ETSI TS 124 174 V19.0.0 (2025-10)

TECHNICAL SPECIFICATION

Universal Mobile Telecommunications System (UMTS);
LTE;
5G;
Support of multi-device and multi-identity
in the IP Multimedia Subsystem (IMS);
Stage 3
(3GPP TS 24.174 version 19.0.0 Release 19)

Reference
RTS/TSGC-0124174vj00

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

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 provides the protocol details for the multi-device and multi-identity aspects in the IP Multimedia (IM) Core Network (CN) subsystem based on the requirements from 3GPP TS 22.173 [2].

The present document is applicable to user equipment (UE) and application servers (AS) which are intended to support multi-device and multi-identity aspects in the IMS.

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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.173: "IP Multimedia Core Network Subsystem (IMS) Multimedia Telephony Service and supplementary services; Stage 1".

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

[4] 3GPP TS 24.607: "Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

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

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

[7] 3GPP TS 24.623: "Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services".

[8] IETF RFC 8946: "Personal Assertion Token (PASSporT) Extension for Diverted Calls".

[9] OMA-TS-CPM_Message_Storage_Using_RESTFul_API-V1_0-20181025-D: "CPM Message Store using RESTFul API, Draft Version 1.0 – 25 Oct 2018", http://member.openmobilealliance.org/ftp/Public_documents/COM/COM-CPM/Permanent_documents/OMA-TS-Message_Storage_Using_RESTFul_API-V1_0-20181025-D.zip.

[10] OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C: "RESTful Network API for Network Message Storage, Candidate Version 1.0 – 28 May 2019", http://member.openmobilealliance.org/ftp/Public_documents/ARCH/Permanent_documents/OMA-TS-REST_NetAPI_NMS-V1_0-20190528-C.zip.

[11] 3GPP TS 24.629: "Explicit Communication Transfer (ECT) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[12] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[13] 3GPP TS 24.175: "Management Object (MO) for Multi-Device and Multi-Identity in IMS; Stage 3".

[14] 3GPP TS 23.003: "Numbering, addressing and identification".

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

[16] IETF RFC 4235: "An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)".

[17] 3GPP TS 24.628: "Common Basic Communication procedures using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[18] RFC 4122 (July 2005): "A Universally Unique IDentifier (UUID) URN Namespace".

[19] 3GPP TS 24.173: "IMS Multimedia telephony communication service and supplementary services; Stage 3".

[20] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[21] 3GPP TS 31.103: "Characteristics of the IP multimedia services identity module (ISIM) application".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

native identity: an identity of form tel URI or SIP URI, used by the UE and which is associated with the IMSI which is currently used by the UE for IMS registration. The native identity is IMS registered by the UE.

alternative identity: an identity of form tel URI or SIP URI, used by the UE and which is not associated with the IMSI which is currently used by the UE for IMS registration and is associated with a different IMSI for the same IMS subscription owned by the same IMS network. The alternative identity can be IMS registered by the UE or can be configured in the service data of the UE's IMS subscription.

call pull: procedure in which a UE takes over an ongoing session from another UE in the set of federated UEs.

call push: procedure in which a UE pushes an ongoing session to another UE in the set of federated UEs.

external alternative identity: an identity of form tel URI or SIP URI, used by the UE and which is not associated with the IMSI which is currently used by the UE for IMS registration but is associated with a different IMSI for another IMS subscription owned by the same or a different IMS network. The external alternative identity is not IMS registered by the UE but is configured in the service data of the UE's IMS subscription.

virtual identity: an identity of form tel URI or SIP URI, used by the UE and which is not associated as native identity with any IMSI that is associated with ISIM or USIM in the UE. The virtual identity can be IMS registered by the UE or can be configured in the service data of the UE's IMS subscription.The virtual identity can be used by a single user only or by several users having IMS subscriptions in the same or different IMS networks.

non-native identity: an identity which is not the native identity. The non-native identity may be an alternative identity, external alternative identity or a virtual identity.

federated UEs: a group of UEs which are configured to use the same public user identity.

user A: user A is the originating user, in the present document user A calls user B, where A can be using the identity C.

user B: user B is the terminating user, in the present document user A calls user B, where B can be reached under the identity D.

identity C: identity C is a non-native identity that can be used by user A and is not registered by user A.

identity D: identity D is a non-native identity that can be used by user B and is not registered by user B.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

3pcc	Third party call control
AS	Application Server
MiD	Multi-iDentity
MuD	Multi-Device

4 Multi-device and multi-identity

4.1 Introduction

The Multi-Device (MuD) service is an operator specific service which enables a user to use different UEs that are registered under the same public user identity. The UEs can be of different types (e.g. phone, tablet, wearable device, PC) and can support a communication log.

The Multi-Identity (MiD) service is an operator specific service which enables a user to use different identities. A served user can use a single UE to receive calls addressed to any of its identities and to make calls using any of its identities.

The MuD and MiD services can be used at the same time.

The UE can indicate to the network which identities are active at the UE. If the identity is not active at the UE, the user cannot use given identity in a communication at the UE.

4.2 Description

4.2.1 MuD service description

The MuD service enables a served user to use, in a communication, any of the UEs that are configured to use the same public user identity, i.e. any of the federated UEs.

The MuD service enables a synchronization of communication logs between the federated UEs which support communication log. The communication log provides lists of incoming and outgoing, missed, accepted and rejected calls. If the served user accepts or rejects call from one of the federated UEs or when a missed call notification has been read on one of the federated UEs, the communication logs of the other federated UEs are updated so the served user will see the same information on different federated UEs.

An outgoing call can be made from any of the federated UEs. A federated UE can indicate to the network which public user identities are (de)activated at the federated UE.

An incoming call towards the served user is sent to all federated UEs where that public user identity is active at the federated UE. The call can be accepted on any of the federated UEs which are alerting the served user of an incoming call. The federated UEs can synchronize the call logs by using the call log functionality in OMA-TS-CPM_Message_Storage_Using_RESTFul_API [9] and OMA-TS-REST_NetAPI_NMS [10].

A federated UE can if authorized by the AS push a call to any other of the federated UEs. A federated UE can if authorized pull a call from any of the other federated UEs.

The number of UEs using the same public user identity is implementation specific.

NOTE: In case federated UEs use common implicit registration set, all federated UEs will subscribe to the registration-state event package and will receive notifications related to all public user identities in this implicit registration set.

If the user of the MuD service also subscribes to the MiD service then the user can use non-native identities in addition to native identities on federated UEs. A federated UE can indicate to the network which of these non-native identities are (de)activated at the federated UE.

4.2.2 MiD service description

The MiD service enables a served user to use any of its identities i.e. native and non-native identities for communication using a single UE. A native identity is always registered by the UE. An alternative identity and a virtual identity can be either registered by the UE, or the UE can be authorized to use these identities based on configuration in the user's service data. An external alternative identity cannot be registered by the UE, but the UE can be authorized to use this identity based on configuration in the user's service data.

NOTE: The identity registered by the UE is received in the P-Associated-URI header field within 200 (OK) response during registration. The identity not registered but authorized to be used by the UE is configured in the user's service data.

When making a call the served user selects one of its identities that will be used by the UE as an originating identity (calling party number) in an outgoing call. Upon reception of an incoming call the UE provides to the served user an indication on which of its identities the served user is contacted (called party number).

The UE can indicate to the network which identities are active at the UE. A native identity is always active at the UE.

Several users of the MiD service can share the same non-native identity for communication.

The number of non-native identities used by a user using a single UE is implementation specific.

If the user of the MiD service also subscribes to the MuD service then the user can use non-native identities on federated UEs. In such case, the UE can indicate to the network which of these non-native identities are active at each federated UE separately.

4.3 Operational requirements

4.3.1 Provision/withdrawal

The MiD service and the MuD service are provided after prior arrangement with the service provider.

The MiD service and the MuD service are withdrawn at the served user's request or for administrative purposes.

4.3.2 Requirements on the originating network side

For the MiD service, the originating network shall support the Additional-Identity header field.

For the MuD service the originating network shall support using a token to identify the registration as specified in TS 24.229 [3].

4.3.3 Requirements in the network

For the MiD service, a network serving an external alternative identity shall support adding the Additional-Identity header field.

For the MuD service no specific requirements are needed in the network.

4.3.4 Requirements on the terminating network side

For the MiD service, the terminating network shall support the Additional-Identity header field.

For the MuD service the terminating network shall support using a token to identify the registration as specified in TS 24.229 [3].

4.4 Coding requirements

No specific coding requirements are defined in the present document.

4.5 Signalling requirements

4.5.1 General

Configuration of the MiD services by the user should take place over the Ut interface using XCAP as enabling protocol as described in TS 24.623 [7].

NOTE: Other possibilities for user configuration, such as web-based provisioning or pre-provisioning by the operator are outside the scope of the present document, but are not precluded.

The enhancements to the XML schema for use over the Ut interface is described in clause 4.8.

4.5.2 Activation/deactivation of MuD/MiD services

4.5.2.1 General

The services and individual identities can be activated or deactivated following procedures in the following clauses.

4.5.2.2 Activation of MuD and MiD services

The MuD and MiD services are activated at provisioning and deactivated at withdrawal or at the user's request.

If the MuD, MiD or both services are activated, the user controls whether identities can be used for incoming and outgoing calls by activation/deactivation of identities.

4.5.2.3 Activation/deactivation of identities

Via activation/deactivation of identities in case of MiD service, the user controls if the identity is active on its device. Via activation/deactivation of identities in case of MuD service, the user controls if the identity is active on each device in federation separately. If the user of MuD service is also using MiD service, the user controls if each identity is active on each device separately. There is a separate <ue-instance> element for each of the device, distinguishable by the "identity" attribute. The "identity" attribute takes the form of a pvalue as derfined in IETF RFC 3261 [15] and can be set by the operator to a value linked with the IMS private user identity. The "alias" attribute is modifiable by the user and is filled with a user-friendly identifier making the UE instance easier distinguishable among all the devices in federation.

The user of MuD, MiD or both services decides which of the identities that it is allowed to use and can be registered are active and can be used for incoming and outgoing calls by changing the "Activated" attribute in the <Registered-identity> elements in the service configuration data.

The user of MiD service decides which of the identities that have been allowed to be used for the user but cannot be registered are active and can be used for incoming and outgoing calls by changing the "Activated" attribute in the <Shared-identity> elements in the service configuration data.

The user decides if it permits another user to use its native identity. The user decides which users among those who have been allowed to use its identity, can use this identity for incoming and outgoing calls by changing the "Activated" attribute in the <Delegated-user> elements in the service configuration data.

