Leliwa Technical Bulletin

IMS Identification and numbering

Date: 23.09.2009

Revision: 009/IIN/009

Author: Jakub Bluszcz

Table of contents

Identification

This section describes the identities, numbers and addresses used in IMS to identify: user, user equipment, network, network elements and services.

ISIM

An IP Multimedia Services Identity Module (ISIM) is an application residing on the Universal Integrated Circuit Card (UICC) that provides access to IP Multimedia Services. ISIM contains parameters for identifying and authenticating the user to the IMS. The ISIM application can co-exist with (U)SIM and/or CSIM on the same UICC.

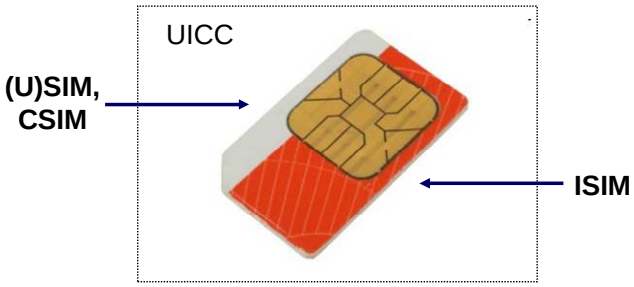

Figure 1 IP Multimedia Services Identity Module (ISIM)

ISIM file structure

The file structure of the ISIM Application Dedicated File (ADF_{ISIM}) is presented in Fig. 2-4[1].

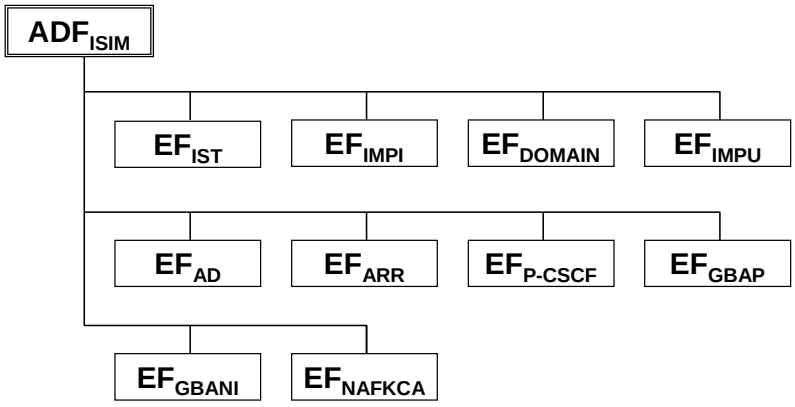

Figure 2 ISIM file structure

[1] R8

The ADF_{ISIM} contains the following Elementary Files (EFs):

- EF_{IMPI} - IMS private user identity,
- EF_{DOMAIN} - Home Network Domain Name,
- EF_{IMPU} - IMS Public User Identity (one or more),
- EF_{AD} - Administrative Data (UE operation mode, e.g. normal or type approval),
- EF_{ARR} - Access Rule Reference (access rules for files located under the ISIM ADF),
- EF_{IST} - ISIM Service Table (lists available optional services:P-CSCF address, Generic Bootstrapping Architecture (GBA), HTTP Digest, GBA-based Local Key Establishment Mechanism, support of P-CSCF discovery for IMS local break out),
- $EF_{P\text{-}CSCF}$ - P-CSCF Address (one or more),
- EF_{GBABP} - GBA Bootstrapping parameters (contains the AKA Random challenge (RAND) and Bootstrapping Transaction Identifier (B-TID) associate with a GBA bootstrapping procedure),
- EF_{GBANL} - GBA NAF List (contains the list of NAF_ID and B-TID associated to a GBA NAF derivation procedure),
- EF_{NAFKCA} - NAF Key Centre Address (one or more).

Home network domain name

The home network domain name is in the format of an Internet domain name (IETF RFC 1035), e.g. operator.com..

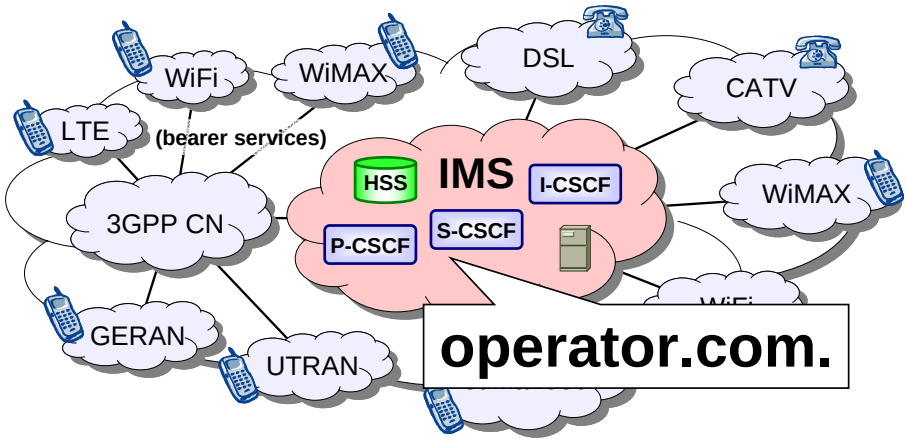

Figure 3 Home network domain name

For 3GPP systems, if there is no ISIM application, the UE derives the home network domain name from the IMSI as described in the following steps:

❶ Take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used and separate them into MCC and MNC; if the MNC is 2 digits then add a zero at the beginning.

