ENUM Guidelines for Service Providers and IPX Providers

Version 1.0

20 March 2017

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice (Test)

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

This document provides the requirements for a standard and global Service Provider/Carrier E.164 managed number resolution system based on ENUM to be used in interconnect routing.

1.2 Scope

This GSMA official document provides recommendations on ENUM to facilitate successful interworking inter-Service Provider services. In particular, guidelines for general and service specific configuration of ENUM servers, GSMA processes and procedures relating to formats, usage of domain names and sub-domain names, and guidelines and recommendations on GSMA Carrier ENUM.

1.3 Definitions

Term	Description
DNS Server	A DNS Server can be a Name server, a Local Caching DNS Server or both. It is common that all DNS Servers cache all results from queries for a specific amount of time.
IPX	GPRS roaming eXchange/IP Packet eXchange. The IPX is an inter-operator IP backbone network that is transparent to subscribers. It is used for back-end routing/tunnelling purposes only.
IPX Domain	Refers to the whole group of business entities comprising interconnected Service Providers and IPX Providers
IPX Provider	A business entity (such as an IP Carrier) offering IP interconnect capability for one or many IPX Services compliant with the IPX PRDs.
IPX Service	An IP based service using the IPX as a means of interconnection that is provided by a Service Provider to an end-user.
Service Provider	The Service Provider who provides the services for a given end user. Originating Service Provider will be named “A”, while destination Service Provider will be named “B” into this document

1.4 Abbreviation

Term	Description
AS	Application Server
CAPEX	Capital Expenditure
CC	Country Code
CNAME	Canonical Name [record]
CS	Circuit Switch
DNS	Domain Name System

ENUM	E.164 Number Mapping
ESP	ENUM Service Provider
FQDN	Fully Qualified Domain Name
GMSC	Gateway Mobile Switching Centre
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
HPMN	Home Public Mobile Network
HSS	Home Subscriber Server
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
I-CSCF	Interrogating Call Session Control Function
IETF	Internet Engineering Task Force
IM	Instant Message
IMS	IP Multimedia Sub-system
IMSI	International Mobile Subscriber Identity
INAP	Intelligent Network Application Protocol
IP	Internet Protocol
IPX	Internet Protocol Packet Exchange
ISUP	ISDN User Part
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunication Standardization Sector
LAN	Local Area Network
LTE	Long Term Evolution
MAP	Mobile Application Part
MCC	Mobile Country Code
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MNC	Mobile Network Code
MNO	Mobile Network Operator
MNP	Mobile Number Portability
MSC	Mobile Switching Centre
NAI	Network Access Identifier
NAPTR	Naming Authority Pointer
NDC	National Destination Code
NNI	Network-Network Interface
NP	Number Portability
NPD	Number Portability Discovery
NPDI	Number Portability Dip Indicator

OPEX	Operational Expenses
O&M	Operation and Maintenance
PMN	Public Mobile Network
PoC	Talk over Cellular
PSTN	Public Switch Telephone Network
QoS	Quality of Service
RCS/RCS-e	Rich Communication Suite/ - enhanced
RR	Requirements
SGSN	Serving GPRS Service Node
SIP	Session initiation Protocol
SMS	Short Message Service
SMTP	Simple Message Transmission Protocol
SN	Subscriber Number
SP	Service Provider
SS7	Signalling System 7 Protocol
TDM	Time-division Multiplexing Protocol
ULR	Uniform Resource Locator
URI	User Resource Identifier
VoLTE	Voice over LTE
VLR	Visitor Location Register

1.5 References

Ref	Document Number	Title
1	IETF RFC 1034	Domain Names - Concepts and Facilities
2	IETF RFC 1035	Domain Names - Implementation and Specification
3	IETF RFC 3761	The E.164 to Uniform Resource Identifiers (URI); Dynamic Delegation Discovery System (DDDS) Application (ENUM)
4	IETF RFC 3401	Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS
5	IETF RFC 3402	Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm
6	IETF RFC 3403	Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database
7	IETF RFC 3404	Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI)
8	3GPP TS 23.003	Numbering, addressing and identification, Version 8.0.0 or higher
9	GSMA PRD IR.52	MMS Interworking Guidelines
11	GSMA PRD IR.65	IMS Roaming and Interworking Guidelines
12	GSMA PRD IR.34	Inter-Service Provider IP Backbone Guidelines

Ref	Document Number	Title
13	IETF RFC 2821	Simple Mail Transfer Protocol
14	IETF RFC 2822	Internet Message Format
15	3GPP TS 23.140	Multimedia Messaging Service (MMS); Functional description; Stage 2, version 6.7.0 or higher
16	IETF RFC 2915	The Naming Authority Pointer (NAPTR) DNS Resource Record
17	IETF RFC 3263	Session Initiation Protocol (SIP): Locating SIP Servers
18	IETF RFC 2782	A DNS RR for specifying the location of services (DNS SRV)
24	IETF RFC 3824	Using E.164 numbers with the Session Initiation Protocol (SIP)
25	IETF RFC 1032	Domain administrators guide
32	ENUMservice Registrations	http://www.iana.org/assignments/ENUM-services
33	IETF RFC 3764	ENUM service registration for Session Initiation Protocol (SIP) Addresses-of-Record
34	IETF RFC 4355	IANA Registration for ENUM services email, fax, mms, ems, and sms
35	3GPP TS 24.229	IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3, version 7.13.0 or higher.
37	ITU-T Recommendation E.164	The international public telecommunication numbering plan
38	IETF RFC 3261	SIP: Session Initiation Protocol
43	IETF RFC 4769	IANA Registration for an ENUM service Containing Public Switched Telephone Network (PSTN) Signalling Information
46	GSMA PRD IR.92	IMS Profile for Voice and SMS
47	RCS Release Docs	RCS 1-4 Release Documents http://www.gsmworld.com/our-work/mobile_lifestyle/rcs/rcs_release_docs.htm
49	GSMA PRD IR.21	GSM Association Roaming Database, Structure and Updating Procedures
51	GSMA PRD IR.67	DNS Guidelines for Service Providers and GRX and IPX Providers
53	GSMA PRD IN.25	Proposed national and international RCS Interworking Requirements
54	GSMA PRD IR.82	Security SS7 implementation on SS7 network guideline
56	IETF RFC 3966	The tel URI for Telephone Numbers
57	IETF RFC 4694	Number Portability parameters for the “tel” URI

2 Number Resolution Requirements

2.1 Number Resolution Requirements

Where a SP (service provider) offers IP (internet protocol) services via a telephone number there is a requirement to translate the phone number into another form of address which is routable in an IP technology domain. This process, where the originating SP discovers the routable destination information and service platform information is called number resolution.

The number resolution solution shall be designed to meet the requirements below:

- Provide IP routable information for a telephone number to enable commonly used routing scenarios.
- Provide a list of service and platform information against a telephone number.
- If NP (number portability) must be taken into account, information of a routable destination to the correct domain must be derivable to ensure connectivity for the service.
- Where legacy TDM/SS7 (time-division multiplexing/signalling system 7) service platforms co-exist with the IP service platform, sufficient information must be provided so routing to the optimal domain within operator constraints would be possible. With this information, related parties will be able to pinpoint where TDM/IP conversions are necessary and minimize TDM/IP (and IP/TDM) conversions.
- If the number resolution is to be done across different SPs, a standard interface must be used. SPs should have the flexibility to participate in a common number resolution framework, whilst retaining the right to implement unilateral commercial/technical solutions with parties outside the framework.

The number resolution solution should be designed to meet the below recommendations:

- The number resolution activity between SPs should take place under secure and private conditions, i.e. the data owner can restrict this data to the required business user group. Steps should be taken to prevent spoofing, fraud, spamming or denial of service attacks if the number resolution systems are susceptible.
- The number resolution approach should enable commonly used routing scenarios, such as internal network routing, national routing and international routing.
- The number resolution approach should be applicable to all commonly used models of interconnection, for example bi-lateral, multilateral and hub.
- The number resolution should be independent of the service and apply to all commonly understood services to simplify network architecture, for example voice, MMS (multimedia messaging service), IM (instant message), Video, RCS (rich communication suite), VoLTE (voice over LTE), and etc. It should also be applicable to a variety of technologies and protocols, for example IMS (IP multimedia sub-system) and SIP (session initiation protocol). Number resolution should be extensible to future services.
- The number resolution system should be applicable to all players in the interconnect ecosystem, such as SPs (fixed and mobile), hubs and National Number Portability Authorities.

- Provide a simple straight forward number resolution solution, where any vendor or SP can offer the functionality. This may result in reducing the CAPEX (capital expenditure) and OPEX (operational expenses).

2.2 Number Resolution Recommendations

GSMA working groups have studied number resolution solutions and recommend the use of ENUM (E.164 number mapping) for number resolution. ENUM is a telephone look up or number resolution technology, standardised by the Internet Engineering Task Force (IETF). It enables number registries to be queried and return lists of end point information relating to a telephone number.

ENUM registries can:

- Provide IP routable information against a phone number
- Provide a list of service/platform information against a number and correction in case of NP

As such ENUM fulfils the number resolution requirements above.

3 ENUM Technology

3.1 Introduction

Telephone numbers compliant with E.164 that identify subscribers cannot be used on their own for addressing in IP based networks. The IETF have defined a mechanism for converting E.164 numbers to an "IP friendly" address relevant to the service that the user wishes to use. IETF RFC 3761 [3] defines the mapping of E.164 numbers to services using DNS (Domain Name System). This mechanism is known as ENUM.

ENUM is only applicable to E.164 numbers (as defined in ITU-T Recommendation E.164 [37]), that are, telephone numbers in their full/international format of CC+NDC+SN (Country Code + National Destination Code + Subscriber Number). If a given dialled number is not in the E.164 number format for example national format, it needs first to be converted to this format. If a given dialled number is a short code or some other type of SP address, it will need to be mapped to an E.164 number, or else, be resolved by a defined reverse lookup function to an E.164 number.