4.5.3 Invocation and operation

4.5.3.1 Actions at the UE of user A

4.5.3.1.1 General

If user A wishes to use a native identity, the UE shall include in the outgoing INVITE or MESSAGE request the From header field and may include the P-Preferred-Identity header field(s) as specified in TS 24.229 [3]. The From header field and the P-Preferred-Identity header field (if included) shall contain the native identity.

If user A wishes to use an alternative identity or a virtual identity that the UE has registered, the UE shall include in the outgoing INVITE or MESSAGE request the From header field and the P-Preferred-Identity header field. The P-Preferred-Identity header field and the From header field shall contain the alternative identity or the virtual identity.

If user A wishes to use the identity C, the UE shall include in any outgoing INVITE or MESSAGE requests, an Additional-Identity header field, defined in TS 24.229 [3], set to the selected identity and shall include the native identity in the From header field. The UE can learn the identity C by device configuration as specified in TS 24.175 [13] or by using the service configuration in clause 4.8.

The UE may support being configured with the identities to be used using one or more of the following methods:

a) the "MultiIdentity" interior node of the $EF_{MuDMiDConfigData}$ file described in TS 31.102 [xx];

b) the "MultiIdentity" interior node of the $EF_{MuDMiDConfigData}$ file described in TS 31.103 [yy]; and

c) the "MultiIdentity" interior node of TS 24.175 [13].

If the UE is configured with both the "MultiIdentity" interior node of TS 24.175 [13] and the "MultiIdentity" interior node of the $EF_{MuDMiDConfigData}$ file described in TS 31.102 [xx] or TS 31.103 [yy], then the Media_type_restriction_policy node of the $EF_{MuDMiDConfigData}$ file shall take precedence.

NOTE: Precedence for files configured on both the USIM and ISIM is defined in TS 31.103 [yy].

When establishing an emergency session and performing the emergency related procedures defined in TS 24.229 [3], the UE shall only use the native identity.

A UE supporting the MuD service may synchronize the local call log with the network stored call log as specified in OMA-TS-CPM_Message_Storage_Using_RESTFul_API [9] and OMA-TS-REST_NetAPI_NMS [10]. If the served user in the "From" header field is an identity not registered by the UE, the UE shall deduce that the call was originated using the Additional-Identity header field.

4.5.3.1.2 Call pull handling

The UE may pull a session from another federated UE by performing the following steps:

NOTE: In this Release of the present document no procedure is specified to receive consent from the UE the call is pulled from.

a) the UE learns about the session to pull by subscribing to the dialog event package, specified in RFC 4235 [16];

b) the UE sends an INVITE request towards the far end populated as follows:

   1) the Request-URI is set to the uri in the <target> element of the <remote> element;

   2) a Replaces header field containing the dialog identifiers contained as attributes in the <dialog> element of the <dialog-info> element; and

   3) any other header field or body as determined by the service logic; and

c) when the UE receives a response to the INVITE request above the UE follows general procedures in TS 24.229 [3].

4.5.3.1.3 Call push handling

The UE may push a session to another federated UE by performing the following steps:

a) the UE learns the status and identities of the other federated UEs using the dialog event package, specified in RFC 4235 [16] and extended as specified in clause 7.X.2 in TS 24.229 [3]; and

b the UE sends a REFER request towards the target UE populated as follows:

NOTE 1: In this Release of the present document only one UE is targeted in the transfer.

1) the Request-URI is set to the own public user identity and includes a "gr" SIP URI parameter set to the value of the "identity" attribute for the target UE received in the <ue-instance> element in the <dialog-info> element in the dialog event notification; and

NOTE 2: The value in the "identity" attribute has the same format as a GRUU, but is not a GRUU assigned by the S-CSCF. It only has local significance.

2) a Refer-to header field set to the SIP URI of the remote end and including in the headers portion of the SIP URI the headers and bodies determined by the service logic.

4.5.3.2 Actions at the AS serving user A

4.5.3.2.1 General

Upon receiving an incoming initial INVITE, REFER or MESSAGE request containing an Additional-Identity header field, the AS shall determine the served user as specified in TS 24.229 [3] clause 5.7.1.3A.2 and shall check if any of the served user's registered identities is also included in the Additional-Identity header field. If the Additional-Identity header field contains a served user's registered identity the AS shall remove the Additional-Identity header field from the request and shall forward the request in accordance with procedures defined in TS 24.229 [3]. Otherwise, if the received Additional-Identity header field does not contain any of the served user's registered identities the AS shall:

a) verify that the user is authorized to use the identity received in the Additional-Identity header field as specified in clause 4.5.3.2.2; and

b) if the user is not authorized to use the identity included in the Additional-Identity header field, then the AS shall reject the incoming request. The originating request may be rejected by operator policy with a 403 (Forbidden) response including a warning header field 399 "Identity not allowed".

If the user is authorized to use the identity in the Additional-Identity header field then the AS shall generate a new SIP request based on the received SIP request in accordance with the procedures in TS 24.229 [3] clause 5.7.3 with the following clarifications:

a) remove any P-Served-User header field and insert a P-Served-User header field with the identity taken from the Additional-Identity header field in the received request;

b) remove any existing Route header field and insert a Route header field pointing to an I-CSCF or to the S-CSCF hosting the identity in the Additional-Identity header field in the received request;

c) in the Route header field above, append the "orig" parameter to the URI; and

d) insert the Additional-Identity header field with the same value as in the received SIP request.

The AS shall send the generated SIP request and may refrain from the invocation of other MMTel services serving the native identity.

NOTE: No specific procedures are needed regarding the Identity header field. The originating network can attest the identity of user A following normal procedures specified in TS 24.229 [3].

If the AS updates the Call Log as specified in OMA-TS-CPM_Message_Storage_Using_RESTFul_API [9] the AS shall populate the "From" attribute of the call log object with the value in the Additional-Identity header field, provided the user is authorized to use this identity.

4.5.3.2.2 Authorization of the Additional-Identity header field

The AS serving user A shall authorize the usage of the identity contained in the Additional-Identity header field as the originating identity by checking:

- if the identity contained in the Additional-Identity header field is included in the user's service data associated to the native identity of the originating user; and
- if the "Activated" attribute of the <Shared-identity> element of the <multi-identity> element in the service configuration data is set to "true".

Otherwise, user A is not authorized to use the identity contained in the Additional-Identity header field as the originating identity.

4.5.3.2.3 Call pull handling

An AS supporting call pull handling, when receiving an INVITE request as specified in clause 4.5.3.1.2 shall verify that the calling user is allowed to pull a call. If the call pull is allowed, the AS forwards the received INVITE request in accordance with TS 24.229 [3], otherwise the AS rejects the request with an appropriate response code.

4.5.3.2.4 Call push handling

An AS supporting call push handling, when receiving a REFER request as specified in clause 4.5.3.1.3 shall

a) verify that the user is allowed to push a call; and

b) if the call push is allowed, based on local policy, either

   1) forward the REFER request towards the REFER target; or

   2) start 3pcc procedures as specified in TS 24.628 [17] to:

      A) transfer the originating leg from the originator of the REFER reqeust to the REFER target; and

      B) if necessary, update the terminating leg.

The AS shall use the "gr" SIP URI parameter in the Request-URI to identify the REFER target UE. If the AS knows that the content of the "gr" SIP URI parameter is not a GRUU assigned by the S-CSCF the AS shall remove the "gr" SIP URI parameter from the Request-URI before forwarding the request.

4.5.3.3 Actions at the AS serving identity C

Upon receiving an incoming INVITE or MESSAGE request containing an Additional-Identity header field, the AS shall:

a) determine the served user as defined in TS 24.229 [3];

b) if the user identified in the P-Asserted-Identity is not allowed to use the identity in the Additional-Identity header field, reject the request using a 403 (Forbidden) response including a warning header field 399 "Identity not allowed" and skip the rest of the steps;

c) replace the identity in the From header field with the identity in the Additional-Identity header field;

d) depending on local configuration, related to the operator policy and regulatory requirements, allowing to determine whether an originating external alternative identity or an originating virtual identity is to be used as an originating identity (calling party number):

   1) if the P-Asserted-Identity header can be modified, replace the identity in the P-Asserted-Identity header field with the identity in the Additional-Identity header field; or

   2) if the P-Asserted-Identity header cannot be modified, set the Privacy header field "id" to keep the native identity private in the P-Asserted-Identity header field as defined in IETF RFC 3325 [6];

e) if the identity of the originating user can be verified, based on local policy initiate addition of an Identity header field attesting the identity C;

f) remove the Additional-Identity header field received in the request; and

g) perform any other originating services as performed by the service logic,

before forwarding the request downstream.

4.5.3.4 Actions at the AS serving identity D

For a terminating user, upon receiving an incoming INVITE or MESSAGE request, the AS shall perform any terminating services as performed by the service logic before forwarding the request downstream.

If the AS service determines based on configuration that the AS shall forward the request to any of the identities that can use the identity received in the Request-URI, the AS shall for each forwarded request modify the request as follows:

a) the Request-URI is set to the identity configured in the AS; and

b) an Additional-Identity header field, defined in TS 24.229 [3], is added and set to the identity received in the Request-URI.

If the AS supports calling number verification using signature verification and attestation information as specified in TS 24.229 [3], the AS treats the forwarding to the identities above as diversions, i.e. uses the "div" PASSporT as specified in IETF RFC 8946.

If the AS identifies the INVITE request as a PSAP callback, the MiD service shall not be triggered.

4.5.3.5 Actions at the AS serving user B

Upon receiving an INVITE or MESSAGE request not containing an Additional-Identity header field and if the terminating user is subscribed to the MuD service, the AS shall when sending the request to the UEs verify whether the identity in the Request-URI is activated by the MiD service and on the target UE. The AS shall only send the request to a target UE if the identity is active both in the MiD service and on the target UE. If the user does not subscribe to the MiD service, but the user has the received identity configured in the implicit registration set, the AS considers the identity to be activated by the MiD service.

Upon receiving an INVITE or MESSAGE request containing an Additional-Identity header field and if the terminating user is subscribed to the MuD and the MiD service, the AS shall when sending the request to the UEs verify whether the identity in the Additional-Identity header field is activated by the MiD service and on the target UE. The AS shall only send the request to a target UE if the identity is active both in the MiD service and on the target UE. The AS may refrain from the invocation of other MMTel services configured for the user of the native identity.

If the AS updates the Call Log as specified in OMA-TS-CPM_Message_Storage_Using_RESTFul_API [9] the AS shall populate the "To" attribute of the call log object with the value in the Additional-Identity header field, provided the user is authorized to use this identity.

An AS supporting call pull and call push handling, uses the procedures specified in clauses 4.5.3.2.3 and 4.5.3.2.4.

4.5.3.6 Actions at the UE of user B

A UE supporting the MiD service shall support the receipt of the Additional-Identity header field, defined in TS 24.229 [3], in SIP requests initiating a dialog or standalone transaction.

