local to the service provider, and therefore are populated with data represented in the same language as the subscriber's. Therefore, semantic translation is not likely to be needed. UEs can offer semantic translation of the display as an individual, manufacturer-based capability. Semantic translation is outside the scope of the present document.

The UE shall support receipt of one or more Call-Info header fields.

The terminating UE shall retrieve the metadata of the originating user from the Call-Info header fields.

NOTE 2: UEs can support capabilities such as text-to-speech for the blind, as well as ensuring that messages delivered in colours intended for warnings be relayed in a different method to accommodate colour-blind users.

4.6 Interaction with other Services

4.6.1 Originating Identification Presentation (OIP)

For users that subscribe to both OIP and eCNAM, and subject to service provider policy, the name information retrieved through eCNAM may override any name information available via OIP.

Subject to service provider policy, eCNAM metadata and other OIP data may both be presented to the end user with or without individual marking to distinguish the eCNAM service data from other call information.

4.6.2 Originating Identification Restriction (OIR)

The OIR service shall take precedence over the eCNAM service.

4.6.3 Terminating Identification Presentation / Terminating Identification Restriction (TIP/TIR)

No impact. Neither service shall affect the operation of the other service.

4.6.4 Advice of Charge

No impact. Neither service shall affect the operation of the other service.

4.6.5 Communication Waiting (CW)

If a terminating party has the eCNAM service active and is notified that an incoming communication is waiting, then this terminating user shall receive the eCNAM data on the incoming session, if presentation is not restricted on that incoming session.

4.6.6 Communication Hold

No impact. Neither service shall affect the operation of the other service.

4.6.7 Explicit Communication Transfer (ECT)

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

4.6.8 Closed User Group (CUG)

In general, CUG members do not communicate with users outside the group. However, if members were allowed to activate eCNAM and to receive calls from outside the group, then eCNAM data will be delivered based on the caller's OIR status.

4.6.9 Completion of Communications to Busy Subscriber (CCBS)

The originating party's eCNAM data shall be transmitted to the CCBS customer's UE when the terminating party becomes free, and a CCBS communication is generated to the terminating party.

4.6.10 Communication Diversion (CDIV)

Subject to service provider policy, the terminating AS serving the diverted to user may optionally deliver the eCNAM data of a diverting user. The identity of the diverting user is obtained from the History-Info header field, as described in 3GPP TS 24.604 [8].

4.6.11 Malicious Communication Identification (MCID)

No impact. Neither service shall affect the operation of the other service.

4.6.12 Anonymous Communication Rejection (ACR) and Incoming Communications Barring (ICB)

Within the network execution of ICB and ACR services, either service shall take precedence over the eCNAM service.

4.6.13 Message Waiting Indication (MWI)

No impact. Neither service shall affect the operation of the other service.

4.6.14 Flexible Alerting (FA)

If the FA Pilot has eCNAM activated, incoming calls to the FA Pilot shall apply eCNAM to the members of the FA group.

Metadata that is obtained from analytics shall be based on the FA Pilot and not the individual members' identity.

NOTE: Analytics can sometimes be based on the called party's identity. Therefore, it should be noted that in an FA group, the only identity available for use shall be that of the Pilot.

4.6.15 Personal Network Management (PNM)

For a user that subscribes to both PNM and eCNAM, both originating user identity and eCNAM identity data shall be delivered to the Personal Network UE that is configured to act as a Personal Network controller.

4.7 Parameter values (timers)

Not applicable.

Annex A (informative):
Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-08	C1-105					Version after implementation of pCRs agreed in C1-105	0.1.0
2017-11	C1-106					Version after implementation of pCRs agreed in C1-106	0.2.0
2017-12	C1-107					Version after implementation of pCRs agreed in C1-107	0.3.0
2017-12	CT-78	CP-173044				Presentation for information at TSG CT	1.0.0
2018-01	C1-108					Version after implementation of pCRs agreed in C1-108	1.1.0
2018-02	C1-109					Version after implementation of pCRs agreed in C1-109	1.2.0
2018-03	CT-79	CP-180102				Presentation for approval at TSG CT	2.0.0
2018-03	CT-79					Version 15.0.0 created after approval	15.0.0

History

Document history		
V15.0.0	July 2018	Publication