There are two types of ENUM: Public ENUM and Private ENUM. There are a number of different terms used in the telecommunications industry to refer to private ENUM. For example: “Carrier ENUM”, “Infrastructure ENUM” and "Operator ENUM". This document uses the term “Carrier ENUM”.

Public ENUM has the following characteristics:

- Uses the public internet DNS infrastructure.
- End User data is exposed to the “public" and can be read by anyone.
- Uses the “e164.arpa” top level domain.
- Intention is to provide an on-line end user opt in service and application directory.
- Data is populated by end users who choose to opt-in and populate their data.

- Data required to be managed by end user and could be out of date because it is up to the end user to keep it up to date.
- May contain “personal” data if the user desires. There are privacy concerns but placing this data in ENUM is according to user choice.

Carrier ENUM has the following characteristics:

- Uses a private DNS infrastructure
- Provides a private routing enabling technology transparent to the end user.
- Cannot be directly accessed by end users or public Internet users as data is contained within a secure end-to-end network.
- Uses a different top level domain to avoid any detrimental effects caused by unintended leakage to the Internet caused by a misconfiguration in a SPs network.
- Data can only be exchanged by those connected to the private routing infrastructure.
- Data populated by SPs who are the telephone number assignee or their designated Agents.
- Data must follow DNS caching and Time to Live requirements so as to avoid call/session failure.
- Contains data required for call/session routing or network discovery to the destination SP only.

Public ENUM cannot be used on the IPX network (internet protocol packet exchange network), as it is insecure, incomplete, no private and has no guaranteed QoS (quality of service) or data integrity. Therefore, Carrier ENUM should be used on the IPX network. The following sub-sections describe how Carrier ENUM is implemented in the IPX network for inter-SP services (referred as "Carrier ENUM on the IPX").

3.2 General Requirements

Carrier ENUM on the IPX is designed to provide the following high-level requirements:

- A competitive environment, where more than one vendor or service bureau can offer ENUM functionality.
- Equal accessibility, so the ENUM data fill is available to all entities that need it but also restricted to those that do not.
- Accuracy in the data populated, meaning that existing authoritative databases with the required information are accessible to query.
- Support for the establishment of permissions and/or reciprocal business policy agreements between SPs to determine the routing and priorities for managing differing types of network traffic that have requested previous access into a terminating SPs network along with the need to identify the querying party.

3.3 Typical example

Figure 1 shows an IMS example of how ENUM is intended to work during the setup of a simple One to One session. In this diagram the ENUM database is shown as a single global database, which is how it should appear to any organisation that queries it. In practice the ENUM database actually consists of many smaller national databases linked together within the ENUM DNS structure.

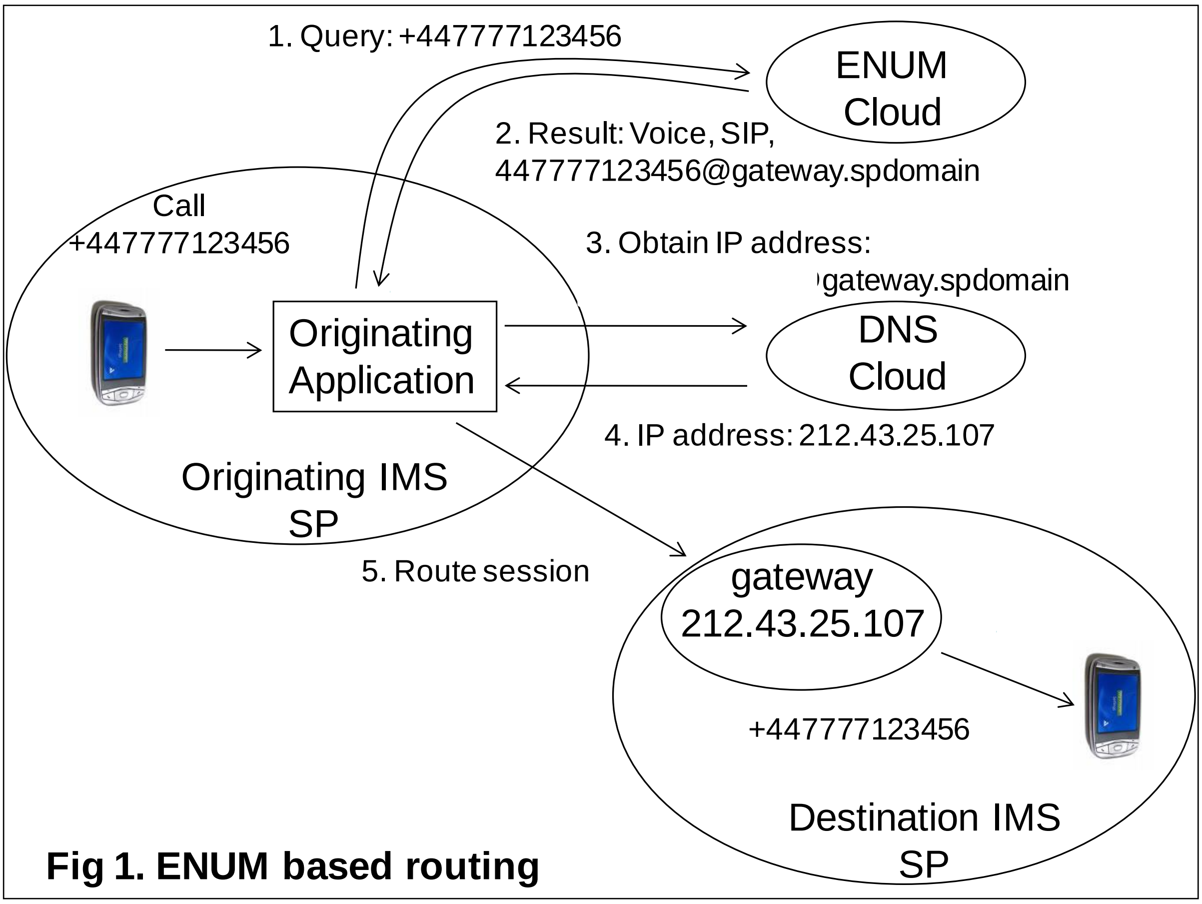


Figure 1 ENUM Based Routing

It should be noted that an ENUM query does not provide a route. It provides another address relevant to the target destination and technology, corrected to solve the NP. Generally, the routing entity will use the ENUM information in combination with commercial policies and the DNS system to determine the route.

4 Architecture

4.1 Hierarchical model

4.1.1 Introduction

The following information details the GSMA recommended structure and delegation model of Carrier ENUM on the IPX network.

In the following architecture model, a hierarchy of ownership is defined. DNS is designed to have a hierarchical structure allowing control of different parts of the overall structure to be established by the destination network's business policies and data access requirements whilst supporting standard DNS tiers. E.164 numbers also have a hierarchical structure and this can be mapped onto the DNS structure on the IPX network.

4.1.2 Data Delegation Structure

To ensure proper distribution and scalability of the DNS structures, ENUM was originally designed to use a strict tiered system, consisting of 3 tiers as follows:

- Tier 0 – Global level
    - Authoritative for the ENUM top level domain.
    - Under this domain are pointers to the Tier-1 authoritative servers.
- Tier 1 – Country Code level (CC)
    - Authoritative for ITU-T (International Telecommunications Union – Telecommunication Standardization Sector) assigned E.164 country codes.
    - Under this domain are pointers to the Tier-2 authoritative servers.
- Tier 2 – Service Provider level (NDC)
    - Authoritative for NDC and individual Subscriber Numbers.
    - Under this domain are the individual Subscriber Numbers. Each one of them has one or more (Naming Authority Pointer) NAPTR records associated to them.

This is depicted as follows, where the arrows show delegation:

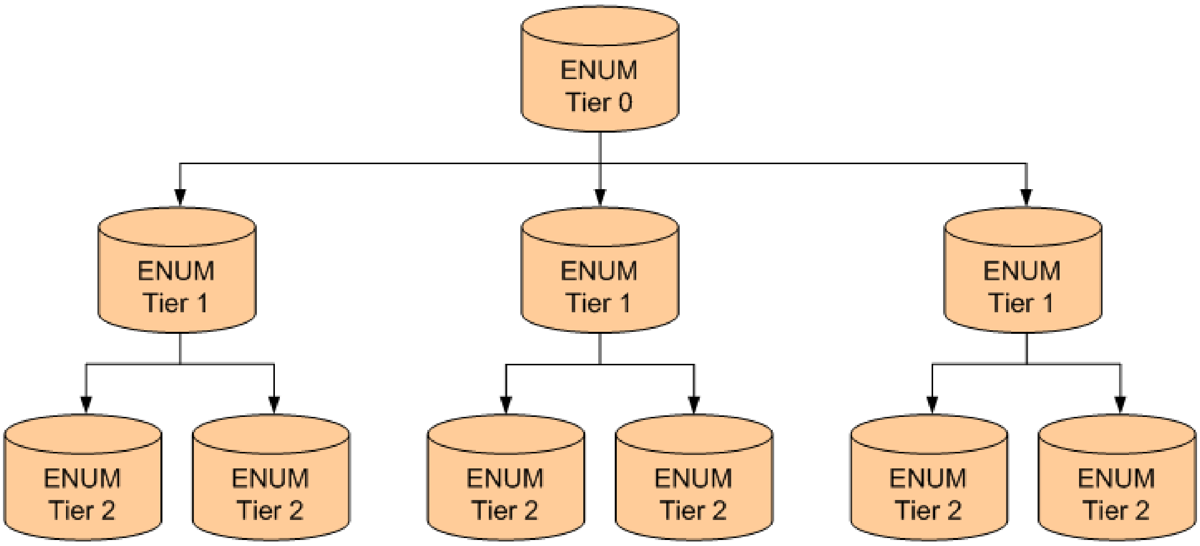


Figure 2 ENUM logical hierarchy

The ENUM hierarchy described above is logical, and does not require each logical ENUM Tier to be mapped to individual ENUM servers. The logical architecture allows flexibility when it comes co-locating different tiers of the ENUM hierarchy onto ENUM servers. Figure 3 provides some examples of possible co-location of the logical Tiers onto physical ENUM servers.