NOTE: The UE finds a targeted external alternative identity in the Additional-Identity header field.

A UE supporting the MuD service may synchronize the local call log with the network stored call log as specified in OMA-TS-CPM_Message_Storage_Using_RESTFul_API [9] and OMA-TS-REST_NetAPI_NMS [10]. If the served user in the "To" header field is an identity not registered by the UE, the UE shall deduce that the call was originated using the Additional-Identity header field.

A UE supporting call pull and call push handling uses the procedures specified in 4.5.3.1.2 and 4.5.3.1.3.

4.6 Service interactions

4.6.1 Originating Identification Presentation (OIP)

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

4.6.2 Originating Identification Restriction (OIR)

No impact.

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

4.6.3.1 MuD

No impact.

4.6.3.2 MiD

For TIP, the AS serving identity D shall in SIP responses remove the P-Asserted-Identity header field received from UE-B and insert a P-Asserted-Identity identifying the served user.

For TIR, the AS serving identity D shall pass any Privacy header field unchanged towards the originating user.

4.6.4 Advice of Charge

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

4.6.5 Communication Waiting (CW)

For MuD, if there are ongoing communications, it is a service option whether to send an incoming initial INVITE to all federated UEs or only those UEs with ongoing communications.

For MiD, no impact.

4.6.6 Communication Hold

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

4.6.7 Explicit Communication Transfer (ECT)

4.6.7.1 Interactions for MuD service

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

4.6.7.2 Interactions for MiD service

4.6.7.2.1 Actions at the UE acting as transferor

When the UE initiates a communication transfer, the UE shall use the same identity in the Referred-By header field as was indicated for the established session. If the UE uses identity C or identity D for the established session, the UE shall add the Addditional-Identity header field containing this identity.

4.6.7.2.2 Actions at the AS serving the transferor

4.6.7.2.2.1 Identifying a request for communication transfer

See TS 24.629 [11] on the criteria to determine that a REFER request is to be treated as a request for transfer of an existing communication.

4.6.7.2.2.2 Handling of transfer requests

When a REFER request identified as a request for transfer is received from the served user and the Additional-Identity header field is included in the REFER request the AS shall authorize the use of the Additional-Identity header field as specified in clause 4.5.3.2.2. If the user is authorized to use the Additional-Identity header field the AS shall forward the REFER request as follows:

a) if the REFER request was received inside the dialog, the AS forwards the request in the existing dialog towards the transferee; or

b) if the REFER request was received outside the existing dialog, as specified in TS 24.629 [11], the AS forwards the REFER request towards the transferee with the same considerations as specified for an initial INVITE request in clause 4.5.3.2.1.

4.6.7.2.2.3 Actions at the AS serving the identity C or identity D

When a REFER request identified as a request for transfer that contains an Additional-Identity header field containing a URI of the served user is received the AS shall in addition to the procedures in clause 4.5.3.3 verify that the Referred-By header field is consistent with the Additional-Identity header field, and if necessary replace the Referred-By header field value with the identity in the received Additional-Identity header field. The AS then forwards the REFER request following normal procedures.

4.6.8 Conference calling (CONF)

4.6.8.1 Interactions for MuD service

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

4.6.8.2 Interactions for MiD service

4.6.8.2.1 UE procedures for MiD service

To be able to later use the CONF service, when the UE sends an INVITE request to a second user, the UE shall use the same identity as the UE used when setting up the first communication.

When creating the conference with an INVITE request the UE shall use the same identity as the UE used in the communications now on HOLD. If the UE uses identity C or identity D for the established sessions, the UE shall add the Addditional-Identity header field containing this identity. The UE sets the Request-URI to the same conference factory URI as the UE uses for the native identities.

When the UE adds a conference participant using the procedures in clause 5.3.1.5.3 in TS 24.147 [12], the UE shall set the Referred-By header field in the REFER request to the same identity as the one used when creating the original session(s). If this identity is a non-registered identity (identity C or identity D) the UE adds the Additional-Identity header field containing this identity.

4.6.8.2.2 Actions at the AS serving the conference call initiator

If the AS receives an INVITE request with a Request-URI to a conference factory used in the serving network and an Additional-Identity header field, the AS in addition to the procedures in clause 4.5.3.2.1 replaces the Request-URI with a default conference factory URI for MMTel (as specified in TS 23.003 [14]) valid in the home network of the identity in the Additional-Identity header field.

4.6.8.2.3 Actions at the AS serving the identity C or identity D

If the AS receives an INVITE request, addressed to a default conference conference factory URI for MMTel as specified in TS 23.003 [14], including an Additional-Identity header field the AS may in additon to the procedures in clause 4.5.3.3 modify the Request-URI to include any conference factory URI of the serving network.

If the AS receives a REFER request containing an Additional-Identity header field, the AS shall in additon to the procedures in clause 4.5.3.3 verify that the identity in the Referred-By header field is consistent with the Additional-Identity header field, and if necessary replace the Referred-By header field value with the identity in the received Additional-Identity header field. The AS then forwards the REFER request following normal procedures.

4.6.9 Closed User Group (CUG)

For MuD no impact, i.e. neither service shall affect the operation of the other service.

For MiD, CUG imposes restrictions on both incoming and outgoing calls. The MiD shall not use any identity C or identity D that are restricted by the CUG service.

4.6.10 Completion of Communications to Busy Subscriber (CCBS)

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

4.6.11 Communication Diversion (CDIV)

At the AS serving the user holding the terminating external alternative or virtual identity, the CFU (communication forwarding unconditional) take precedence over execution of MiD and MuD services.

At the terminating side, it is implementation specific to select CDIV service when different CDIV services apply to different federated UEs.

4.6.12 Malicious Communication Identification (MCID)

NOTE: When the originating user has a MiD service invoked and if the operator policy and regulatory requirements state that for the originating request the P-Asserted-Identity header cannot be modified, identities from the P-Asserted-Identity header field and From header field stored by MCID service represent different users.

4.6.13 Anonymous Communication Rejection (ACR) and Communication Barring (CB)

The Incoming Communications Barring (ICB), Outgoing Communications Barring (OCB) and Anonymous Call Rejection (ACR) of the non-native identity take precedence over MuD and MiD services.

4.6.14 Message Waiting Indication (MWI)

In case of the MuD service, there is no impact on the operation of the other service.

The MWI is not supported for the identities, which are shared.

4.6.15 Flexible Alerting (FA)

MuD service can be combined with FA with no impacts.

Terminating MiD service is competing with FA.

4.6.16 Enhanced Calling Name (eCNAM)

In case of the MuD service, if the terminating user with MuD service has eCNAM activated, incoming calls to an identity shall apply eCNAM to all federated UEs.

4.6.17 Multi-Device (MuD)

When a user has the MiD service, any external alternative or virtual identity that is authorized to be used and activated by the MiD service can be activated on any of the Federated UEs as part of the user's MuD service.

4.6.18 Multi-Identity (MiD)

No impact. The activation of an identity by the MiD service is a condition for that identity to be active on a federated UE by the MuD service.

4.6.19 Customized Alerting Tones (CAT)

No impact.

4.6.20 Customized Ringing Signal (CRS)

No impact.

4.7 Parameter values and timers

No parameters and timers are defined in the present document.

4.8 Service configuration for multi-device and multi-identity

4.8.1 General

The multi-device and multi-identity documents are subtrees of the *simservs* document specified in TS 24.623 [7]. As such, multi-device and multi-identity documents use the XCAP application usage in TS 24.623 [7].

XML schema: Implementations in compliance with the present document shall implement the XML schema that minimally includes the XML schema defined in clause 4.8.2 and the *simservs* XML schema specified in TS 24.623 [7].

Data semantics: The semantics of the multi-device and multi-identity XML configuration document is specified in clause 4.8.3.

The UE can only read the MuD and MiD configuration document and modify the "Activated" attribute of the <Registered-identity>,<Shared-identity> and <Delegated-user> elements.

4.8.2 XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ss="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
targetNamespace="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
elementFormDefault="qualified"
attributeFormDefault="unqualified" >
  <xs:include schemaLocation="XCAP.xsd"/>
  <xs:element name="multi-device" substitutionGroup="ss:absService">
    <xs:annotation>
      <xs:documentation>Element describing the multi-device specific features for a given UE
instance</xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:complexContent>
        <xs:extension base="ss:simservType">
          <xs:sequence>
            <!-- Element identitifying the UE among federated UEs, containing the attributes
"identity" for IMPI and "alias" for user friendly name) -->
            <xs:element name="ue-instance" minOccurs="1" maxOccurs="unbounded">
              <xs:complexType>
```