❷ Use the MCC and MNC derived in step ❶ to create the "mnc<MNC>.mcc<MCC>.3gppnetwork.org" domain name.

❸ Add the label "ims." to the beginning of the domain.

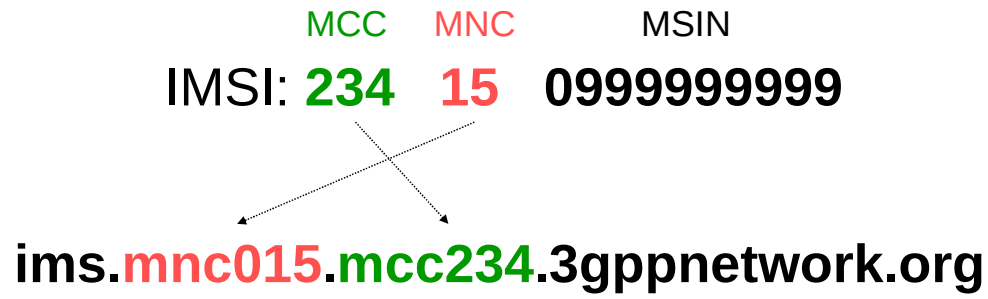

Figure 4 Home network domain name derivation from IMSI

Private User Identity

Every IMS user has one or more Private User Identities. The private identity is assigned by the home network operator, and used, for example, for Registration, Authorisation, Administration, and Accounting purposes. This identity takes the form of a Network Access Identifier (NAI) and has the form username@realm (IETF RFC 4282).

Figure 5 Private user identity

It is possible for a representation of the IMSI to be contained within the NAI for the private identity.

The following points are giving a short characteristics of the Private User Identity:

- The Private User Identity is not used for routing of SIP messages.
- The Private User Identity shall be contained in all Registration requests, (including Re-registration and De-registration requests) passed from the UE to the home network.
- An ISIM application securely stores one Private User Identity. It shall not be possible for the UE to modify the Private User Identity information stored on the ISIM application.
- The Private User Identity is a unique global identity defined by the Home Network Operator, which may be used within the home network to identify the user's subscription (e.g. IM service capability) from a network perspective. The Private User Identity identifies the subscription, not the user.
- The Private User Identity is permanently allocated to a user's subscription (it is not a dynamic identity), and is valid for the duration of the user's subscription with the home network.
- The Private User Identity is used to identify the user's information (for example authentication information) stored within the HSS (for use for example during Registration).
- The Private User Identity may be present in charging records based on operator policies.
- The Private User Identity is authenticated only during registration of the user, (including re-registration and de-registration).
- The HSS needs to store the Private User Identity.
- The S-CSCF needs to obtain and store the Private User Identity upon registration and unregistered termination.

Private User Identity derivation from IMSI

For 3GPP systems, if there is no ISIM application, the private user identity is not known. If the private user identity is not known, the private user identity is derived from the IMSI.

The following steps show how to build the private user identity out of the IMSI:

❶ Use the whole string of digits as the username part of the private user identity; and

❷ convert the leading digits of the IMSI, i.e. MNC and MCC, into a domain name, as described in previous section.

The result will be a private user identity of the form "<IMSI>@ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org".

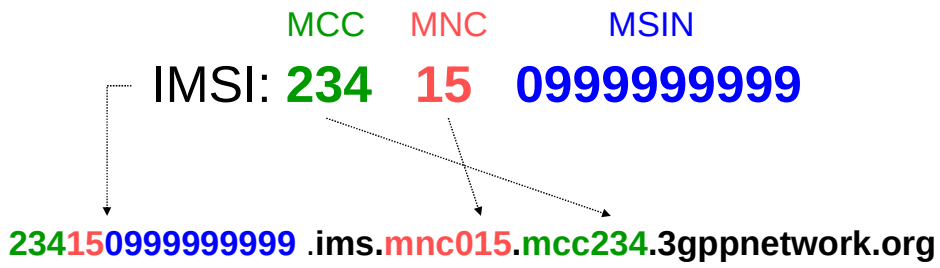

Figure 6 Private user identity derivation from IMSI

Public User Identity

Every IMS user has one or more Public User Identities. The Public User Identity/Identities are used by any user for requesting communications to other users. For example, this might be included on a business card.

The public user identity takes the form of either a SIP URI (IETF RFC 3261) or a Tel URI (IETF RFC 3966).

A SIP URI for a public user identity takes the canonical form "sip:username@domain".

A Tel URI for a public user identity representing an E.164 number takes the canonical form "tel:<Global Number>" which contains a global number without visual separators. The UE may use also local format. The local to global numbering translation is performed in the originating network.

A SIP URI can also represent an E.164 number if it includes "user=phone" URI parameter. The "userinfo" part of this SIP URI shall follow the same format of the Tel URI for a Public User Identity (i.e. "<Global Number>").