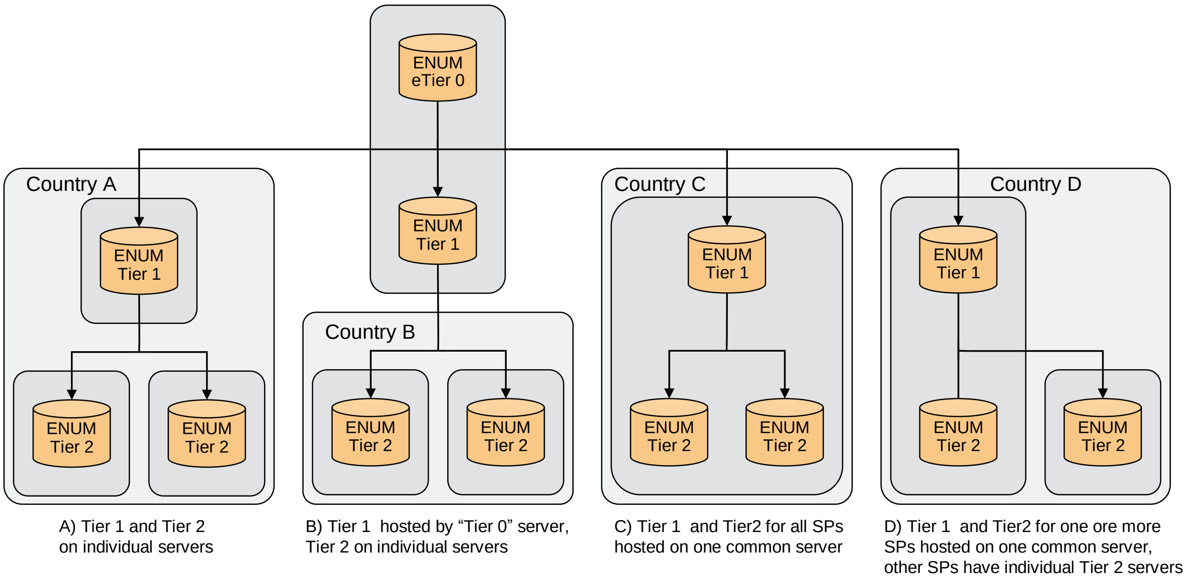


Figure 3 Logical architecture for Carrier ENUM on the IPX

Figure 3 provides only a set of examples on how the logical Tiers can be mapped onto ENUM servers, and does not preclude other configurations such as co-locating both Tier-1 and Tier-2 for a country on the Tier-0 server neither the possibilities to support further Tiers below Tier-2 if needed. The possibility to support several Logical Tiers for different countries on one ENUM server is also possible allowing a SP with operations in several countries to co-locate the logical Tier-2 for all or several countries on a common multi-country Tier-2 ENUM server.

In countries where SP Number Portability is employed, this flexibility of the ENUM server and Tier structure allows each individual country to agree on different types of arrangements of the ENUM structure suiting the situation and requirements of that specific country.

Therefore, Carrier ENUM on the IPX builds upon this tiered structure, including the flexibility to allow diverse national level, and SP level implementation strategies. The following diagram depicts the overall logical architecture for Carrier ENUM on the IPX.

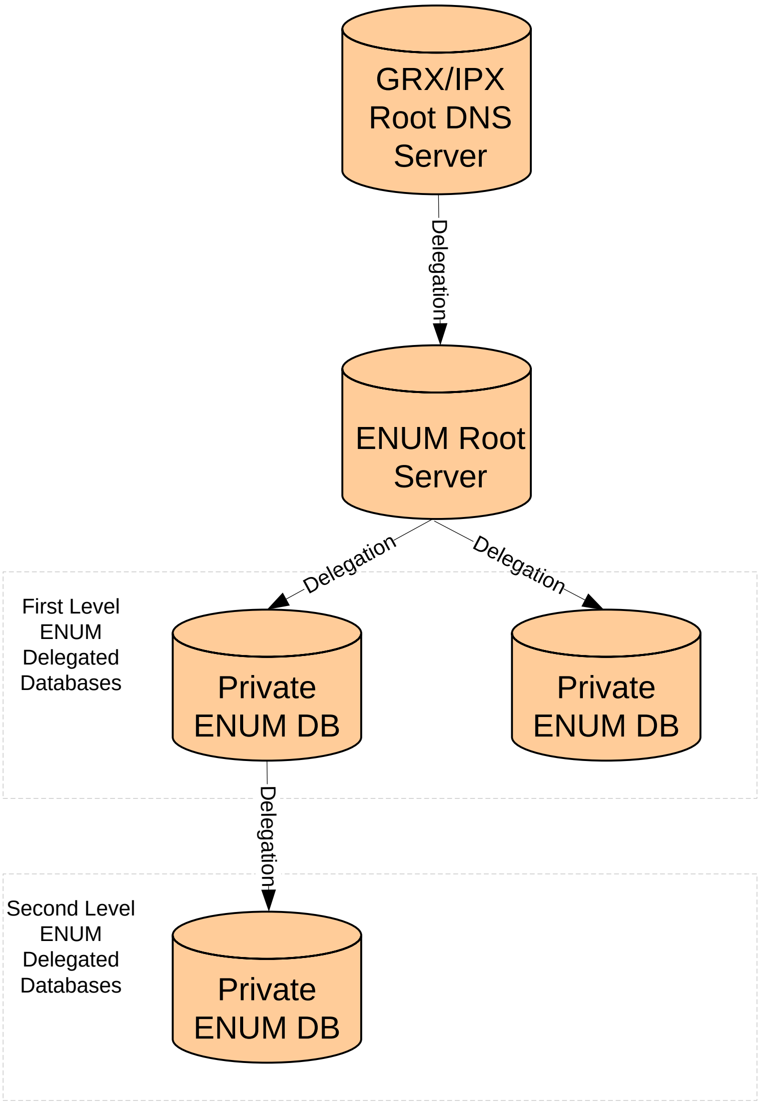


Figure 4 Logical architecture for Carrier ENUM on the IPX

NOTE 1: Represented in the above figure are *logical* entities and thus one or more instances of those logical entities can be offered by one physical server.

NOTE 2: The IPX Root DNS Server delegates to the ENUM Root Server the agreed Carrier ENUM on the IPX top level domain name, as detailed in section 4.2.2. The ENUM Root Server and all Private ENUM databases located directly or in-directly below are different delegated parts of the E.164 number (which commonly, although not always, align to the CC, NDC and SN).

In practice there are many considerations relating to DNS delegation. Who maintains data integrity and has control of particular ENUM databases and E.164 number ranges is of concern to SPs, specifically in countries where numbers are portable between mobile and fixed operators and there are potentially a large number of organisations involved. In the "real world" the delegation structure may not follow the model shown above and different Tiers may share the same server and delegation model.

Commercial arrangements for DNS/ENUM delegation, control and administration are not described in this document. The scope is restricted to describing technical details only.

4.1.3 Resolution procedure

A given E.164 number is converted to a FQDN (Fully Qualified Domain Name) using the procedure described in IETF RFC 3761 [3]. The resultant FQDN used in Carrier ENUM on the IPX slightly differs from the definition in IETF RFC 3761 [3], and is defined below in section 4.2.2.

IPX Carrier ENUM utilises the IPX DNS structure. Therefore, a Slave IPX Root DNS Server is queried first, then the ENUM Root Server, and then one or more Private ENUM Database servers, until a final result is obtained.

The following depicts an example of successful ENUM resolution using Carrier ENUM on the IPX.

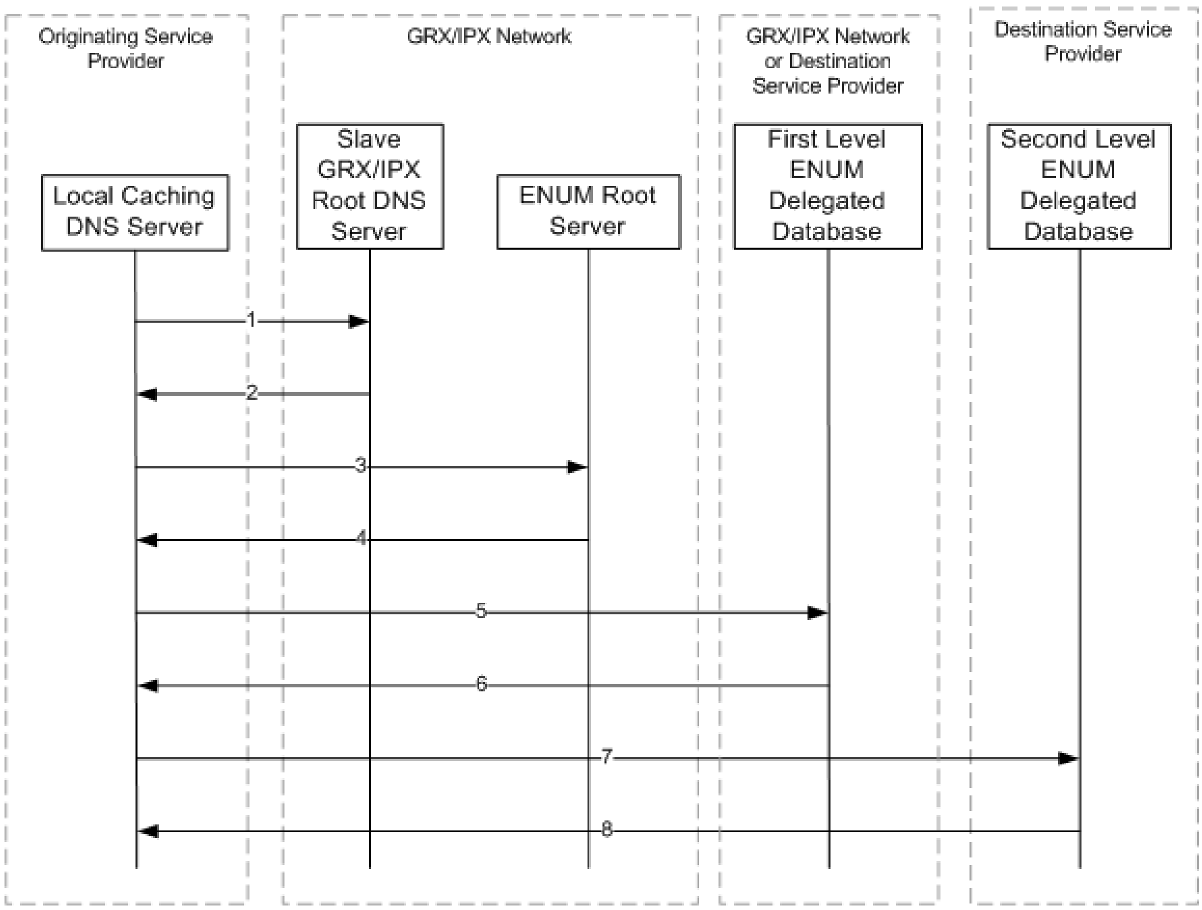


Figure 5 Example ENUM resolution for an IMS session establishment

The numbers in the messages in the above diagram refer to the below:

1. Originating SP's Local Caching DNS Server sends the DNS query to the IPX Root DNS Server.
2. IPX Root DNS Server replies with a referral to the ENUM Root Server.
3. Originating SP re-sends the DNS query, but to the ENUM Root Server.
4. ENUM Root Server replies with a referral to the First Level ENUM Delegated Database Server.