```
                <xs:sequence>
  <!-- Element containing the identity the UE can use, which can be registered -->
                  <xs:element name="Registered-identity" type="ss:Registered-identityType"
minOccurs="1" maxOccurs="unbounded"/>
  <!-- Element containing the identity the UE can use since it is shared with it -->
                  <xs:element name="Shared-identity" type="ss:Shared-identityType" minOccurs="0"
maxOccurs="unbounded"/>
                </xs:sequence>
                <xs:attribute name="identity" type="xs:string"/>
                <xs:attribute name="alias" type="xs:string"/>
              </xs:complexType>
            </xs:element>
          </xs:sequence>
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>
  </xs:element>
  <xs:element name="multi-identity" substitutionGroup="ss:absService">
    <xs:annotation>
      <xs:documentation>Element describing the multi-identity specific features</xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:complexContent>
        <xs:extension base="ss:simservType">
          <xs:sequence>
  <!-- Element containing the delegated identity, i.e., which can use the identity of the UE since
it is shared with it -->
            <xs:element name="Delegated-user" type="ss:Delegated-userType" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>
  </xs:element>
  <xs:complexType name="Registered-identityType">
    <xs:simpleContent>
      <xs:extension base="xs:anyURI">
        <xs:attribute name="Activated" type="xs:boolean" default="true"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
  <xs:complexType name="Shared-identityType">
    <xs:simpleContent>
      <xs:extension base="xs:anyURI">
        <xs:attribute name="Activated" type="xs:boolean" default="true"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
  <xs:complexType name="Delegated-userType">
    <xs:simpleContent>
      <xs:extension base="xs:anyURI">
        <xs:attribute name="Activated" type="xs:boolean" default="true"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
</xs:schema>
```

4.8.3 Semantics

4.8.3.1 General

This clause contains the description of the data elements in the XML schema.

4.8.3.2 multi-device element

This is a root element for elements related to MuD service. This element contains one or more occurrences of <ue-instance> element.

The <ue-instance> element represents the instance of the UE. If the user of the UE is subscribed to the MuD service, there is a dedicated element per each of the devices within MuD. This element has following attributes:

- "identity" – a unique identity allowing to distinguish the UEs within the user's federated UEs. The "identity" value shall take the form of a pvalue as defined in IETF RFC 3261 [15] and is derived from the IMS private user identity using the name-based UUID algorithm specified in RFC 4122 [18]. The hash algorithm shall be SHA-1.;
- "alias" – a user friendly identifier of given UE instance.

NOTE: A single <ue-instance> element exists even if the user did not subscribe to MuD service, but is using MiD service on a single UE.

Each <ue-instance> element contains one or more <Registered-identity> element, containing the identity, which can be registered by a given UE instance. The identity has an attribute associated, which indicates if the identity can be used for incoming and outgoing communication.

Each <ue-instance> element contains zero or more occurrences of <Shared-identity> element, containing the shared identity for a given UE instance. The identity has an attribute associated, which indicates if the identity can be used for incoming and outgoing communication.

4.8.3.3 multi-identity element

This is a root element for elements related to MiD service. This element contains zero or more occurrences of <Delegated-user> element.

The <Delegated-user> element contains the delegated identity that is allowed to use the native identity. The identity has an attribute associated, which indicates if the user of delegated identity can use the native identity for incoming and outgoing communication.

Annex A (informative): Call Flows

A.1 Introduction

A.1.1 Call flow overview

This annex contains originating and terminating call flow examples for the following use cases:

- Originating flow when user A uses a non-native identity A1 registered by the UE.
- Originating flow when user A uses an identity C.
- Terminating flow when user B is reached by an identity D.
- Terminating flow when user B is reached by a native identity on multiple devices.
- MuD call flow: subscription to notifications of network call log changes.
- MuD call flow: synchronization of list of outgoing calls.
- MuD call flow: synchronization of missed call notifications.

A.1.2 Identity conventions used in this annex

A native identity is designated A-or B-in the flows for originating and terminating users, respectively. In the coding examples tel:+11111111 is used for originating native identities and tel:+11112222 is used for terminating native identities. For originating user A, a non-native identity registerd by the UE is designated A1 in the flows. In the coding examples, for simplicity reason, tel:+11111111 is also used in case of originating non-native registered identity.

Identity C and D are used in the flows for originating and terminating users, respectively. In the coding examples tel:+22221111 is used for originating non-registered identities and tel:+22222222 is used for terminating non-registered identities.

A.2 Originating call flows

A.2.1 UE-A indicates a non-native identity A1 registered by the UE

This call flow illustrates the handling of the identity A1 registered by the UE for originating call.

It applies to the cases when alternative identity registered by the UE or virtual identity registered by the UE is used.

In this case, only the AS of user A is involved on the originating side.

NOTE: A deployment option where the UE-A indicates an identity not registered by the UE and only the AS serving user A is involved is out of the scope of this specification.

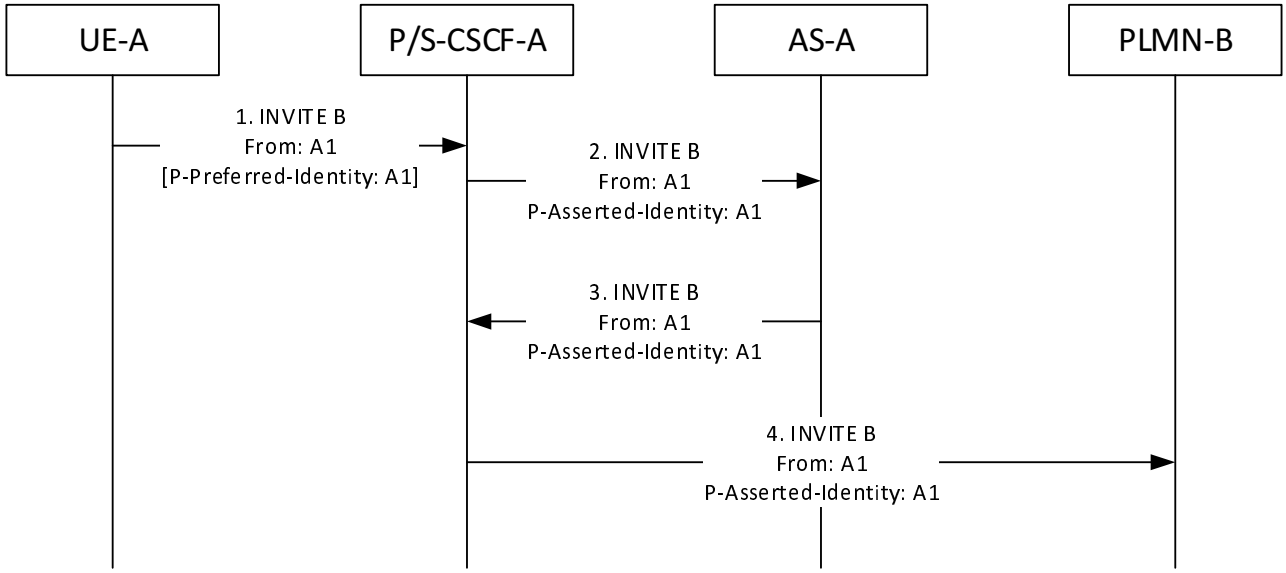

Figure A.2.1-1: UE-A indicates a non-native identity A1 registered by the UE

1. **UE-A sends an INVITE message to P/S-CSCF-A, for an example see table A.2.1-1**

   The UE-A includes in the initial INVITE request the From header field and the P-Preferred-Identity header field set to the identity A1 registered by the UE and sends the initial INVITE request to the P/S-CSCF-A according to TS 24.229 [3].

Table A.2.1-1: INVITE request (UE-A to P/S-CSCF-A)

```
INVITE tel:+11112222 SIP/2.0

To: <tel:+11112222>
From: <tel:+11111111>;tag=4fa3
P-Preferred-Identity: <tel:+11111111>

Other SIP header fields and SDP according to 3GPP TS 24.229 [3]
```

2. **P/S-CSCF-A forwards the INVITE message to AS-A, for an example see table A.2.1-2**

   The P-CSCF-A populates the P-Asserted-Identity header field with the identity A1 registered by the UE following procedures defined in TS 24.229 [3].

   The S-CSCF-A forwards the request to the AS-A using initial filter criteria.

Table A.2.1-2: INVITE request (P/S-CSCF-A to AS-A)

```
INVITE tel:+11112222 SIP/2.0

To: <tel:+11112222>
From: <tel:+11111111>;tag=4fa3
P-Asserted-Identity: <sip:+11111111@plmnA.net;user=phone>, <tel:+11111111>

Other SIP header fields and SDP according to 3GPP TS 24.229 [3]
```

3. **AS-A forwards the INVITE message to the S-CSCF-A, for an example see table A.2.1-3**

   AS-A performs originating services as needed and forwards the request to the S-CSCF-A according to TS 24.229 [3].

Table A.2.1-3: INVITE request (AS-A to P/S-CSCF-A)

```
INVITE tel:+11112222 SIP/2.0

To: <tel:+11112222>
```

```
From: <tel:+11111111>;tag=4fa3
P-Asserted-Identity: <sip:+11111111@plmnA.net;user=phone>, <tel:+11111111>

Other SIP header fields and SDP according to 3GPP TS 24.229 [3]
```

4. **S-CSCF-A forwards the INVITE message towards the PLMN-B**

A.2.2 UE-A indicates an identity C

This alternative is applicable to the cases when the UE-A indicates an identity which has not been registered by UE-A (i.e., it applies to the cases when UE-A indicates an alternative identity not registered by the UE or a virtual identity not registered by the UE) or an external alternative identity.

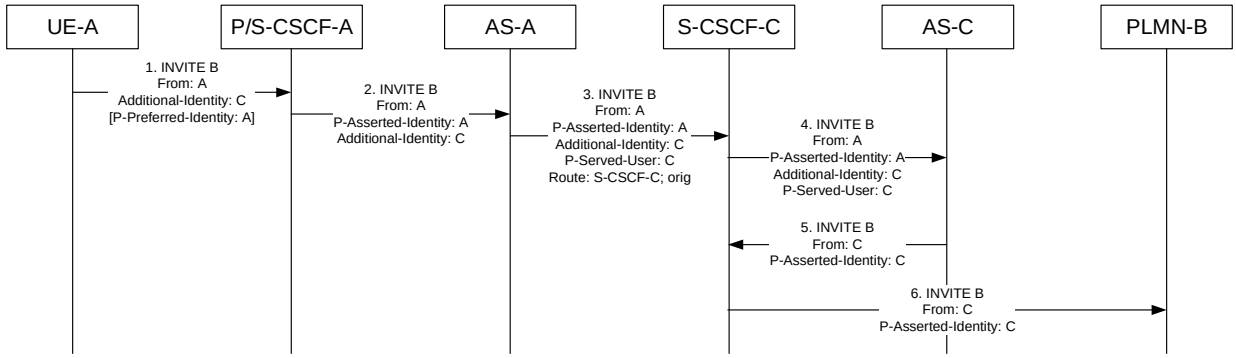

Figure A.2.2-1: UE-A indicates an identity C

1. **UE-A sends an INVITE message to P/S-CSCF-A, for an example see table A.2.2-1**

   User A at UE-A initiates a call on behalf of the identity C. The UE-A includes the Additional-Identity header field in the initial INVITE request to indicate that the user of UE-A wishes to use the identity C for this call, the From and the P-Preferred-Identity header fields set to the native identity and sends the initial INVITE request to the P/S-CSCF-A according to TS 24.229 [3].

NOTE 1: According to procedures defined in TS 24.229 [3] the P-Preferred-Identity header field can be omitted.

Table A.2.2-1: INVITE request (UE-A to P/S-CSCF-A)

```
INVITE tel:+11112222 SIP/2.0

To: <tel:+11112222>
From: <tel:+11111111>;tag=4fa3
Additional-Identity: <tel:+22221111>
P-Preferred-Identity: <tel:+11111111>

Other SIP header fields and SDP according to 3GPP TS 24.229 [3]
```

2. **S-CSCF-A forwards the INVITE message to AS-A, for an example see table A.2.2-2**

   The P-CSCF-A populates the P-Asserted-Identity header field with the native identity following procedures defined in TS 24.229 [3].

   The S-CSCF-A forwards the request to the AS-A using initial filter criteria.

Table A.2.2-2: INVITE request (P/S-CSCF-A to AS-A)

```
INVITE tel:+11112222 SIP/2.0

To: <tel:+11112222>
From: <tel:+11111111>;tag=4fa3
P-Asserted-Identity: <sip:+11111111@plmnA.net;user=phone>, <tel:+11111111>
Additional-Identity: <tel:+22221111>
```