Figure 7 Public user identity

The following points are giving a short characteristics of the Public User Identity:

- Both telecom numbering and Internet naming schemes can be used to address users depending on the Public User identities that the users have.
- An ISIM application securely stores at least one Public User Identity . It shall not be possible for the UE to modify the Public User Identity), but it is not required that all additional Public User Identities be stored on the ISIM application..
- A Public User Identity shall be registered either explicitly or implicitly before IMS sessions and IMS session unrelated procedures can be established by/to a UE using the Public User Identity.
- It is possible to identify Alias Public User Identities. For such a group of Public User Identities, operations that enable changes to the service profile and the service data configured applies to all the Public User Identities within the group. This grouping information is stored in the HSS, and it is available to AS via the Sh interface, S-CSCF via the Cx interface, and UE via the Gm interface.
- It is possible to register globally (i.e. through one single UE request) a user that has more than one public identity via a mechanism within the IP multimedia CN subsystem (e.g. by using an Implicit Registration Set). This does not preclude the user from registering individually some of his/her public identities if needed.
- Public User Identities are not authenticated by the network during registration.
- Public User Identities may be used to identify the user's information within the HSS (for example during mobile terminated session set-up).

Wildcarded Public User Identities

Public User Identities may be stored in the HSS as Wildcarded Public User Identities. A Wildcarded Public User Identity represents a collection of Public User Identities that share the same service profile and are included in the same implicit registration set. Wildcarded Public User Identities enable optimisation of the O&M of the nodes for the case in which a large amount of users are registered together and handled in the same way by the network.

A wildcarded Public User Identity consists of a delimited regular expression located either in the userinfo portion of the SIP URI or in the telephone-subscriber portion of the Tel URI. The regular expression in the wildcarded Public User Identity takes the form of Extended Regular Expressions (ERE). The delimiter is the exclamation mark character ("!").

When stored in the HSS, the wildcarded Public User Identity includes the delimiter character to indicate the extent of the part of the Public User Identity that is wildcarded. It is used to separate the regular expression from the fixed part of the wildcarded Public User Identity.

Example 1:

The following Public User Identities could be stored in the HSS - "sip:user!.*!@example.com", or "tel:4832376630!.*!"

When used on an interface, the exclamation mark characters within a Public User Identity are not interpreted as delimiter.

Example 2:

The following Public User Identities communicated in interface messages to the HSS will match to the wildcarded Public User Identity of "sip:user!.*!@example.com"., stored in the HSS:

- sip:chatlist1@example.com,
- sip:chatlist2@example.com,
- sip:chatlist42@example.com,
- sip:chatlistAbC@example.com,
- sip:chatlist!1@example.com.

Example 3:

The following Public User Identities communicated in interface messages to the HSS will match to the wildcarded Public User Identity of "tel:4832376630!.*!" stored in the HSS:

- tel: 48323766300,
- tel: 48323766301,
- tel: 48323766302,
- tel: 48323766303,
- …
- tel: 48323766309.

sip:user!.*!@example.com	**tel:4832376630!.*!**
sip:chatlist1@example.com	tel: 48323766300
sip:chatlist2@example.com	tel: 48323766301
sip:chatlist42@example.com	tel: 48323766302
sip:chatlistAbC@example.com	tel: 4832376630356
sip:chatlist!1@example.com	tel: 483237663098888

Figure 8 Wildcarded Public User Identities

Relationship of Private and Public User Identities

The home network operator is responsible for the assignment of the Private User Identities, and public user identities; other identities that are not defined by the operator may also exist.

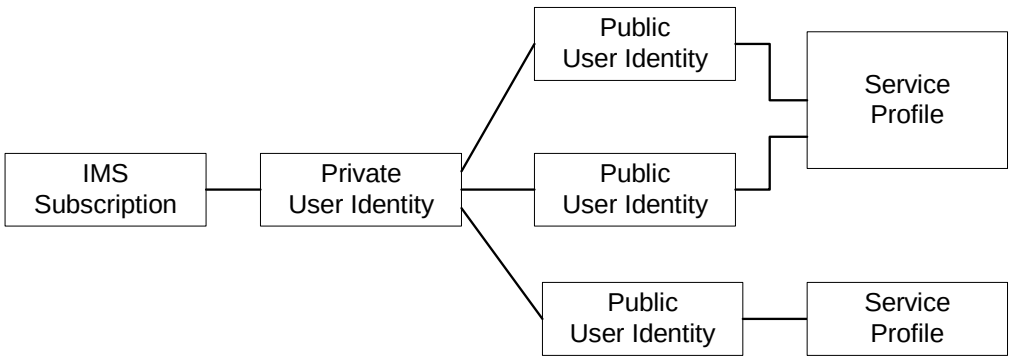

Figure 9 Relationship of the Private User and Public User Identities

The IMS Service Profile is a collection of service and user related data. The Service Profile is independent from the Implicit Registration Set, e.g. Public User Identities with different Service Profiles may belong to the same Implicit Registration Set. Initial filter criteria in the service profile provide a simple service logic comprising of user / operator preferences that are of static nature i.e. they do not get changed on a frequent basis.

All Public User Identities of an IMS subscription shall be registered at the same S-CSCF. The service profile is downloaded from the HSS to the S-CSCF. Only one service profile shall be associated with a Public User Identity at the S-CSCF at a given time. Multiple service profiles may be defined in the HSS for a subscription. Each Public User Identity is associated with one and only one service profile. Each service profile is associated with one or more Public User Identities.