5. Originating SP re-sends the DNS query to the First Level ENUM Delegated Database Server.
6. First Level ENUM Delegated Database Server replies with either a referral to a Second Level ENUM Delegated Database Server, or a final result.
7. If a referral was received, then Originating Service Provider re-sends the DNS query to the Second Level ENUM Delegated Database Server.
8. Second Level ENUM Delegated Database Server replies with a final result.

NOTE 1: As per normal DNS procedures, each reply that a SP receives is retained for a certain amount of time allowing some later queries to be answered from the cache instead of always querying other DNS/ENUM servers.

NOTE 2: The originating SP may apply an optional policy check upon receiving any response.

It is recommended no more than two ENUM Delegated Databases (that is First Level and Second Level) to be provisioned in a resolution "chain" for an E.164 number. However, an originating SP for ENUM queries needs to be able to query at least as many queries as there are labels in the ENUM FQDN, which is more than recommended (see section 4.3).

4.1.4 Access to ENUM servers and Interconnection policy

SPs connected to the IPX network will be able to perform an ENUM Query and obtain a result dependant on the policy established for data accessibility. That is, either the querying SP has access to all ENUM servers, or, an error is returned (see section 4.2.3 for more details on responses).

In some instances, it is possible to resolve an E.164 number to a URI (user resource identifier), even though there is no interconnection agreement (commercial or technical) with the target SP for the identified service. This may happen to an originating SP in a number of cases, including (but not necessarily limited to) the following:

- Where access to the ENUM Tier-2 is available due to interconnection agreement with the destination SP, but for a different service for example Push to Talk over Cellular (PoC) agreement in place but no agreement for Voice/Video Share (both services are based on IMS and hence use the same URI scheme).
- Using a localised ENUM architecture, such as that detailed in Annex B.
- Automatic derivation of the URI from the E.164 number for example MAP_SRI_For_SM look-up (also known as an "IMSI look-up"), back-end connection to a number range database (for example an MNP, mobile network portability database), static look-up table of E.164 number block data assignment. For examples of architectures, see Annex B.

In such a case, extra analysis needs to be performed by the originating SP on the derived URI in order to check local policies on interconnection with regards to both the Destination Operator and the service being requested by the subscriber. Such a policy should also dictate which interconnect address or third-party interconnect provider should be used for routing the service.

For example, policy checking could take place in the service node (for example. MMSC, S-CSCF, AS), or, it also could take place in the local DNS caching server that is taking care of the ENUM resolution. For both cases, there are commercially available solutions.

4.1.5 Number Portability considerations

NP implementations differ from country to country, based on national requirements and organisation of NDCs, thus there is no single solution that suits all countries. Therefore, the ENUM architecture implemented by SPs who are part of a NP "group", need to provide a common approach between them.

Different implementation options for the support of NP can be identified, where some rely on the involvement of the Tier-1 as:

- Combined Tier-1 and Tier-2 ENUM database, at least per NP "group"
- Intelligent Tier-1 ENUM database that always redirects the querying entity to the currently serving SP

NOTE: See Annex C for more information

Other implementation options do not rely on the involvement of the Tier-1 and are managed solely based on the SP Tier-2 which includes:

- Redirection from Tier-2 of number range owning SP to the Tier-2 of the currently serving SP
- Final response from the Tier-2 of the number range owning SP on behalf of the Tier-2 of the currently serving SP

The NP resolution may be based on information that is natively stored on the ENUM server. Also the Tier-1 or Tier-2 servers may interact in real-time with legacy systems for NP to derive information about the currently serving SP, and provide responses based on this information.

Another aspect of NP that needs to be considered is when the Tier-1 redirects queries to the Tier-2 of the number range owning SP, which shall provide responses to cater for ported numbers. In case not all SPs within an “NP group” participates in the IPX Carrier ENUM, there is no “natural” Tier-2 server that would be the first to query and therefore would cater for numbers that are ported out from that SP.

4.2 ENUM interface definition

4.2.1 Introduction

The following sections specify the agreed implementation details for ENUM on the IPX network so that it is fully interoperable between all network entities.

4.2.2 ENUM Query

Carrier ENUM on the IPX reuses the ENUM Query procedures and format as described in IETF RFC 3761 [3], with the exception that the top level domain name "e164enum.net" shall be used instead of "e164.arpa". For example, for the E.164 number 447700900123, the translated ENUM FQDN to be resolved would be 3.2.1.0.0.9.0.0.7.7.4.4.e164enum.net.

Therefore, all ENUM Servers that are part of the Carrier ENUM for IPX shall support ENUM queries to this ENUM FQDN.

NOTE: In addition to "e164enum.net", other top level domains may also be supported (for example in accordance with local in-country ENUM requirements); however, they must follow "e164enum.net" service requirements. Only "e164enum.net" is mandatorily required for Carrier ENUM on the IPX.

The top level domain name "e164enum.net" has been chosen for Carrier ENUM on the IPX for the following reasons:

- To ensure there is no conflict with Public ENUM.
- It is registered on the Internet to GSMA
- Neutral to service provider technology i.e. neutral between mobile/fixed SPs and IPX Providers
- Has an indication of its purpose that is E.164 and ENUM
- The “.net” suffix was felt to be relevant to the use of this domain. From IETF RFC 1032 [25]:

".net" was introduced as a parent domain for various network-type organizations. Organizations that belong within this top-level domain are generic or network-specific, such as network service centres and consortia. ".net" also encompasses network management-related organizations, such as information centres and operations centres.

4.2.3 ENUM Response

4.2.3.1 General

All ENUM queries to the mandatory FQDN for Carrier ENUM on the IPX as defined in section 4.2.2 shall return a result that should never be discarded by an ENUM server, firewall and so on (for example due to access control lists). The result returned can be a pointer to another ENUM Server, a final result (that is list of URIs/URLs (User Resource Identifier

/uniform resource locator) or a standard DNS/ICMP error (domain name system/internet control message protocol error).

In order to avoid querying entities having to support multiple NP solutions, terminating SPs in countries that use NP need to provide NP corrected data in their final results. Such NP corrected final results should avoid relying upon the querying entity supporting any nationally required NP solution, local to the terminating SP.

The Number Resolutions RR (as defined in IETF RFC 1034 [1]) shall be used to provide a pointer to the next ENUM Server to query.

The NAPTR RR (as defined in IETF RFC 3403 [6] and IETF RFC 3761 [3]) shall be used to return a successful final response. It should be a list of URIs/URLs for different services. The following sections provide recommendations on how to populate the fields of the NAPTR Requirements.

4.2.3.2 URI formats

The domain name part of URIs returned in NAPTRs shall be in the format detailed in section GSMA IR.67 [51]**Error! Reference source not found.** of the present document, to enable routing through the IPX network using the current IPX DNS.

4.2.3.2.1 SIP/IMS URI format

The SIP/IMS URI format is:

```
sip:+<E.164_number>@<xxx>.mnc<MNC>.mcc<MCC>.3gppnetwork.org;user=phone
```

Where "<xxx>" can be any characters or null (if null, then the trailing "." shall not be present), and <MNC>/<MCC> are the MNC/MCC (mobile network code/mobile country code) allocated to the SP. Other domain names that are routable on the inter-Service Provider IP network may also be used.

"`sip:`" indicates the protocol to be used which in this case is SIP.

With regard to the "<xxx>" prefix there was no consensus on using any specific value of "<xxx>". However, in order to avoid conflicts with sub-domains allocated already and any possible new sub-domains for new services, the sub-domain of ".ims" is recommended.

The SIP URI parameter "user=phone" is included to explicitly indicate that the user part contains an E.164 number and is recommended in all cases. For operators that provision the SIP URI NAPTR RR only for IMS subscribers, the SIP URI parameter "user=phone" could be excluded as long as the same SIP URI is also provisioned in their HSS (home subscriber server). For operators that provision the SIP URI NAPTR RR for both IMS and non-IMS subscribers, they should always include the SIP URI parameter "user=phone" in the SIP URI of the NAPTR RR.

The following examples are all acceptable NAPTR RR SIP URIs for IMS where the E.164 number is 447700900123, the MNC is 01 and the MCC is 234:

```
sip:+447700900123@mnc001.mcc234.3gppnetwork.org
sip:+447700900123@ims.mnc001.mcc234.3gppnetwork.org
sip:+447700900123@mnc001.mcc234.3gppnetwork.org;user=phone
sip:+447700900123@ims.mnc001.mcc234.3gppnetwork.org;user=phone
```

For SPs who offer IMS based services it is recommended that, where possible, all of that SPs subscribers should be provisioned with a SIP URI. However, SPs should be warned that if a subscriber who does not have an HSS (home subscriber server) entry, then is provisioned with a NAPTR RR containing a SIP URI without the SIP URI parameter "user=phone" and this may result in SIP sessions/calls failing indefinitely as the I-CSCF (interrogating call session control function).
handling the incoming session, after not finding any corresponding users in the HSS (, it may not be able to request routing based on the E.164 number that is contained in the SIP URI, due to the absence of "user=phone"). This is in contrast to when no SIP URI NAPTR RR is provisioned for the user and the session/call is alternatively delivered via the PSTN by the originating SP.