```
Other SIP header fields and SDP according to 3GPP TS 24.229 [3]
```

3. **AS-A forwards the INVITE message to the S-CSCF-C, for an example see table A.2.2-3**

   AS-A verifies that the user is authorized to use the identity received in the Additional-Identity header field and if so, it does not modify the P-Asserted-Identity header field, it creates a P-Served-User header field with the identity copied from the received Additional-Identity header field and it insert a Route header field pointing to an I-CSCF or to the S-CSCF hosting the identity in the Additional-Identity header field and append the "orig" parameter to it. AS-A performs the originating services as needed and forwards the request to the S-CSCF-C.

Table A.2.2-3: INVITE request (AS-A to S-CSCF-C)

```
INVITE tel:+11112222 SIP/2.0

To: <tel:+11112222>
From: <tel:+11111111>;tag=4fa3
P-Asserted-Identity: <sip:+11111111@plmnA.net;user=phone>, <tel:+11111111>
Additional-Identity: <tel:+22221111>
P-Served-User: <tel:+22221111>
Route: <sip:server-C.plmnA.net; orig>

Other SIP header fields and SDP according to 3GPP TS 24.229 [3]
```

4. **S-CSCF-C forwards the INVITE message to AS-C, for an example see table A.2.2-4**

   The S-CSCF-C removes the Route header field pointing to it and forwards the request to the AS-C using initial filter criteria.

Table A.2.2-4: INVITE request (S-CSCF-C to AS-C)

```
INVITE tel:+11112222 SIP/2.0

To: <tel:+11112222>
From: <tel:+11111111>;tag=4fa3
P-Asserted-Identity: <sip:+11111111@plmnA.net;user=phone>, <tel:+11111111>
Additional-Identity: <tel:+22221111>
P-Served-User: <tel:+22221111>

Other SIP header fields and SDP according to 3GPP TS 24.229 [3]
```

5. **AS-C forwards the INVITE message to the S-CSCF-C, for an example see table A.2.2-5**

   AS-C verifies that the identity C received in the Additional-Identity header field has been authorized to be used by user A. If it is the case, it creates the P-Asserted-Identity header field with the identity copied from the received Additional-Identity header field and performs originating services as needed. AS-C replaces the identity in the From header field with the identity copied from the received Additional-Identity header field, removes from the INVITE request the received P-Asserted-Identity, P-Served-User and Additional-Identity header fields and forwards the request to the S-CSCF-C according to TS 24.229 [3].

NOTE 2: Depending on local configuration, related to the operator policy and regulatory requirements, AS-C replaces the identity in the P-Asserted-Identity header field with the identity in the Additional-Identity header field, or if the P-Asserted-Identity header cannot be modified, AS-C sets the Privacy header field to value "id", as specified in clause 4.5.3.3.

Table A.2.2-5: INVITE request (AS-C to S-CSCF-C)

```
INVITE tel:+11112222 SIP/2.0

To: <tel:+11112222>
From: <tel:+22221111>;tag=4fa3
P-Asserted-Identity: <sip:+22221111@plmnA.net;user=phone>, <tel:+22221111>

Other SIP header fields and SDP according to 3GPP TS 24.229 [3]
```

6. **S-CSCF-C forwards the INVITE message towards the PLMN-B**

A.3 Terminating flows

A.3.1 UE-B reached by identity D

This call flow illustrates the handling of an identity for terminating calls not registered by UE-A. For simplicity the CSCF nodes have been omitted.

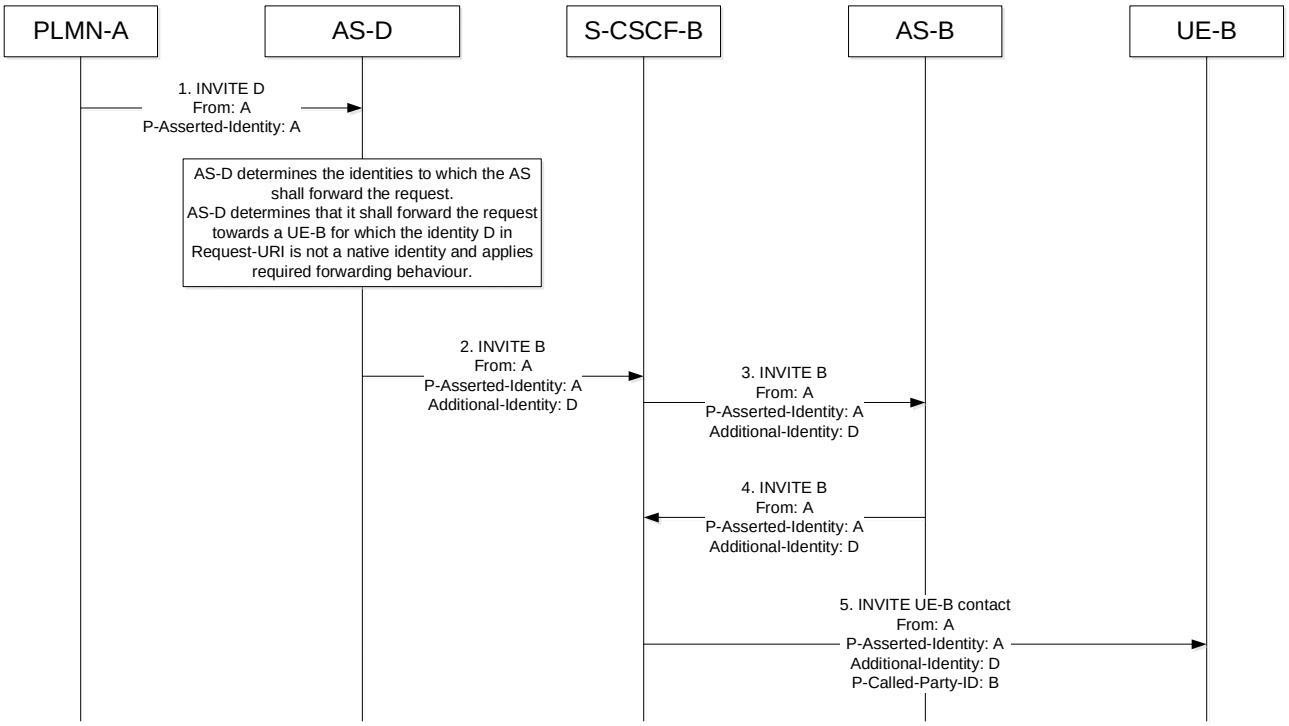

Figure A.3.1-1: UE-B reached by an identity D

1. **AS-D receives an INVITE message from PLMN-A, for an example see table A.3.1-1**

   The Request-URI identifies the target user as D. Based on that, AS-D determines the identities to which it shall forward the request.

   The AS-D determines that this request needs to go to UE-B for which the identity in Request-URI is not a native identity and it applies required forwarding behavior, as part of the MiD service.

   The AS-D also sends this message to UE(s) of the user owning identity D following procedures defined in TS 24.229 [3].

   The AS-D sets the Request-URI to identity B and adds an Additional-Identity header field set to identity D.

Table A.3.1-1: INVITE request (PLMN-A to AS-D)

```
INVITE tel:+22222222 SIP/2.0

To: <tel:+22222222>
From: <tel:+11111111>;tag=4fa3
P-Asserted-Identity: <sip:+11111111@plmnA.net;user=phone>, <tel:+11111111>

Other SIP header fields and SDP according to 3GPP TS 24.229 [3]
```

2. **AS-D forwards the INVITE message towards S-CSCF-B, for an example see table A.3.1-2**

Table A.3.1-2: INVITE request (AS-D to S-CSCF-B)

```
INVITE tel:+11112222 SIP/2.0
```

```
To: <tel:+22222222>
From: <tel:+11111111>;tag=4fa3
P-Asserted-Identity: <sip:+11111111@plmnA.net;user=phone>, tel:+11111111
Additional-Identity: <tel:22222222>

Other SIP header fields and SDP according to 3GPP TS 24.229 [3]
```

3. **S-CSCF-B forwards the INVITE message to AS-B**

- AS-B performs terminating services.

4. **-AS-B forwards the INVITE message to S-CSCF-B**

5. **S-CSCF-B forward the INVITE message to UE-B**

   S-CSCF-B replaces B identity with the UE-B contact in the Request-URI and adds a P-Called-Party-ID header field.

   UE-B determines from the Additional-Identity header field that it has been reached using the identity D. The P-Called-Party-Id header field can be ignored.

A.3.2 UE-B reached by native identity on multiple devices

This call flow illustrates the handling of the terminating call case when the request is forwarded towards the user holding the requested identity as native identity who subscribes to the MuD service. It follows normal procedures and is included for completeness.

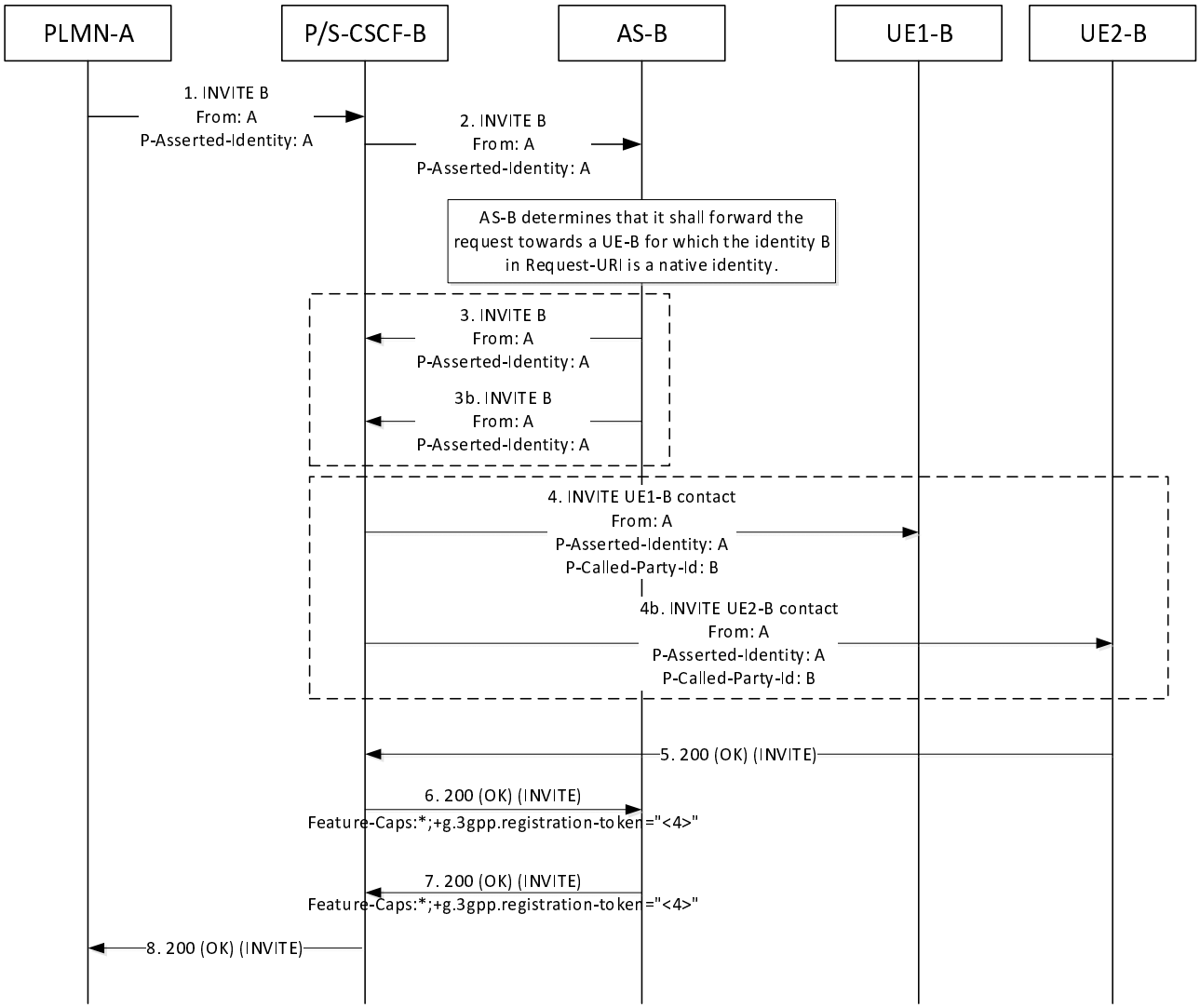

Figure A.3.2-1: UE-B reached by a native identity on multiple devices

1. **S-CSCF-B receives an INVITE message from PLMN-A, for an example see table A.3.2-1**

   The Request-URI identifies user B as B-native.

Table A.3.2-1: INVITE request (PLMN-A to I/S/P-CSCF-B)