Public user identities may be shared across multiple Private User Identities within the same IMS subscription. Hence, a particular Public User Identity may be simultaneously registered from multiple UEs that use different Private User Identities and different contact addresses. If a Public User Identity is shared among the Private User Identities of a subscription, then it is assumed that all Private User Identities in the IMS subscription share the Public User Identity.

All Service Profiles of a user are stored in the same HSS, even if the user has one or more shared Public User Identities.

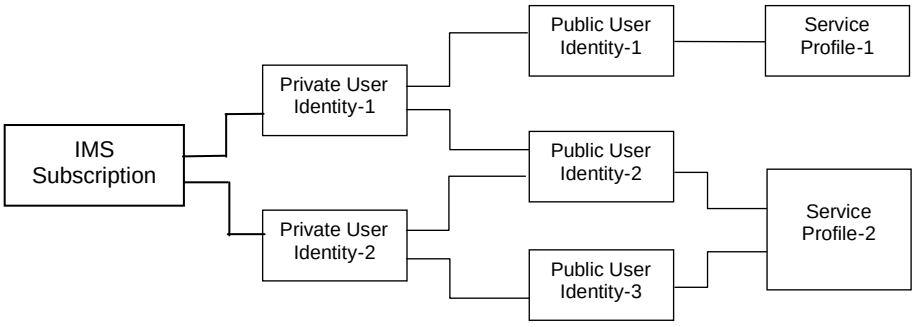

Figure 10 The relation of a shared Public User Identity (Public-ID-2) and Private User Identities

Temporary public user identity

For 3GPP systems, if there is no ISIM application to host the public user identity, a temporary public user identity is derived, based on the IMSI. The temporary public user identity consist of the string "sip:" appended with a username and domain portion equal to the IMSI derived private user identity, e.g. "sip:234150999999999@ims.mnc015.mcc234.3gppnetwork.org".

Public Service Identity (PSI)

With the introduction of standardized presence, messaging, conferencing, and group service capabilities in IMS, there is a need for Public Service Identities (PSIs). These identities are different from the Public User Identities in the respect that they identify services, which are hosted by ASs. In particular, PSIs are used to identify groups. For example a chat-type service may use a PSI (e.g. sip:chatlist_X@example.com) to which the users establish a session to be able to send and receive messages from other session participants.

The IM CN subsystem provides the capability for users to create, manage, and use PSIs under control of AS. It is possible to create statically and dynamically a PSI.

Each PSI is hosted by an AS, which executes the service specific logic as identified by the PSI.

The IMS provides capability of routing IMS messages using PSI.

The PSI takes the form of either a SIP URI or a Tel URI. The domain part is pre-defined by the IMS operators and the IMS system provides the flexibility to dynamically create the user part of the PSIs.

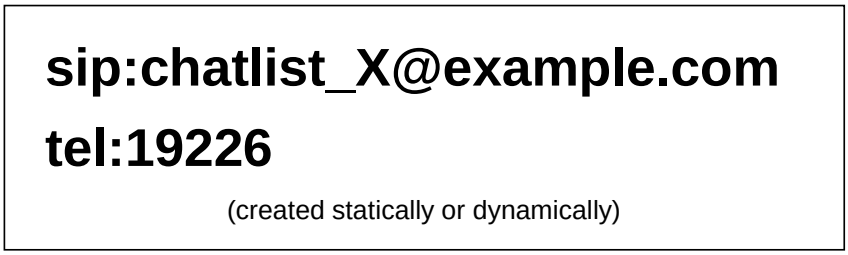

Figure 11 Public Service Identity (PSI)

Wildcarded Public Service Identities

The PSIs are stored in the HSS either as a distinct PSI or as a wildcarded PSI. A distinct PSI contains the PSI that is used in routing, whilst a wildcarded PSI represents a collection of PSIs. Wildcarded PSIs enable optimisation of the O&M of the nodes.

The format of a Wildcarded PSI is the same as for the Wildcarded Public User Identity, described earlier in this chapter.

Private Service Identity

The Private Service Identity is applicable to a PSI user and is similar to a Private User Identity in the form of a NAI. The Private Service Identity is operator defined and although not operationally used for registration,

authorisation and authentication in the same way as Private User Identity, it enables Public Service Identities to be associated to a Private Service Identity which is required for compatibility with the Cx (HSS-CSCF) procedures.

Anonymous User Identity

The Anonymous User Identity takes the form of a SIP URI. A SIP URI for an Anonymous User Identity takes the form "sip:user@domain". The user part is the string "anonymous" and the domain part is the string "anonymous.invalid". The full SIP URI for Anonymous User Identity is thus: "sip:anonymous@anonymous.invalid".

In case of terminating signalling the “From” header may contain an Anonymous User Identity, which means that the calling party desired anonymity.