It is recommended that a SP should always include the SIP URI parameter “user=phone” in the SIP URI NAPTR RR and configure and set the I-CSCF to support the “local configuration option” to attempt request routeing using the E.164 number derived from the SIP URI as described in Section 5.3.2 of 3GPP TS 24.229 [35] when the I-CSCF receives the response to the location query from the HSS indicating that the user does not exist.

4.2.3.2.2 SIP-I/Packet Voice Interconnect URI format

The same recommendations as in section 4.2.3.2.1 apply here, with the exception that the sub domain labelled “<xxx>" is recommended to be "sip-i" or be absent/null. This is recommended in order to avoid conflicts with reserved sub-domains and any possible new sub-domains for new services.

4.2.3.2.3 MMS URI format

The MMS ENUM URI domain format is the following:

```
mailto:+<E.164_number>/TYPE=PLMN@mms.mnc<MNC>.mcc<MCC>.gprs
```

where <MNC>/<MCC> are the MNC/MCC allocated to the SP.

The “mailto:” prefix indicates the protocol to be used which in this case is SMTP. It should be noted that this prefix used to be "mms:", however, the use of this prefix is now deprecated and should no longer be used. For more information, see 3GPP TS 23.140 [15].

The following example is an acceptable mailto URIs for MMS where the E.164 number is 447700900123, the MNC is 01 and the MCC is 234:

```
mailto:+447700900123/TYPE=PLMN@mms.mnc001.mcc234.gprs
```

For SPs who offer MMS it is recommended that, where possible, all of that SPs subscribers should be provisioned with a MMS URI. This allows fall MMS interconnecting SPs to utilise ENUM instead of MAP (mobile application part) (in order to determine the destination SP and thereby reduces the load on that SPs HLR.

4.2.3.3 ENUMservice field

4.2.3.3.1 Introduction

The ENUMservice field appears in the NAPTR records for a particular E.164 number. It describes the services supported by that number. See section 4.2.3.4 for an example. The following are recommended values to be used for different services.

4.2.3.3.2 SIP/IMS

The ENUMservice to be used for IMS is “E2U+SIP” as specified in IETF RFC 3764 [33].

4.2.3.3.3 SIP-I/Packet Voice Interconnect

The ENUMservice to be used for SIP-I/Packet Voice Interconnect is "E2U+PSTN:SIP" as specified in IETF RFC 4769 [43].

4.2.3.3.4 MMS

The ENUMservice to be used for MMS is “E2U+MMS:mailto” as specified in IETF RFC 4355 [34].

It should be noted that this ENUMservice used to be "mms+E2U". However, use of this ENUMservice field value is now deprecated and should no longer be used. For more information, see 3GPP TS 23.140 [15].

4.2.3.3.5 Other services

The value for the ENUMservice field to be used for any other service that uses the GSMA Carrier ENUM service should seek to reuse those values that have been reserved with IANA as detailed in the List of ENUMservice Registrations [32]. Private/non standardised ENUMservice field values should be avoided and instead, registration with IANA should be sought (as per the IANA (Internet Assigned Numbers Authority) registration process defined in IETF RFC 3761 [3]).

4.2.3.4 Example NAPTR RR

The following shows an example of the E.164 number +447700900123 that supports SIP/IMS, SIP-I/Packet Voice Interworking and MMS, in a SP's network with E.212 number range of MNC 01 and MCC 234 allocated to it. Note that the $ORIGIN statement is used here to ensure correct syntax and would have limited use in a large scale, live DNS.

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
    3.2.1.0.0.9 NAPTR 100 10 "u" "E2U+SIP"
                   "!^.*$!sip:+447700900123@ims.mnc001.mcc234.3gppnetwork.org;user=phone!" .
                NAPTR 100 10 "u" "E2U+PSTN:SIP"
                      "!^.*$!sip:+447700900123@sip-i.mnc001.mcc234.3gppnetwork.org!" .
                NAPTR 100 10 "u" "E2U+MMS:mailto"
                      "!^.*$!mailto:+447700900123/TYPE=PLMN@mnc001.mcc234.3gppnetwork.org!" .
```

The querying application asks the DNS for all the NAPTR records for a given E.164 number. There may be multiple NAPTR records returned as in this example. The querying application then selects the NAPTR record(s) that contains the desired service(s), and discards the rest.

The "u" flag indicates the result of this lookup is a URI. The last part of the NAPTR is a Regular Expression and the querying application applies the Regular Expression to the query string (that is the E.164 number) to get the result. In the example above the pattern of "^.*$" instructs the application to match all and any text from the start to the end of the query string (that is the E.164 number) and replace it with the following string delimited by the following two "!", which contains a complete URI/URL.

As an alternative to including a complete URI/URL, many DNS/ENUM servers make use of the input regular expression operator ("\1"). This instructs the querying application to insert the query string (that is the E.164 number used for the query) wherever it appears. This saves repeating of the E.164 number itself in the URI/URL.

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
    3.2.1.0.0.9 NAPTR 100 10 "u" "E2U+SIP"
                   "!^(.*)$!sip:\\1@ims.mnc001.mcc234.3gppnetwork.org;user=phone!" .
                NAPTR 100 10 "u" "E2U+PSTN:SIP"
                   "!^(.*)$!sip:\\1@sip-i.mnc001.mcc234.3gppnetwork.org!" .
                NAPTR 100 10 "u" "E2U+MMS:mailto"
                   "!^(.*)$!mailto:\\1/TYPE=PLMN@mnc001.mcc234.3gppnetwork.org!" .
```

Here the pattern “^(.*)$”instructs the application to match all and any text from the start to the end of the application user string (AUS; that is the E.164 number) and replace it with the following string delimited by the following two “!”.

This string contains the “backref” “\\1” (the first “\” being an escape character) instructing the application to insert the first matching group extracted from the AUS.

The resulting URIs/URLs returned by these regular expressions are evaluated as in the first example provided previously.

Here the pattern “^(.*)$” instructs the application to match all and any text from the start to the end of the application user string (AUS; that is the E.164 number) and replace it with the following string delimited by the following two “!”.

This string contains the “backref” “\\1” (first “\ ” is an escape character) and instructs the application to insert the first matching group extracted from the AUS.

The resulting URIs/URLs returned by these regular expressions are evaluated as in the first example.

4.3 ENUM Proxy

At the operational side, this ENUM hierarchical model, defined in section 4.1, is really difficult to setup worldwide for two main reasons:

- There is no NP management in the international backbone: ENUM Hierarchical model may not be available and /or NP is not applicable within the country. Indeed, for the majority of countries, the handling portability solution is still based on “legacy” solution without ENUM interface. Moreover, some countries have legal constraints which could limit the national NP database access from international entities.
- Customer Data Exposure is still a real issue: ENUM Tier-2 (Service Provider level) may not be open to external queries: some IMS SPs do not intend to open ENUM servers to external queries for security reasons.

The goal of the next section is to present an ENUM Framework, enabling the IMS interconnection and complementing the ENUM hierarchical model with various options of non-ENUM interrogations.

4.3.1 ENUM Framework architecture

The ENUM Framework will capitalise on the ENUM hierarchical model defined section 4.1 and will propose a complementary solution while waiting for the availability and interconnection of all ENUM Tier-0/1/2.

To reach this objective, NNI selection will be also available through non ENUM components, such as current signalling that is able to retrieve SP identity or user profile information of the destination.

In order to integrate ENUM and non ENUM environments, a new component, called ENUM proxy, is proposed: the ENUM Proxy will be able to retrieve the routing information from ENUM or non ENUM domains.

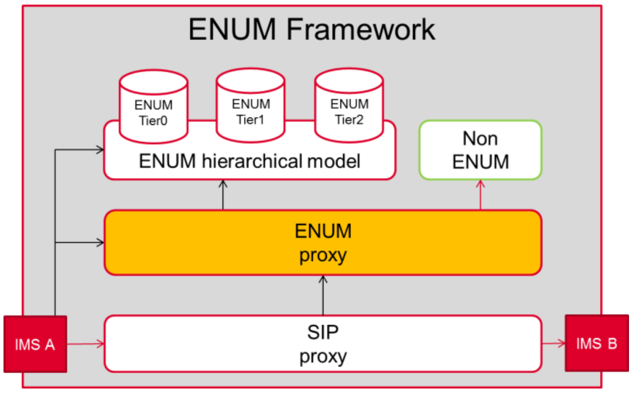


Figure 6 ENUM Proxy

4.3.2 Functional Node Description

The ENUM proxy could be divided into 2 sub-components, implementing two major functions in order to support the IMS interconnection and handle SIP messages from IMS A to B:

- ENUM proxy 1: discovery of the destination SP (with NP taken into account)
- ENUM proxy 2: retrieval of the IMS destination profile

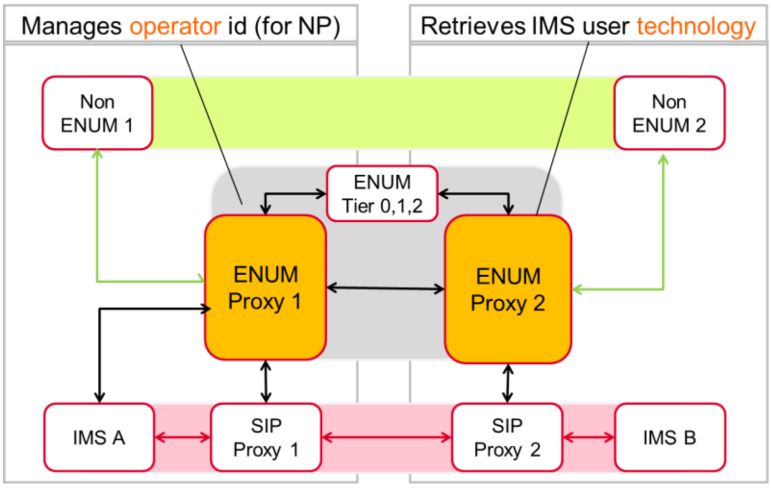


Figure 7 ENUM Proxy functional description

The ENUM proxy could retrieve information from both environments, ENUM and non-ENUM.