```
INVITE tel:+11112222 SIP/2.0

To: <tel:+11112222>
From: <tel:+11111111>;tag=4fa3
P-Asserted-Identity: <sip:+11111111@plmnA.net;user=phone>, <tel:+11111111>

Other SIP header fields and SDP according to 3GPP TS 24.229 [3]
```

2. **S-CSCF-B forwards the INVITE message to AS-B**

   The AS-B determines that it shall forward the request towards UE1-B and UE2-B for which the identity in Request-URI is a native identity.

   AS-B can also send this to UEs configured to use the identity from the Request-URI as external alternative identity. This follows the terminating procedure in clause A.3.1.

3. **AS-B forwards the INVITE message to the S-CSCF-B**

The S-CSCF-B replaces B identity with the UE1-B contact and UE2-B contact , respectively, in the Request-URI and adds a P-Called-Party-ID header field.

4. **S-CSCF-B forwards the INVITE message to UE-B**

5. **UE2-B responds with 200 (OK)**

6. **The S-CSCF-B forwards the 200 (OK) response to AS-B**

   The S-CSCF-B inserts a Feature-Caps header field including a "registration-token" header field parameter to identify the registration flow.

NOTE: The AS-B learns the values of the registration-token during registration as specified in TS 24.229 [3]

7. **The AS-B forwards the 200 (OK) response to the S-CSCF-A.**

8. **The S-CSCF-B forwards the 200 (OK) response to PLMN-A.**

   The S-CSCF-B removes the "registration-token" header field parameter.

A.4 MuD call flows: Synchronization of call logs

A.4.1 General

The call flows in the following clauses illustrate typical scenarios to synchronize local call logs in federated UEs with the network stored call log.

The network call log storage is hosted in the AS. The AS updates the call log objects as appropriate based on the SIP call control signalling. The UE uses HTTP over the Ut reference point to subscribe to changes in the centralized call log, and use the notifications received to update the own local call log. The UE and the AS procedures and signalling related to the call log synchronization are based on the "strict synchronization" mechanism in accordance to OMA-TS-CPM_Message_Storage_Using_RESTFul_API [9] and OMA-TS-REST_NetAPI_NMS.

Incoming and outgoing calls of user A follow normal procedures as specified in TS 24.229 [3] but for simplicity only the AS node is shown (the CSCF, MRF, IBCF nodes have been omitted).

In the examples, "solid" lines represent the HTTP signalling between the UE and the AS and "dashed" lines represent the SIP call control signalling.

A.4.2 Subscription to notifications of network call log changes

This call flow illustrates subscription to notifications of network call log changes for the user of the MuD service which has two UEs. Subscription to notifications of network call log changes needs to be done separately for each UE.

NOTE 1: The UE can also read an individual subscription to a call log notification, update an individual subscription to notifications of network call log changes or unsubscribe to call log notifications.

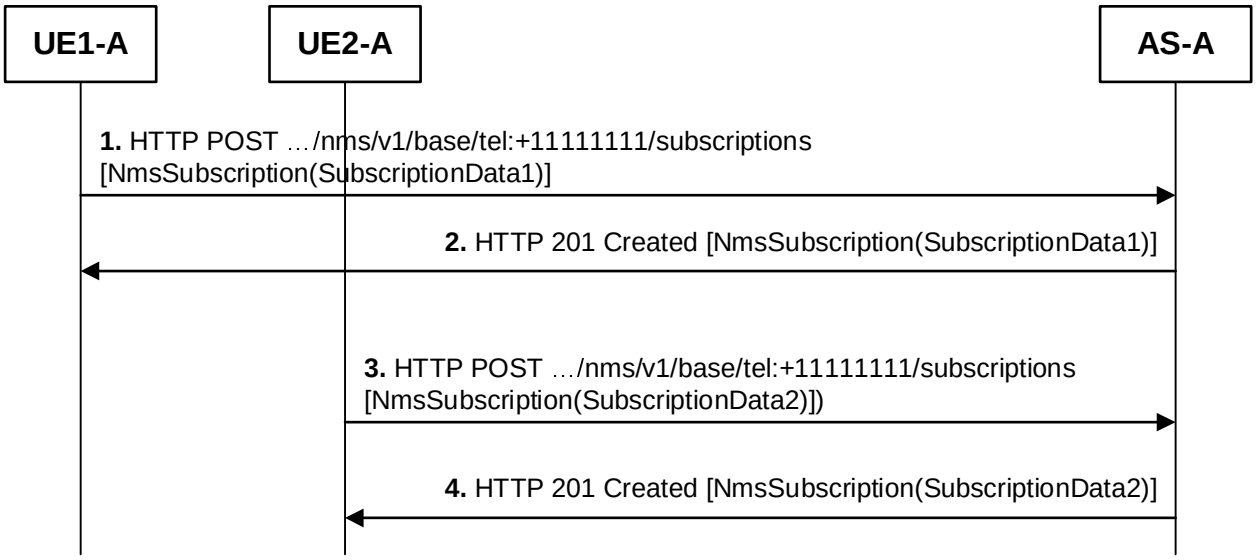

Figure A.4.2-1: Subscription to notifications of network call log changes

1. **UE1-A sends an HTTP POST request to AS-A**

   To subscribe to notifications of network call log changes, the UE1-A sends the HTTP POST request with "{apiRoot}/nms/{apiVersion}/{storeName}/{boxId}/subscriptions" as a request URI and the "NmsSubscription" data structure as a request body to the AS-A.

NOTE 2: The "NmsSubscription" data structure is defined in OMA-TS-REST_NetAPI_NMS.

The UE1-A includes in the "NmsSubscription":

- a UE1-A_callback_URI where the UE1-A wants to receive the requested notifications in the "callbackReference" attribute;

- changes in the call log the UE1-A is interested to receive in the "filter" attribute i.e. flag for an indication of a call log entry with enriched calling information received in association with the call (type = Flag, name = $CPM_CallLog_EnCall);

and can include:

- period of time (in seconds) notifications are provided for in the "duration" attribute; and
- subscription restart token indicating the point at which this UE1-A subscription is to start in the "restartToken" attribute (e.g., if the UE1-A has been offline for a period).

NOTE 3: If the "restartToken" attribute is absent, any changes from the time this UE1-A subscription is created will be notified by the AS-A.

2. AS-A sends a HTTP response "201 Created" to UE1-A

The AS-A creates a new Individual Subscription resource and sends a "201 Created" response to the UE1-A. The AS-A includes in the "201 Created" response:

- a Location header field containing the URI of the created resource i.e. "{apiRoot}/nms/{apiVersion}/{storeName}/{boxId}/subscriptions/{subscriptionId-1}"; and
- "NmsSubscription" data structure.

The AS-A includes in the "NmsSubscription" data structure subscription data for the UE1-A:

- period of time (in seconds) which the UE1-A subscription will still be valid in the "duration" attribute;
- index of the next notification to be issued to the UE1-A in the "index" attribute; and
- subscription restart token indicating the point at which this UE1-A subscription currently starts in the "restartToken" attribute,

and can include:

- the maximum number of events that can be delivered in a NmsEventList in the "maxEvents" attribute if "maxEvents" attribute was not provided by the UE1-A.

3. UE2-A sends an HTTP POST request to AS-A

This step is same as step 1, but in the "NmsSubscription" data structure the UE2-A includes its own subscription data e.g. the "callbackReference" attribute contains a UE2-A_callback_URI where the UE2-A wants to receive the requested notifications.

4. AS-A sends a HTTP response "201 Created" to UE2-A

This step is same as step 2, but the AS-A creates a new Individual Subscription resource for the UE2-A. The "NmsSubscription" data structure contains subscription data for the UE2-A. The URI of the created resource is indicated in a Location header field: "{apiRoot}/nms/{apiVersion}/{storeName}/{boxId}/subscriptions/{subscriptionId-2}".

A.4.3 Synchronization of list of outgoing calls

This call flow illustrates synchronization of list of outgoing calls when the user of the MuD service has two UEs and both UEs subscribed to notifications of network call log changes, as shown in clause A.4.2.

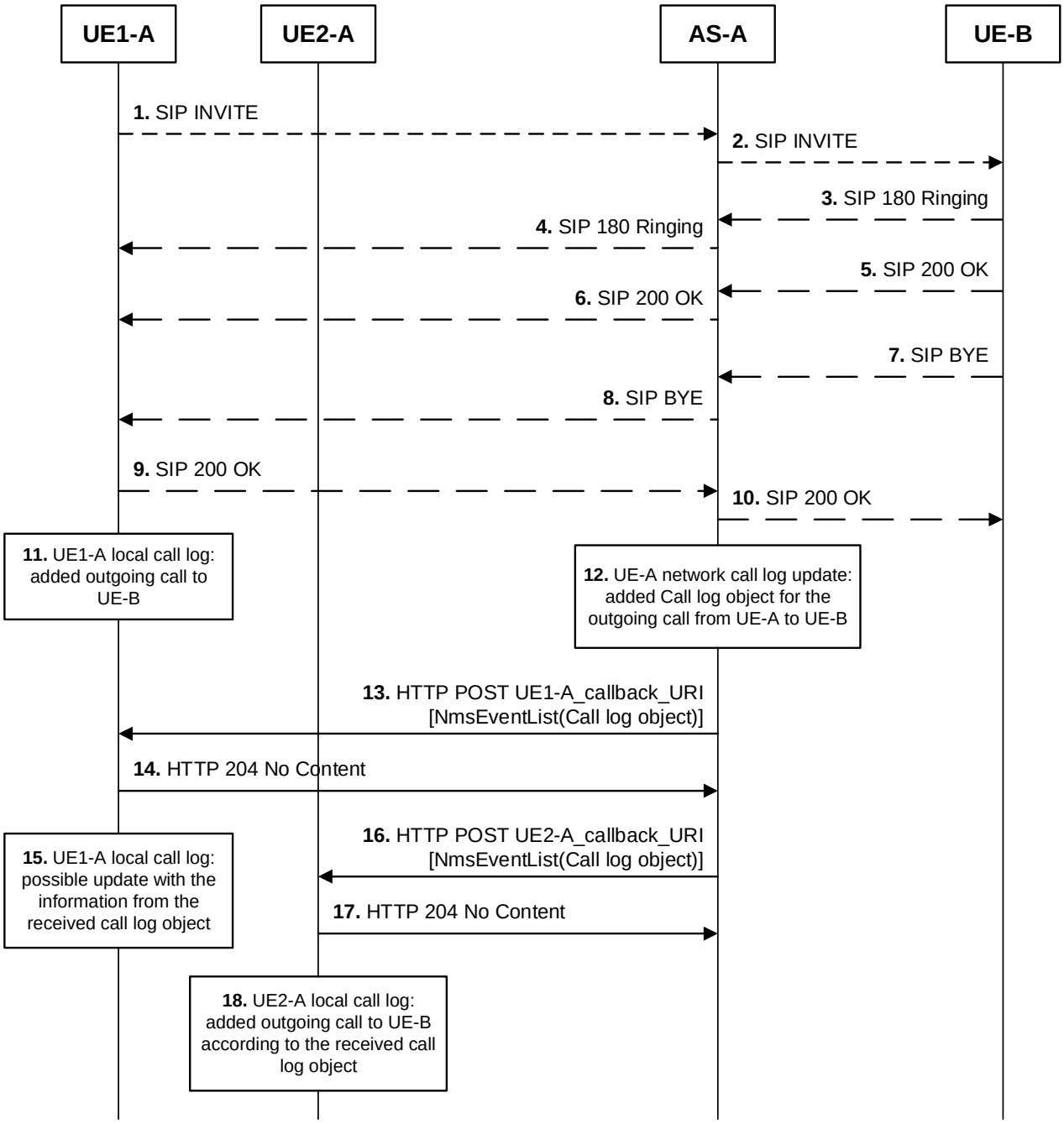

Figure A.4.3-1: Synchronization of list of outgoing calls

1. - 10 User A makes a call towards UE-B from UE1-A

The call flow between the UE1-A and the UE-B via the AS-A follows normal procedures as specified in TS 24.229 [3]. The UE-B answered call.

NOTE 1: For simplicity SIP "100 Trying", "183 Session Progress" responses, SIP ACK requests etc. are not shown.

11. UE1-A updates local call log