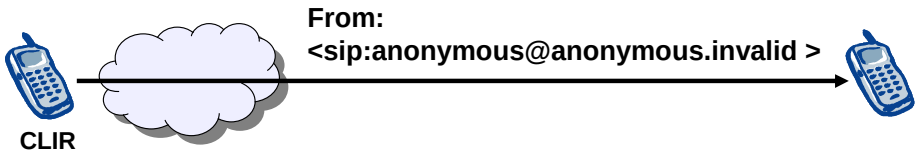

Figure 12 Anonymous User Identity

Unavailable User Identity

The Unavailable User Identity takes the form of a SIP URI. A SIP URI for an Unavailable User Identity takes the form "sip:user@domain". The user part is the string "unavailable" and the domain part is the string "unknown.invalid". The full SIP URI for Anonymous User Identity is thus: "sip:unavailable@unknown.invalid".

In case of terminating signalling the “From” header may contain an Unavailable User Identity, which means that the calling party is unknown.

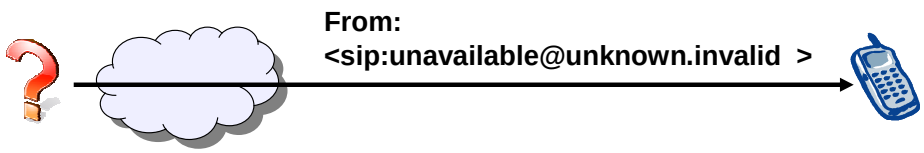

Figure 13 Unavailable User Identity

Instance-ID

An Instance-Id is a SIP Contact header parameter that uniquely identifies the SIP UA performing a registration.

When an IMEI is available, the Instance-Id takes the form of a IMEI Uniform Resource Name (URN). The format of the instance-id takes the form "urn:gsma:imei:<gsma-specifier-defined-string>" where the the gsma-specifier-defined-string is the IMEI encoded as defined in draft-montemurro-gsma-imei-urn e.g. urn:gsma:imei:90420156-025763-0.

If no IMEI is available, the instance-id takes the form of a string representation of a Universally Unique IDentifier (UUID) as a URN (RFC 4122), e.g. urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6.

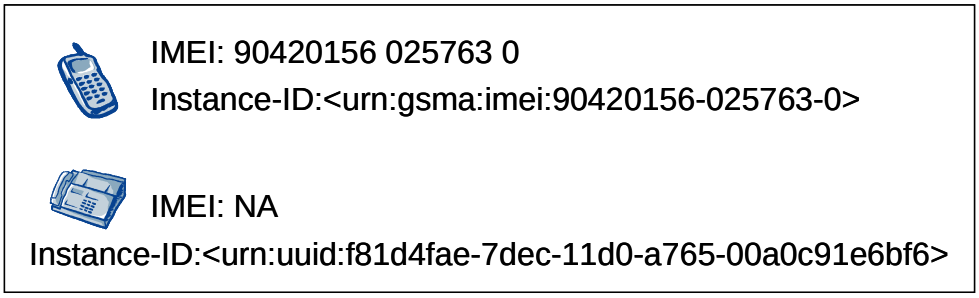

Figure 14 Instance-ID

Globally Routable User Agent URI

A Globally Routable User Agent URI (GRUU) is an identity that identifies a unique combination of Public User Identity and UE instance that allows a UE to address a SIP request to a specific Public User Identity UE combination instance, as opposed to a Public User Identity, in order to ensure that the SIP request is not forked to another registered UE of the same Public User Identity. There are two types of GRUUs; Public GRUUs (P-GRUUs) and Temporary GRUUs (T-GRUUs). P-GRUUs are GRUUs that reveal the Public User Identity of the user and are very long lived. T-GRUUs are GRUUs that contain a URI that do not reveal the Public User Identity of the user and are valid until the contact is explicitly de-registered or the current registration expires. The IMS supports the capability for IMS UEs to obtain both T-GRUUs and P-GRUUs when performing IMS registration, exchange GRUUs using SIP requests and responses and use GRUUs to address SIP requests to specific UEs according to draft-ietf-sip-gruu[2].

Relationship of Public User Identities, GRUUs, and UEs

Each Public User Identity may have one or more Globally Routable User Agent URIs (GRUUs). There are two types of GRUU, P-GRUUs and T-GRUUs which are associated with Public User Identities and are generated and assigned to the UE together during registrations and re-registration in a pair of one P-GRUU and one T-GRUU. Each pair of a P-GRUU and a

[2] Today, RFC 5627

T-GRUU is associated with one Public User Identity and one UE. During subsequent re-registrations the same P-GRUU will be assigned to the UE but a new and different T-GRUU will be generated and assigned. After a re-registration all the previous T-GRUUs generated during the period of this registration are all still valid. A UE may retain some or all of the previous T-GRUUs obtained during the initial registration or previous re-registrations along with the new T-GRUU or the UE may replace some or all of the previous T-GRUUs with the new T-GRUU. The current set of the P-GRUU and all T-GRUUs which are currently valid during this registration period is referred to here as the GRUU set. If a UE registers (explicitly or implicitly) with multiple Public User Identities, a separate GRUU set is associated with each. If different UEs register with the same Public User Identity, a different GRUU set is associated with each.