- ENUM: using ENUM interface and various Tier-0/1/2
- Non-ENUM: using other signalling like MAP, Diameter or SIP

Notes:

- The ENUM Framework could be seen as an end-to-end approach, including all the ENUM hierarchical model, the non-ENUM interfaces, but also the SIP call routing from IMS A to IMS B.
- The ENUM Framework could be used for different architectures, for bilateral or multilateral approaches; the NNI selection (Network-Network Interface selection) could be done by various SPs (origin or destination) or by the carriers

- ENUM proxy could store the subscriber routing information into a cache (like DNS architecture) for performance matters and in order to avoid ENUM or Non-ENUM queries for each IMS session setup
- A unique IMS NNI per destination SP will be discovered by the ENUM framework, even in case of multi IMS platforms designed at the destination SP. It will be the responsibility of the B SP to route to the appropriate IMS platform.
- ENUM proxy will also resolve Customer Data Exposure by limiting data access via the ENUM proxy.

4.3.3 Interface description

The key feature of ENUM framework is to standardize how destination user information could be exchanged between ENUM proxies, non ENUM components and SIP nodes, especially for SP identity and user profile of the destination.

Note:

- Interface names are only referred to this report.
- All components into this technical framework are optional, except IMS A & B; various use cases will be described later, like the bilateral case without SIP proxies or Routing on Numbering Range without ENUM proxies

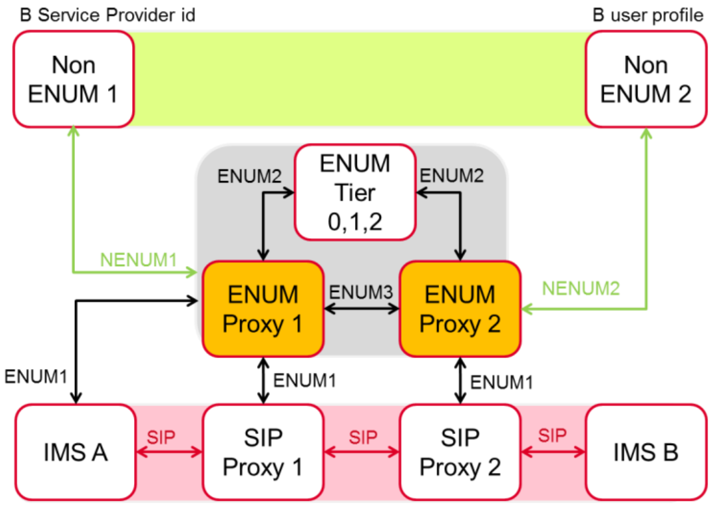


Figure 8 ENUM Framework: Interfaces definition

<u>ENUM (E):</u>

- ENUM1 is an ENUM interface used by IMS and/or SIP Proxy to query ENUM Proxy
- ENUM2 is an ENUM interface used by the ENUM Proxy to query ENUM hierarchical model using ENUM FQDN format like 9.8.7.6.5.4.3.2.1. e164enum.net for “+123456789” E.164 number as defined in section 4.2.2).
- ENUM3 is an ENUM interface used to exchange information between ENUM proxy1 and ENUM Proxy2 when they are interconnected.

<u>SIP (S):</u>

- SIP interface used to manage the IMS session between the SIP nodes (IMS A, SIP proxies, IMS B)

Non ENUM (NE):

- NENUM1 is a Non ENUM interface used to query external database able to provide the destination SP identity.
- NENUM2 is a Non ENUM interface used to query external database able to provide the destination user profile.

4.3.4 ENUM/SIP interfaces

4.3.4.1 SIP/IMS URI format

On the ENUM and SIP interfaces of the ENUM framework, addressing must be specified to assure interworking between the SIP Proxy and/or ENUM proxy provided by different entities or suppliers.

It is especially important to standardize the SIP/IMS URI format (sip:+<E.164_number>@<domain>;user=phone) to be used in the ENUM response and to be routed in the SIP signalling for the IMS session setup.

In fact, SIP/IMS URI format could be adapted depending of the status of the knowledge of the 2 following parameters of the destination:

- Service Provider identity
- user profile

The following table summarises, for different states, the NNI selection which could be performed by IMS A, SIP proxy 1/2 or IMS B:

Service Provider Identity	User Profile	NNI Selection
yes	IMS	Select IMS NNI
yes	Non IMS (or tel)	Break out to legacy NNI (if applicable)
yes	Unknown	Continue the IMS session setup
Unknown	Unknown	Continue the IMS session setup

In order to carry this state node by node in ENUM or SIP, domain names will be adapted with the following structure: <service>.<Service Provider identity>

Where

- <service> could identify the user profile knowledge (ims, tel, ukn) as defined in the previous table
- <Service Provider identity>
    - mnc<MNC>.mcc<MCC>3gppnetwork.org for mobile network operators
    - Non mobile networks could use SPN identifier to replace MCC/MNC

Additionally, npdi (Ref.9, number portability dip indicator) parameter could be used in the SIP messages to indicate that NP resolution was performed correctly.

4.3.4.2 ENUM/SIP basic use cases

In order to clarify the different cases described in the previous section, the four basic scenarios will be illustrated hereafter.

ENUM query result: Service Provider is known and profile is IMS

SIP proxy 1 (or IMS A) will send a standard ENUM query (9.8.7.6.5.4.3.2.1. e164enum.net) to ENUM proxy 1 in order to resolve NP and discover user profile. ENUM proxy 1 will be able to resolve NP and will add in the domain name the MCC/MNC information. ENUM proxy 2 will discover the IMS user and reply with an “ims” prefix in the domain name.

SIP proxy 1 (or IMS A) will then select a IMS NNI and route to the next SIP node (SIP proxy 2 or IMS B) by sending an INVITE with sip:+123456785@ims.mnc<MNC>.mcc<MCC> 3gppnetwork.org;user=phone

Npdi flag could be added in the SIP INVITE in order to indicate that NP resolution was performed correctly (tel:+123456785;user=phone; npdi

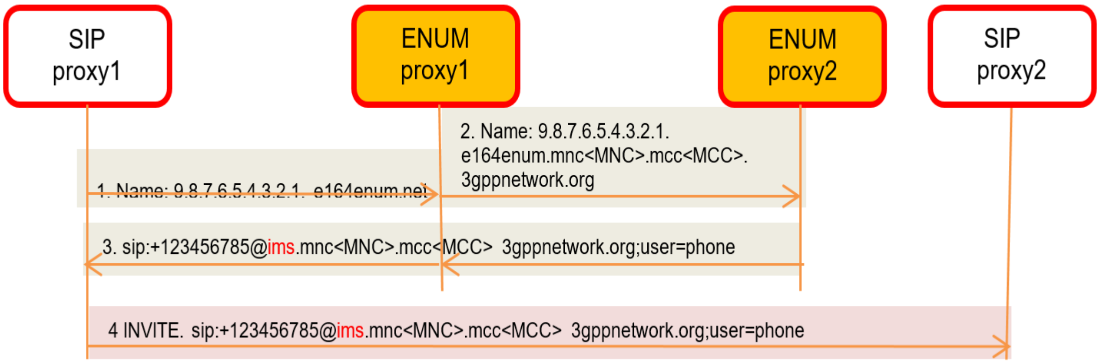


Figure 9 Basic use case: SP id defined and IMS user

ENUM query result: Service Provider is known and profile is not IMS

SIP proxy 1 (or IMS A) will send a standard ENUM query (9.8.7.6.5.4.3.2.1. e164enum.net) to ENUM proxy 1 in order to resolve NP and discover the user profile. ENUM proxy 1 will be able to resolve NP and will add in the domain name the MCC/MNC information. ENUM proxy 2 will discover the non IMS user and reply with “no such name”.

SIP proxy 1 (or IMS A) will then select a non IMS NNI

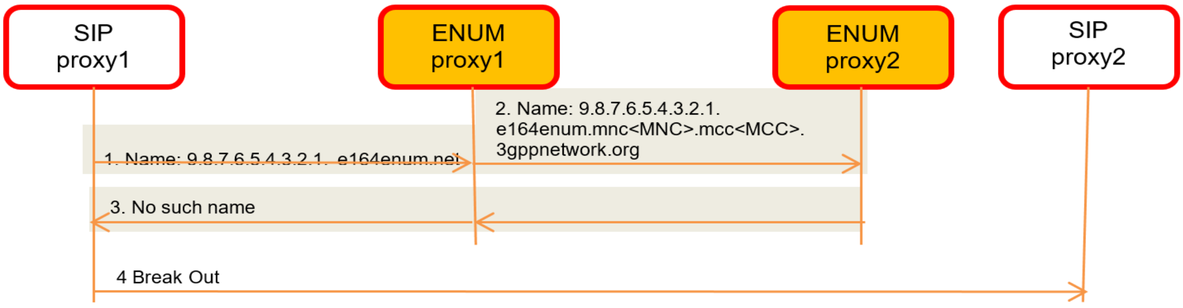
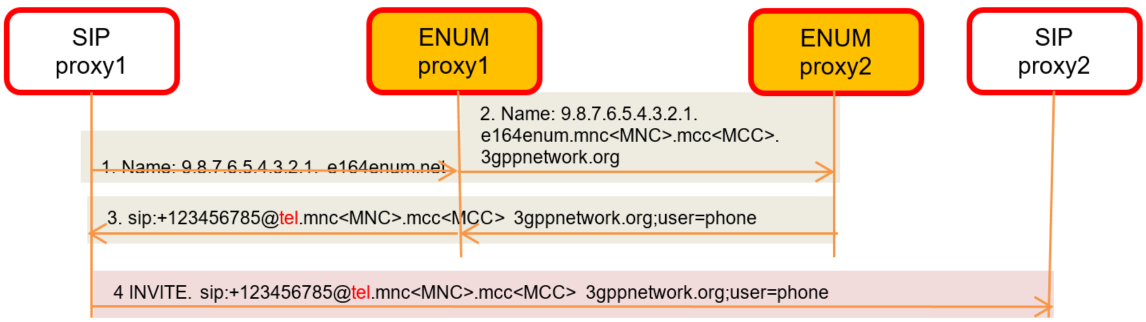


Figure 10 Basic Use Case: SP Id defined and not IMS user

ENUM query result: Service Provider is known and profile is unknown

SIP proxy 1 (or IMS A) will send a standard ENUM query (9.8.7.6.5.4.3.2.1. e164enum.net) to ENUM proxy 1 in order to resolve NP and discover user profile. ENUM proxy 1 will be able to resolve NP and will add in the domain name the MCC/MNC information. ENUM proxy 2 will not be able to discover the user profile and reply with a “tel” prefix in the domain name.