After call release i.e. in this example sending SIP 200 OK response to the UE-B, the UE1-A adds outgoing call to the UE-B in the local call log.

12. AS-A updates UE-A network call log

After call release i.e. in this example sending SIP 200 OK response to the UE-B, the AS-A adds a call log entry with enriched calling information in the UE-A's network call log.

13. AS-A sends a HTTP POST request to UE1-A

The AS-A observes changes in the call log for which the UE1-A has subscribed to and sends an HTTP POST request with "callbackReference" as a request URI (i.e. UE1-A_callback_URI) and the "NmsEventList" data structure as a request body, containing the call log object.

NOTE 2: The "NmsEventList" data structure is defined in OMA-TS-REST_NetAPI_NMS [10] and Call log object is defined in OMA-TS-CPM_Message_Storage_Using_RESTFul_API [9].

14. UE1-A sends a HTTP response "204 No Content" to AS-A

Upon successful reception of the HTTP POST request the UE1-A:

- stores received "index" attribute;
- stores received "restartToken" attribute; and
- sends an HTTP "204 No Content" response to the AS-A.

15. UE1-A local call log update

The UE1-A may update its local call log with the call log object for the outgoing call from the UE1-A to the UE-B as needed.

16. AS-A sends a HTTP POST request to UE2-A

The AS-A observes changes in the call log for which the UE2-A has subscribed to and sends an HTTP POST request with "callbackReference" as a request URI (i.e. UE2-A_callback_URI) and the "NmsEventList" data structure as a request body, containing the call log object.

17. UE2-A sends a HTTP response "204 No Content" to AS-A

Upon successful reception of the HTTP POST request the UE1-A:

- stores received "index" attribute;
- stores received "restartToken" attribute; and
- sends an HTTP "204 No Content" response to the AS-A.

18. UE2-A local call log update

Based on information received from the AS-A in the HTTP POST request, the UE2-A adds the outgoing call log object from the UE-A to the UE-B in the local call log.

A.4.4 Synchronization of missed call notifications

This call flow illustrates synchronization of missed call notifications when the user of the MuD service has two UEs and both UEs subscribed to notifications of network call log changes, as shown in clause A.4.2.

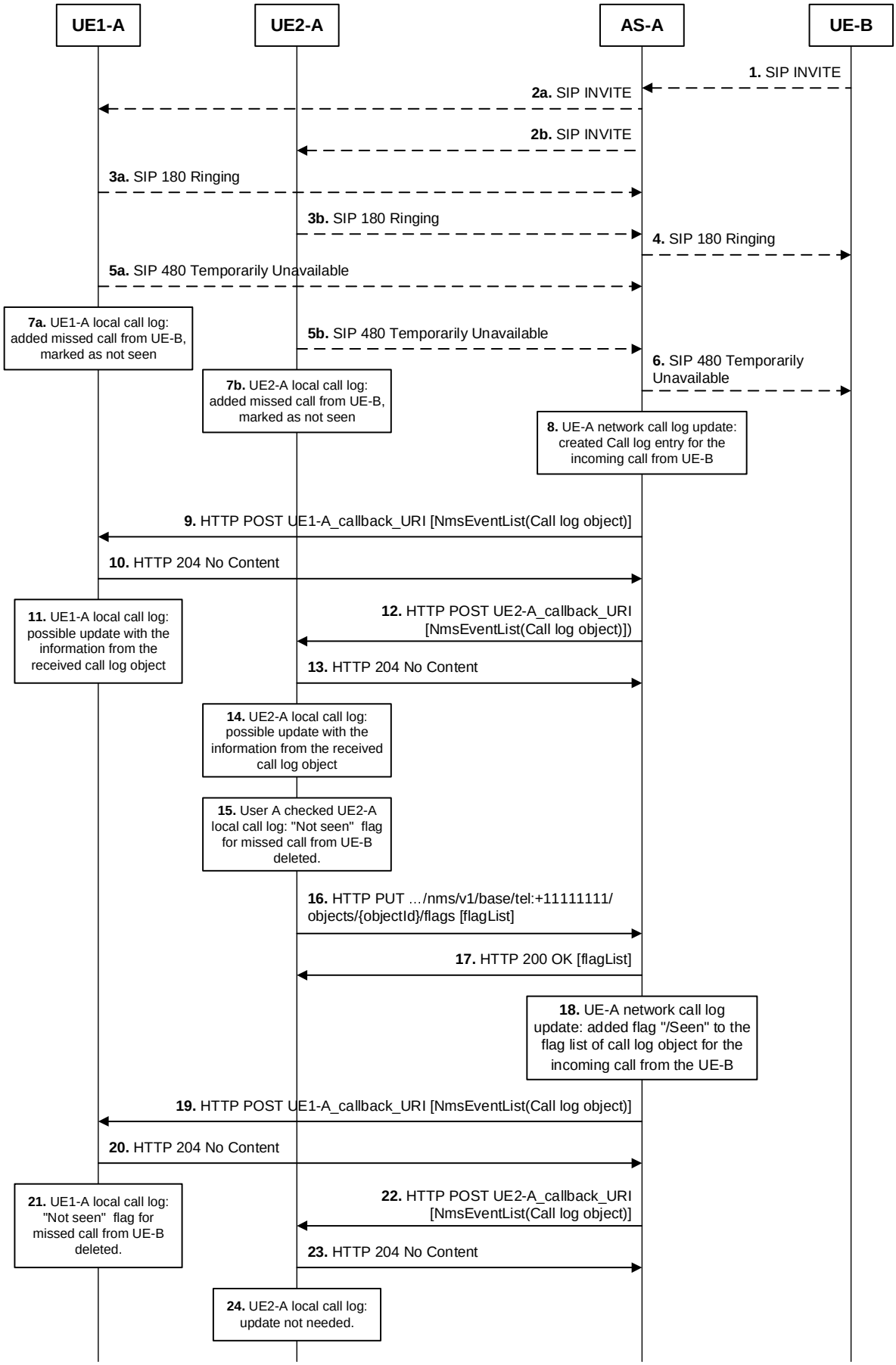

Figure A.4.4-1: Synchronization of missed call notifications

1. - 6 UE-B makes a call towards UE-A

The call flow between the UE-B and the user A UE's via the AS-A follows normal procedures as specified in TS 24.229 [3]. The user A subscribed to MuD service and the AS-A forwards SIP initial INVITE request to the UE1-A and the UE2-A. The user A did not answer call from the UE-B.

NOTE 1: For simplicity SIP "100 Trying", "183 Session Progress" responses, SIP ACK requests etc. are not shown.

7a. UE1-A updates local call log

After sending of an unsuccessful SIP response on SIP initial INVITE request (i.e. in this example SIP "480 Temporarily Unavailable" response) to the UE-B, the UE1-A adds incoming call from the UE-B in the local call log and marks it as "Missed" and flagged as "Not seen".

7b. UE2-A updates local call log

After sending of an unsuccessful SIP response on SIP initial INVITE request (i.e. in this example SIP "480 Temporarily Unavailable" response) to the UE-B, the UE2-A adds incoming call from the UE-B in the local call log and marks it as "Missed" and flagged as "Not seen".

8. AS-A updates UE-A network call log

After sending of unsuccessful SIP response on SIP initial INVITE request (i.e. in this example SIP "480 Temporarily Unavailable" response) to the UE-B, the AS-A creates a call log entry with enriched calling information in the UE-A's network call log: incoming call from the UE-B is marked as "LEFT_MESSAGE".

NOTE 2: The following values are specified for the incoming call: "ANSWERED", "LEFT_MESSAGE", "HUNG_UP", "REJECTED", "BUSY" or "BLACKLISTED", see attribute "Call-Disposition" defined in clause 5.3.9.3 of OMA-TS-CPM_Message_Storage_Using_RESTFul_API [9].

9. AS-A sends a HTTP POST request to UE1-A

The AS-A observes changes in the call log for which the UE1-A has subscribed to and sends an HTTP POST request with "callbackReference" as a request URI (i.e. UE1-A_callback_URI) and the "NmsEventList" data structure as a request body, containing the call log object.

10. UE1-A sends a HTTP response "204 No Content" to AS-A

Upon successful reception of the HTTP POST request the UE1-A:

- stores received "index" attribute;
- stores received "restartToken" attribute; and
- sends an HTTP "204 No Content" response to the AS-A.

11. UE1-A local call log update

The UE1-A may update the local call object if needed with information from the call log object for the incoming call from the UE-B.

12. AS-A sends a HTTP POST request to UE2-A

The AS-A observes changes in the call log for which the UE2-A has subscribed to and sends an HTTP POST request with "callbackReference" as a request URI (i.e. UE2-A_callback_URI) and the "NmsEventList" data structure as a request body, containing the call log object.

13. UE2-A sends a HTTP response "204 No Content" to AS-A

Upon successful reception of the HTTP POST request the UE2-A:

- stores received "index" attribute;
- stores received "restartToken" attribute; and
- sends an HTTP "204 No Content" response to the AS-A.

14. UE2-A local call log update

The UE2-A may update the local call object if needed with information from the call log object for the incoming call from the UE-B.

15. User A checked UE2-A local call log

The user A checked UE2-A local call log and flag "Not seen" is deleted from call log.

16. UE2-A sends HTTP PUT request to AS-A

The UE2-A indicates to the AS-A that the call from the UE-B needs to be flagged as "Seen" by sending the HTTP PUT request.

NOTE 3: Flag "/Seen" is added to the flaglist of a call log object in accordance to clause 6.6.1.1. of OMA-TS-CPM_Message_Storage_Using_RESTFul_API [9] and clause 6.3.4 of OMA-TS-REST_NetAPI_NMS [10].

17. AS-A sends a HTTP response "200 OK" to UE2-A

The AS-A responds with HTTP "200 OK" response to the UE2-A.

18. AS-A updates UE-A network call log

The AS-A adds flag "/Seen" to the call log object for the incoming call from the UE-B.

19. AS-A sends a HTTP POST request to UE1-A

Since the AS-A observes changes in the call log for which the UE1-A has subscribed to (flag "/Seen" added to the call log object for the incoming call from the UE-B), the AS-A sends an HTTP POST request with "callbackReference" as a request URI (i.e. UE1-A_callback_URI) and the "NmsEventList" data structure as a request body containing the call log object with the flag "/Seen".

20. UE1-A sends a HTTP response "204 No Content" to AS-A