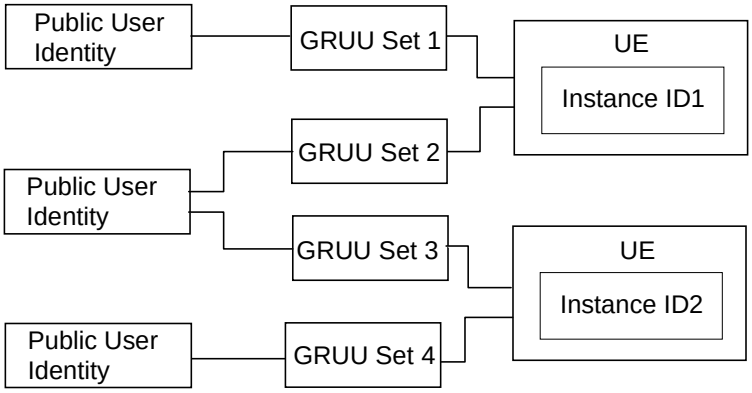

Figure 15 The relationship of Public User Identities, GRUUs, and UEs

Dialled number formats

When using a phone number as the dialled address, the UE can provide this number in the form of a SIP URI or a Tel URI. This phone number can be in the form of E.164 format (prefixed with a '+' sign), or a local format using local dialling plan and prefix. The IMS will interpret the phone number with a leading '+' to be a fully defined international number.

When a non-international formats of E.164 addresses (including geo-local numbers and home-local numbers and other local numbers) is used as a Tel URI, it must be followed by a "phone-context" Tel URI parameter. The "phone-context" parameter includes the access technology information. In case the access technology information is not available the "phone-context" is set to the home network domain name preceded by the string "geo-local".

Tel URI: <tel:+48323764433>

Tel URI: <tel:323764433;phone-context=260.01.gprs.polkomtel.pl>

Tel URI: <tel:0048323764433; phone-context=428.02.gprs.polkomtel.pl>

Tel URI: <tel:0323764433; phone-context=geo-local.tp.pl>

Figure 16 Phone number as the dialled address (Tel URI)

SIP URI: <sip:+48-32-376-4433@neofon.tp.pl.com;user=phone>

SIP URI: <sip:=323764433@neofon.tp.pl;user=phone>

Figure 17 Phone number as the dialled address (SIP URI)

Dialstring URI

In some cases a dialled string is not representing a telephone number, or the UE is not able to identify a dialstring to be a telephone number. In that case the dialled string can be expressed as dialstring URI, with the "userinfo" parameter of the 'sip:' set to "dialstring".

The dial string is a sequence of the characters 0-9, A-D, P, X, '*' and '#'. In coding '*' is represented by 'E' and '#' is represented by 'F'. P is a pause (short wait, like a comma in a modem string) and X represents "wait for call completion".

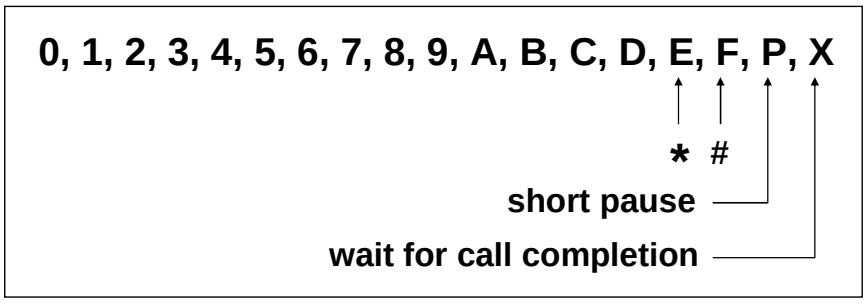

Figure 18 Dialstring URI (available characters)

A dial string always exists within a context. The context must be specified when expressing a dial string.

Examples:

- the UE might emit "sip:123;phone-context= 260.01.gprs.polkomtel.pl;user=dialstring" when a user dials extension 123,

- the UE might emit “sip:323766305X123;phone-context=geo-local.neofon.tp.pl;user=dialstring” when a user dials a telephone number together with PABX extension.

SIP URI: <sip:123;phone-context= 260.01.gprs.polkomtel.pl;user=dialstring>

SIP URI: <sip:323766305X123;phone-context=geo-local.ekiga.net;user=dialstring>

Figure 19 Dialstring URI (examples)

Identification of network nodes

The CSCF, BGCF and MGCF nodes shall be identifiable using a valid SIP URI (Host Domain Name or Network Address) on those interfaces supporting the SIP protocol, (e.g. Gm, Mw, Mm, and Mg). These SIP URIs would be used when identifying these nodes in header fields of SIP messages. However this does not require that these URIs will be globally published in DNS.

ENUM

Telephone number mapping is the process of unifying the telephone number system of the public switched telephone network with the Internet addressing and identification name spaces. Telephone numbers are systematically organised in the E.164 standard, while the Internet uses the Domain Name System (DNS) for linking domain names to IP addresses and other resource information. Telephone number mapping systems provide facilities to determine applicable Internet communications servers responsible for servicing a given telephone number by simple lookups in the DNS.

The most prominent facility for telephone number mapping is the E.164 Number Mapping (ENUM) standard. It uses special DNS record types to translate a telephone number into a URI or IP address that can be used in Internet communications.

ENUM query

For the purpose of ENUM query the E.164 number has to be translated into domain name, as described in the following steps:

❶ Remove all characters with the exception of the digits. For example, this step would remove the leading "+" from "+442079460148" producing "442079460148".

❷ Put dots (".") between each digit (example: "4.4.2.0.7.9.4.6.0.1.4.8").