SIP proxy 1 (or IMS A) will then select a IMS NNI and route to the next SIP node (SIP proxy 2 or IMS B) by sending an INVITE with sip:+123456785@tel.mnc<MNC>.mcc<MCC>



3gppnetwork.org;user=phone

Npdi flag (number portability dip indicator flag) could be added in the SIP INVITE in order to indicate that NP resolution was performed correctly (tel:+123456785;user=phone;npdi

Figure 11 Basic use case: SP id defined and unknown user

ENUM query result: Service Provider and profile are unknown

SIP proxy 1 (or IMS A) will send a standard ENUM query (9.8.7.6.5.4.3.2.1. e164enum.net) to ENUM proxy 1 in order to resolve NP and discover the user profile. ENUM proxy 1 will not be able to resolve NP and will reply with a “ukn” prefix in the domain name. MCC/MNC could be fill in with the MCC/MNC of the owner of the numbering range

SIP proxy 1 (or IMS A) will then continue the IMS session and route to the next SIP node by sending an INVITE with tel:+123456785;user=phone

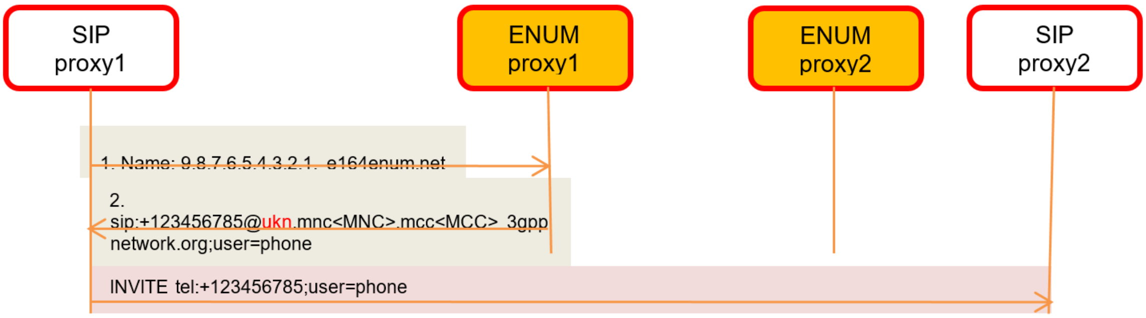


Figure 12 Basic use case: SP id not defined and unknown user

4.3.5 Non ENUM1 interface

If ENUM interfaces are not available, Non ENUM 1 (NENUM1) interface may be used to query Non ENUM databases to retrieve information related to the SP of the destination taking into account NP.

The table hereafter describes the different databases which could be interrogated, the associated protocol used and the message(s) and parameter(s) containing relevant information.

Most of those interfaces could be considered as private interfaces between ENUM proxy and those external databases and will not be detailed into this document due to this private characteristic.

Additionally, some interfaces could be considered as public interfaces because they are more related to widely open and deployed databases like HLR or HSS (generally accessible for roaming and/or interconnection): such standardized interfaces will be detailed in the next sections (MAP, Diameter).

NENUM1				ENUM1/3
Database	**Protocol**	**Msg**	**Parameter**	**Parameter**
HLR	MAP	SRIforSM SendImsi	MCC-MNC (IMSI)	MCC-MNC
HSS	DIAMETER	SRIforSM	MCC-MNC (IMSI)	MCC-MNC
SIP	SIP	SIP 302 Redirect	-prefix (inside a tel URI or inside the user part of a SIP URI) -"rn" parameter (inside a tel URI or inside the user part of a SIP URI) -domain name inside the host part of a SIP URI	MCC-MNC
NP Aggregator	Non ENUM (as defined in section 4.2)	ENUM	MCC-MNC and/or SPN	MCC-MNC
NP Aggregator	WS (Web Service)	GET	MCC-MNC	MCC-MNC

Table 1 Different databases which could be interrogated

4.3.5.1 MAP

Various MAP messages (defined in 3GPP TS 29.002) could be used to retrieve MCC-MNC information and are described hereafter:

MAP_SendRoutingInfoForSM

This service is used between the gateway MSC (mobile switching Centre) and the HLR to retrieve the routing information needed for routing the short message to the servicing MSC.

Map_SendIMSI.

This service is used by a VLR (visitor location register) in order to fetch the IMSI of a subscriber in case of some Operation & Maintenance procedure where subscriber data is needed in the Visited PLMN and MSISDN is the only know subscriber's identity.

> Note: Due to SS7 vulnerability, some SPs could anonymise the IMSI, but MCC/MNC information will be still provided in order to solve MNP issue (as described in GSMA IR.82 [54]).

4.3.5.2 DIAMETER

Various DIAMETER (defined in RFC 3588) messages could be used to retrieve MCC-MNC information

3GPP TS 29.338 – S6c Interface - Send Routing Info for SM procedure

This procedure shall be used between the SMS-GMSC (short message service – gateway mobile switching centre) or the IP-SM-GW (IP-short message-gateway) and the HSS to retrieve the routing information needed for routing the short message to the serving MSC or MME (mobility management entity) or SGSN (serving GPRS service node). This procedure is also used between the SMS-GMSC and the SMS Router or the IP-SM-GW, and between the HSS and the SMS Router or the IP-SM-GW in order to enforce routing of the SM delivery via the HPMN (home public mobile network) of the receiving MS.

Note: Due to Diameter vulnerability, some SPs could anonymise the IMSI (international mobile subscriber identity), but MCC/MNC information will be still provided in order to solve MNP issue.

4.3.5.3 SIP

SIP INVITE could also be used to query the ENUM Proxy. In this case the ENUM proxy is used like SIP Redirect Server and will use SIP 302 Redirect defined in RFC 3261 to answer to queries. A 3xx response may contain one or more Contact header field values providing new addresses where the caller might be reachable (In our context, NP info will be contained in the SIP 302 Redirect Contact Header).

4.3.6 Non ENUM2 Interface

Non ENUM 2 (NENUM2) interface will be used to query Non ENUM database to retrieve information related to the user profile of the destination.

NENUM2				**ENUM1/3**
Database	Protocol	**Msg**	**Parameter**	**Parameter**
HSS	**DIAMETER**	**UDR**		

Table 2 NENUM2 Interface Table

4.3.6.1 DIAMETER

Various DIAMETER (defined in RFC 3588) messages could be used to retrieve B user profile information.

3GPP TS 29.329 – Sh Interface

The IMS specification defines the Sh interface as the method of communication between the Application Server (AS) function and the HSS, or between multiple IMS Application Servers. The AS uses the Sh interface in two basic ways:

- To query or update a user's data stored on the HSS
- To subscribe to and receive notifications when a user's data changes on the HSS

User-Data-Request/Answer (AS-->HHS)

This AS asks for the subscriber related information from HSS. Subscriber related data at HSS is either provisioned by the SP and/or received from the network and/or it has been earlier stored by the AS itself with the help of the Profile-Update-Request/Answer.

5 Implementation aspects

5.1 ENUM Framework

The next sections will detail some call flows for different use cases which could be optionally deployed based on the ENUM framework.

Note: That the npdi option will not be presented into those call flows for simplification purposes.

5.1.1 SP A retrieves SP id and B user profile (Bilateral Mode)

In bilateral mode, it is basically possible to use the ENUM framework.

SP A will retrieve routing information by implementing an ENUM proxy that is able to connect to ENUM or non ENUM components to solve NP and to select the appropriate NNI according to the destination user profile (IMS or not).

In this example, an IMS NNI is selected, and the domain name is adapted with

“ims” prefix to specify that it is an IMS destination
“mnc<MNC>.mcc<MCC>.3gppnetwork.org” of the destination SP

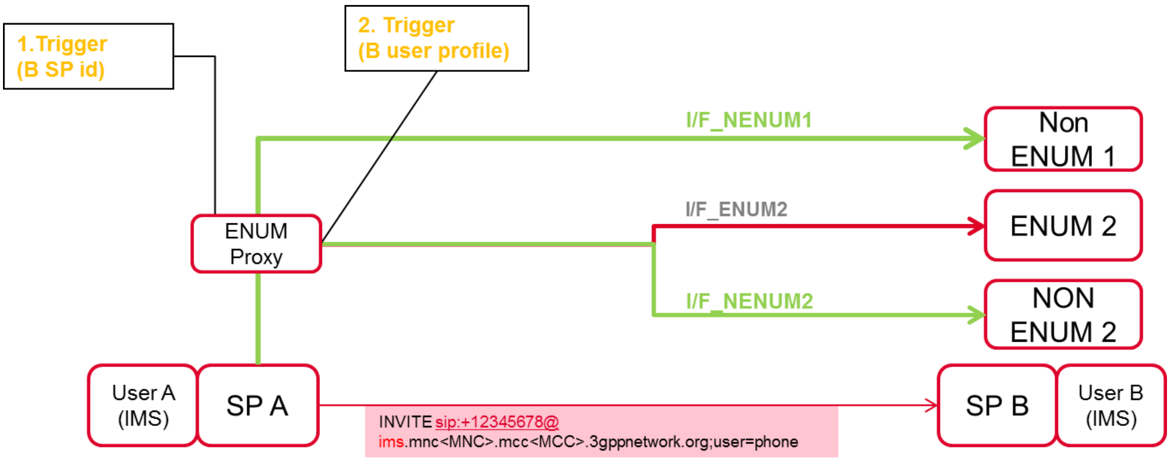


Figure 13 Use Case - bilateral

5.1.2 IPX (s) Routing based on Number Range B Service Provider manages Number Portability

This use case is based on the fact that no NP resolution will be done by the IPX providers. All IMS messages will be routed at SIP level between the SPs based on number ranges (no need to implement ENUM proxy, or ENUM proxy could be configured in order to analyse numbering ranges).