Upon successful reception of the HTTP POST request the UE1-A:

- stores received "index" attribute;
- stores received "restartToken" attribute; and
- sends an HTTP "204 No Content" response to the AS-A.

21. UE1-A local call log update

The UE1-A updates local call log and deletes flag "Not seen" for the incoming call from the UE-B.

22. AS-A sends a HTTP POST request to UE2-A

Since the AS-A observes changes in the call log for which the UE2-A has subscribed to (flag "/Seen" added to the call log object for the incoming call from the UE-B), the AS-A sends an HTTP POST request with "callbackReference" as a request URI (i.e. UE2-A_callback_URI) and the "NmsEventList" data structure as a request body containing the call log object with the flag "/Seen".

23. UE2-A sends a HTTP response "204 No Content" to AS-A

Upon successful reception of the HTTP POST request the UE2-A:

- stores received "index" attribute;
- stores received "restartToken" attribute; and
- sends an HTTP "204 No Content" response to the AS-A.

24. UE2-A local call log update

The UE2-A observes that local call update is not needed since the UE2-A deleted flag "Not seen" for the incoming call from the UE-B in step 15.

Annex B (normative): IP-Connectivity Access Network specific concepts when using GPRS (Iu mode only) to access IM CN subsystem

B.1 Scope

The present annex defines IP-CAN specific requirements for a multimedia telephony communication service and associated supplementary services in the IP Multimedia (IM) Core Network (CN) subsystem, where the IP-CAN is General Packet Radio Service (GPRS).

B.2 GPRS aspects when connected to the IM CN subsystem

B.2.1 Procedures at the UE

B.2.1.1 Service specific access control

B.2.1.1.1 General

This clause specifies service specific access control in addition to procedures as specified in annex K of 3GPP TS 24.173 [19].

B.2.1.1.2 Call pull specific procedures

When the UE decides to pull a call from another federated UE, the UE provides a "call-pull-initiated" indication to the lower layers.

Annex C (normative): IP-Connectivity Access Network specific concepts when using EPS to access IM CN subsystem

C.1 Scope

The present annex defines IP-CAN specific requirements for a multimedia telephony communication service and associated supplementary services in the IP Multimedia (IM) Core Network (CN) subsystem, where the IP-CAN is Evolved Packet System (EPS).

C.2 EPS aspects when connected to the IM CN subsystem

C.2.1 Procedures at the UE

C.2.1.1 Service specific access control

C.2.1.1.1 General

This clause specifies service specific access control in addition to procedures as specified in annex J of 3GPP TS 24.173 [19].

C.2.1.1.2 Call pull specific procedures

When the UE decides to pull a call from another federated UE, the UE provides a "call-pull-initiated" indication to the lower layers.

Annex D (normative): IP-Connectivity Access Network specific concepts when using 5GS to access IM CN subsystem

D.1 Scope

The present annex defines IP-CAN specific requirements for a multimedia telephony communication service and associated supplementary services in the IP Multimedia (IM) Core Network (CN) subsystem, where the IP-CAN is 5G System (5GS).

D.2 5GS aspects when connected to the IM CN subsystem

D.2.1 Procedures at the UE

D.2.1.1 Service specific access control

D.2.1.1.1 General

This clause specifies service specific access control in addition to procedures as specified in annex M of 3GPP TS 24.173 [19].

D.2.1.1.2 Call pull specific procedures

When the UE decides to pull a call from another federated UE, the UE provides a "call-pull-initiated" indication to the lower layers.

Annex E(informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2018-08	CT1#112					First version	
2018-10	CT1#112bis					C1-186439 C1-186934 C1-186946	0.1.0
2018-12	CT1#113					C1-188701, C1-188738, C1-188739	0.2.0
2019-01	CT1#114					C1-190443, C1-190479, C1-190480, C1-190481	0.3.0
2019-03	CT1#115					C1-191438, C1-191441, C1-191485, C1-191486, C1-191491, C1-191492	
2019-04	CT1#116					C1-192514, C1-192515, C1-192518, C1-192534, C1-192536, C1-192537, C1-192540, C1-192541, C1-192542	0.5.0
2019-05	CT1#117					C1-193252, C1-193253, C1-193254, C1-193624, C1-193629, C1-193630, C1-193631, C1-193698, C1-193699, C1-193800	0.6.0
2019-06	CT1#117					Corrected implementation error in C1-103699	0.6.1
2019-09	CT1#119					C1-194332, C1-194701, C1-194864, C1-194865, C1-194866, C1-194868, C1-194869, C1-194870, C1-194871, C1-194875, C1-195051, C1-195052	0.7.0
2019-09	CT#85	CP-192085				Presentation for information to TSG CT	1.0.0
2019-10	CT1#120					C1-196381, C1-196394, C1-196692. C1-196693, C1-196694, C1-196695, C1-196698, C1-196699, C1-196804	1.1.0
2019-11	CT1#121					C1-198201, C1-198348, C1-198499, C1-198510, C1-198671, C1-198672, C1-198673, C1-198674, C1-198676, C1-198842	1.2.0
2020-02	CT1#122E					C1-200360, C1-20654, C1-200656, C1-200947, C1-200950, C1-201046	1.3.0
2020-03	CT-87e	CP-200163				Presentation for approval to TSG CT	2.0.0
2020-03	CT-87e					Version 16.0.0 created after approval	16.0.0
2020-06	CT-88e	CP-201125	0001		F	Text for empty headings	16.1.0
2020-06	CT-88e	CP-201125	0002		F	Reference update for PASSporT Extension for Diverted Calls	16.1.0
2020-09	CT-89e	CP-202182	0003		B	Overview Activation/deactivation of a user's identities	17.0.0
2020-09	CT-89e	CP-202184	0004		F	Correct spelling of an element name	17.0.0
2020-09	CT-89e	CP-202182	0007	2	B	MuDe Identity activation status indication for MiD	17.0.0
2020-12	CT-90e	CP-203214	0014	1	F	Correction to call flows	17.1.0
2021-03	CT-91e	CP-210130	0015	5	B	MuDE Identity activation status indication via Ut interface – option 1	17.2.0
2021-03	CT-91e	CP-210110	0021		A	Reference update: RFC 8946	17.2.0
2021-06	CT-92e	CP-211156	0023	3	F	Corrected text for identities	17.3.0
2021-06	CT-92e	CP-211158	0024		D	Corrections of MuDe introduced text	17.3.0
2021-06	CT-92e	CP-211158	0025	1	B	Precedence for activated identities	17.3.0
2021-06	CT-92e	CP-211158	0026	1	F	XML schema correction	17.3.0
2021-06	CT-92e	CP-211158	0027	1	F	Possibility of native identity deactivation	17.3.0
2021-06	CT-92e	CP-211158	0028	1	F	Handling of identity and alias attributes of ue-instance	17.3.0
2021-06	CT-92e	CP-211158	0029	1	F	Format of "identity" in <ue-instance>	17.3.0
2021-12	CT-94e	CP-213036	0030	2	B	Transfer between federated UEs	17.4.0
2022-03	CT-95e	CP-220272	0031	-	C	Format of identity attribute	17.5.0
2022-03	CT-95e	CP-220272	0034	-	F	Removal of Editor's Notes	17.5.0
2022-06	CT-96	CP-221257	0032	5	B	Call-pull-initiated indication	17.6.0
2023-06	CT-100	CP-231232	0035	3	F	Configuration precedence for MiD.	18.0.0
2025-10	-	-	-	-	-	Update to Rel-19 version (MCC)	**19.0.0**

History

Document history		
V19.0.0	October 2025	Publication