❸ Reverse the order of the digits (example: "8.4.1.0.6.4.9.7.0.2.4.4").

❹ Append the string ".e164.arpa" to the end (example: "8.4.1.0.6.4.9.7.0.2.4.4.e164.arpa").

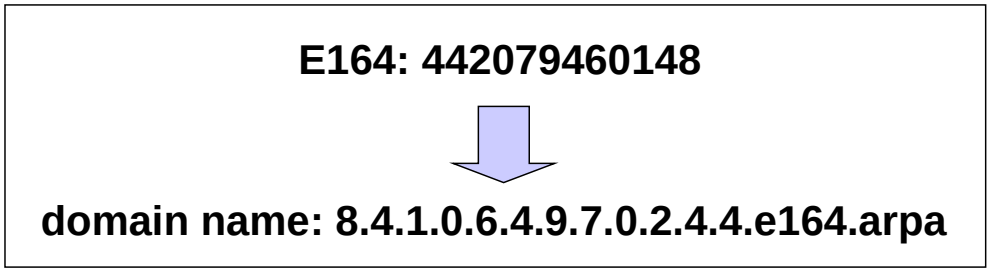

Figure 20 Domain name derivation from E.164 number

This domain-name is used to request Naming Authority Pointer (NAPTR) DNS Resource Records, containing URIs to be used to access Internet communications services, see example in Fig. 2-23.

```
NAPTRs for 4.5.9.1.2.2.7.0.6.8.4.e164.arpa.
IN NAPTR 200 10 u E2U+tel            !^.*$!tel:+48607221954!
IN NAPTR 200 20 u E2U+tel            !^.*$!tel:+48399571981!
IN NAPTR 200 30 u E2U+tel            !^.*$!tel:+48323766305!
IN NAPTR 300 10 u E2U+fax            !^.*$!tel:+48323766307!
IN NAPTR 100 10 u E2U+sip            !^.*$!sip:jakub.bluszcz@ekiga.net!
IN NAPTR 100 20 u E2U+sip            !^.*$!sip:48399571981@neofon.tp.pl!
IN NAPTR 400 10 u E2U+x-skype:callto !^.*$!callto:jakub.bluszcz!
IN NAPTR 500 10 u E2U+sms            !^.*$!tel:+48607221954!
IN NAPTR 600 10 U E2U+mailto         !^.*$!mailto:jakub.bluszcz@leliwa.com!
IN NAPTR 700 10 u E2U+http           !^.*$!http:www.leliwa.com!
IN NAPTR 800 10 u E2U+vcard          !^(.*)$!http://www.leliwa.com/vcf/bluszcz.vcf!
```

Figure 21 NAPTR records (example)

ENUM in IMS

The ENUM/DNS translation mechanism (RFC 3761) can be used by all IMS nodes that require E.164 address to SIP URI resolution. The actual ENUM/DNS database(s) used to perform address translations are outside the scope of 3GPP and are therefore a matter for the network operator. There is no requirement that the universal ENUM service on the Internet be used. As such, it is possible that the ENUM/DNS mechanism uses a different top level domain to that of "e164.arpa.", therefore, the top level domain to be used for ENUM domain names is a network operator configurable option in all IMS nodes that can perform ENUM/DNS resolution.

Handling of Tel URIs

The S-CSCF supports the ability to translate the E.164 address contained in a Request-URI in the Tel: URI format (RFC 3966) to a SIP routable SIP URI using the ENUM/DNS translation mechanism. If this translation succeeds, then the session is routed according to the returned SIP URI.

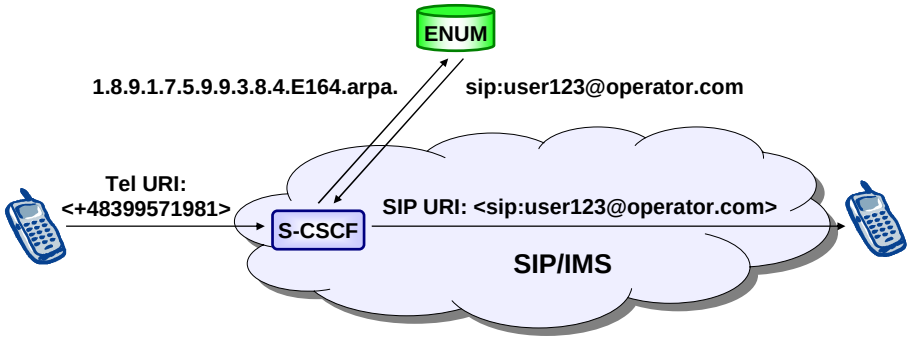

Figure 22 Handling of Tel URI (successful ENUM translation)

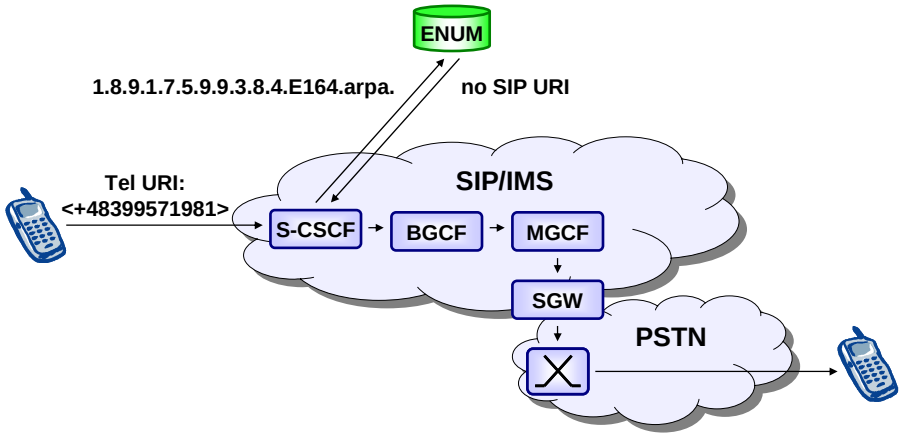

Figure 23 Handling of Tel URI (unsuccessful ENUM translation)

If this translation fails, then the session may be forwarded to a BGCF for further routing (e.g. to the PSTN) or appropriate notification is sent to the originating session endpoint, depending on network operator configuration.

Handling of SIP URIs representing a telephone number

Per network operator policy, the network may attempt to resolve and route a SIP URI representing a telephone number and a domain that does not own the target user using the ENUM/DNS translation mechanism. The need for address resolution may be triggered by the S-CSCF, and the I-CSCF or transit function, as determined by network operator configuration.

Acronyms and Abbreviations

3GPP	3rd Generation Partnership Project
AAA	Accounting, Authentication, Authorization
AD	Administrative Data
ADF	Application Dedicated File
ARR	Access Rule Reference
AS	Application Server
BGCF	Breakout Gateway control function
BICC	Bearer Independent Call Control
CAP	Camel Application Part
CATV	Community Access Television
CDMA	Code Division Multiple Access
CSCF	Call Session Control Function
DNS	Domain Name System
DSL	Digital Service Line
EF	Elementary File
eNB	eNode B
ENUM	E.164 Number Mapping
ERE	Extended Regular Expressions
GBA	Generic Bootstrapping Architecture
GERAN	GSM/Edge Radio Access Network
GRUU	Globally Routable User Agent URI
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
I-CSCF	Interrogating-CSCF
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMS-MGW	IMS - Media Gateway Function
IP	Internet Protocol
ISIM	IP Multimedia Services Identity Module
IST	ISIM Service Table
ISUP	ISDN User Part
LTE	Long Term Evolution
MAP	Manufacturing Application Protocol
MCC	Mobile Country Code
MGCF	Media Gateway Control Function
MNC	Mobile Network Code
MRFC	Multimedia Resource Function Controller
MRFP	Media Resource Function Processor
MS	Mobile Station
NAI	Network Access Identifier

NAPTR	Naming Authority Pointer
P-CSCF	Proxy-CSCF
P-GW	PDN (Packet Data Network) Gateway
PSI	Public Service Identity
PSTN	Public Switched Telephone Network
PUI	Private User Identity
RTP	Real-Time Protocol
S-CSCF	Serving-CSCF
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
S-GW	Signalling Gateway Function
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
URN	Uniform Resource Name
UTRAN	UMTS Terrestrial Radio Access Network
UUID	Universally Unique IDentifier
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access

References

This section contains the locations of various specifications, document references and useful information where you can learn more about this subject.

[1] 22.228 Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1

[2] 22.016 International Mobile Equipment Identities (IMEI)

[3] 23.008 Organization of subscriber data

[4] 23.228 IP Multimedia Subsystem (IMS); Stage 2

[5] 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3

[6] 31.103 Characteristics of the IP Multimedia Services Identity Module (ISIM) application

[7] rfc3261 SIP: Session Initiation Protocol

[8] rfc5627 Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)

[9] rfc3986 Uniform Resource Identifier (URI): Generic Syntax

[10] rfc3966 The tel URI for Telephone Numbers

[11] rfc3761 The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)

[12] rfc2915 The Naming Authority Pointer (NAPTR) DNS Resource Record

[13] rfc1035 DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

[14] rfc4282 The Network Access Identifier

[15] rfc4122 A Universally Unique IDentifier (UUID) URN Namespace

[16] e.164 Assigned Country Codes

[17] e.212 The international identification plan for public networks and subscriptions

Disclaimer

This document is based on Leliwa training materials.

Information in this document is subject to change without notice. Leliwa assumes no responsibility for any errors that may appear in this document.

This document may be freely redistributed. You can store it on any servers and make it available for public download. In such case it must be clearly indicated that it comes from Leliwa website www.leliwa.com

If you received only this file, you can download more Leliwa Technical Bulletins from the following address:

http://www.leliwa.com/downloads

If you want to be informed when the new bulletins are uploaded, please send a blank e-mail with Subject="Update_request" to bulletins@leliwa.com or click this link: bulletins@leliwa.com

Leliwa Sp. z o.o.

Plebiscytowa 1.122
PL-44-100 Gliwice
Poland
GPS: N50.2981°, E018.6561°

telephone: +48 32 376 63 05
fax: +48 32 376 63 07
Skype: leliwa_poland
email: info@leliwa.com

Leliwa Telecom AB

Orrpelsvägen 66
SE-167 66 BROMMA
Sweden
GPS: N59.3260°, E17.9464°

telephone: +46 8 4459430
email: info@leliwa.com