This architecture may be valid for the following scenario:

NP managed only at the national side between all the potential destinations in country B could be applied in cases where local regulation requires such method.

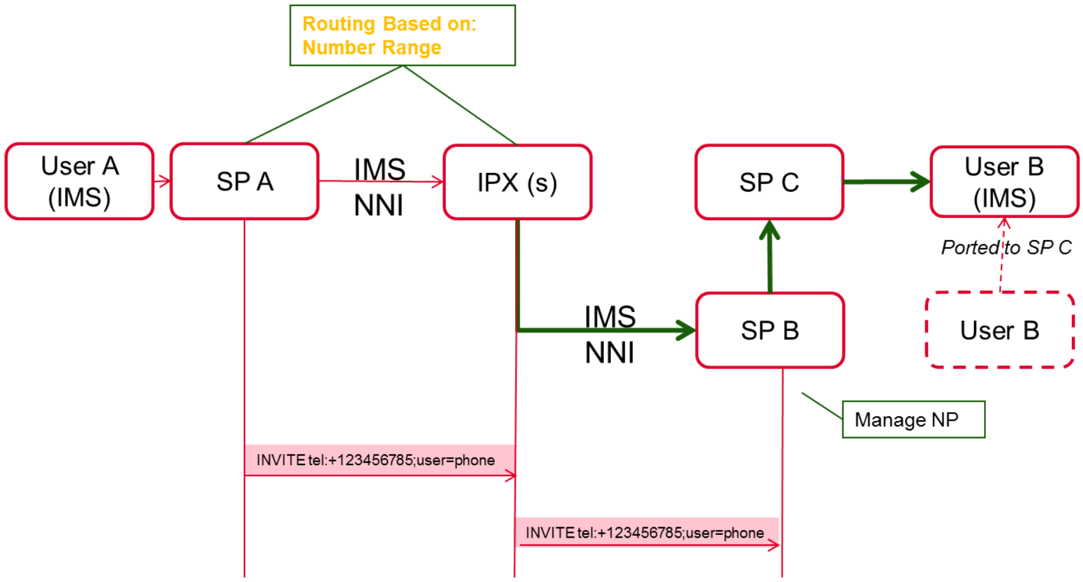


Figure 14 Use Case – multilateral – no NP resolution in IPX – TEL URI

In this example, IPX can manually configure the mapping between number range (CC or CC+NDC) and IMS entry information to select the corresponding IMS NNI. For originating calls, SP A sends the call flow through the IPX provider to SP B which is Original Number Range Holder. SP B use internal ENUM/NP query and national interconnection for the following routing.

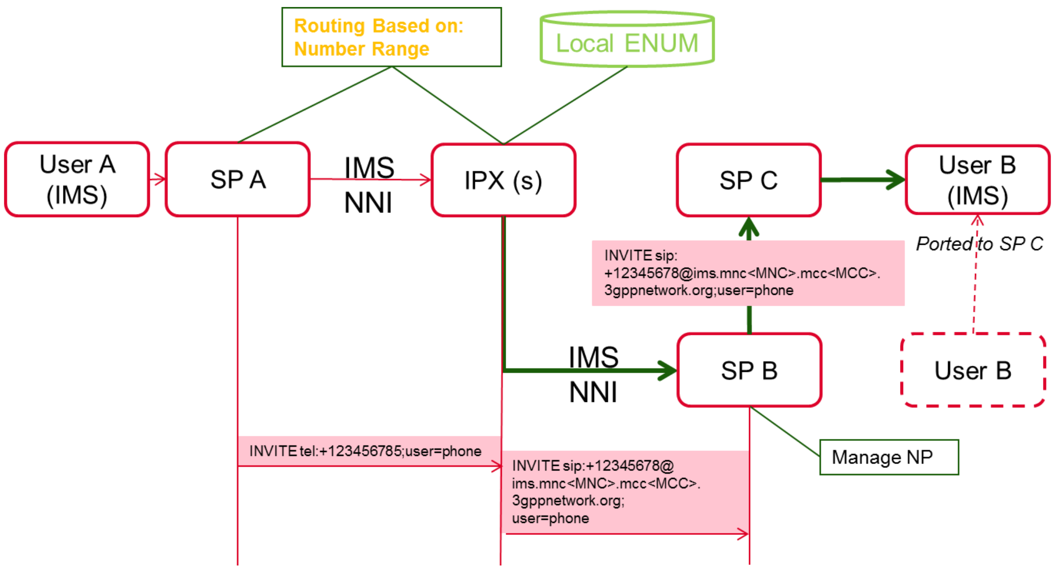


Figure 15 Use Case – multilateral – no NP resolution in IPX – SIP URI

Another method for IPX routing is to use local ENUM queries to generate an intermediate SIP URI. For originating calls, SP A sends the call flow to IPX providers. IPX can query a local ENUM and get an intermediate domain name by Number Range. By replacing TEL URI with intermediate SIP URI and user=phone tag, IPX will use intermediate SIP URI to query DNS and send call flow to SP B. Then SP B will deal with the following routing by using internal ENUM/NP query.

Note 1: This architecture is not optimised at SIP level, adding an intermediate B SP in the IMS session, and requesting national IMS NNI to be available for all SPs at destination side. Moreover, all traffic has to be routed to IMS NNI, in order to preserve IMS features (End-to-End).

Note 2: This architecture could be used to start the IMS NNI testing at SIP level, with no ENUM protocol, by using B user number from the Original Number Range.

5.1.3 IPX A determines SP id to select IPX B which will retrieve B User Profile

This use case is based on 2 IPX providers, just interconnected by SIP protocol.

The first IPX A will resolve the NP by querying the ENUM proxy, providing in this example the information in a non ENUM interface. IPX A will then route the SIP messages to the next IPX B provider, having a direct interconnection with the B SP by filling correctly the SIP/IMS URI domain with the “MCC / MNC” parameters.

In this example, IPX B will retrieve the B user profile (IMS), and route to the appropriate IMS NNI: the SIP/IMS URI domain will be prefixed with “ims”.

The SIP signalling will be progressively enriched to discover finally the IMS B.

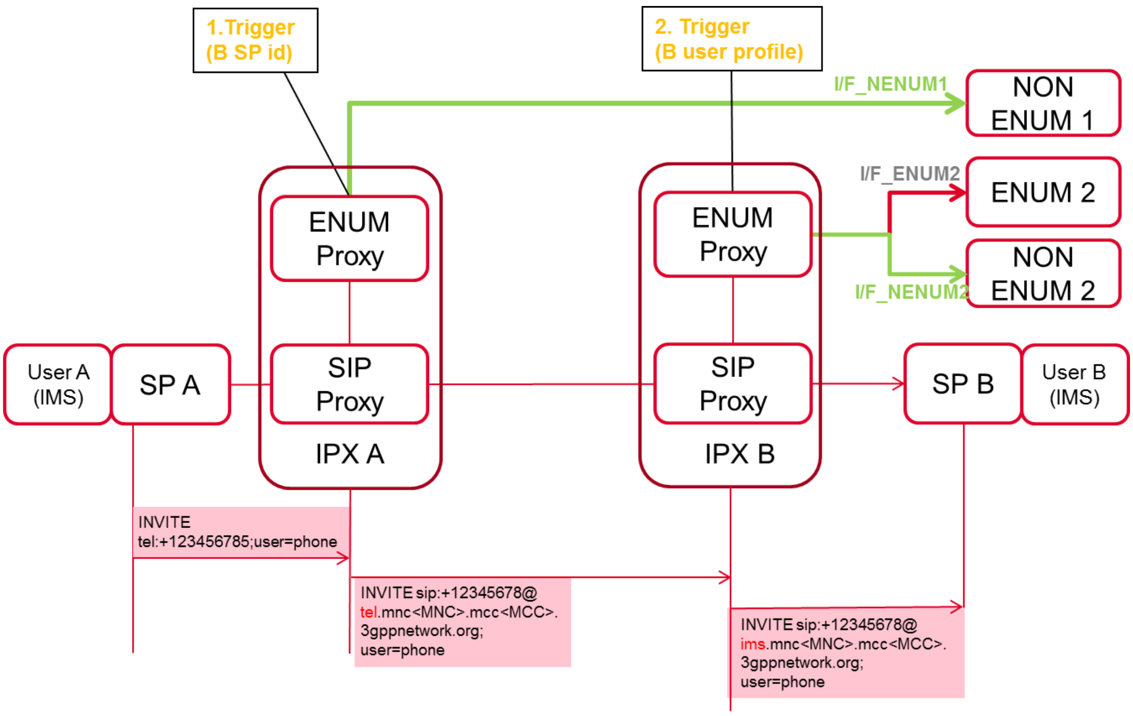


Figure 16 Use Case – multilateral with 2 IPX – no ENUM proxy interface

5.1.4 IPX A retrieves SP id and queries User Profile via ENUM3

This use case is based on 2 IPX providers, interconnected by SIP and ENUM protocol.

The first IPX A will resolve the NP by querying the ENUM proxy, providing in this example the information in a non ENUM interface. IPX A will then fill in the domain with the “MCC / MNC” parameters and delegate via ENUM3 interface the ENUM query to the next IPX B provider, having a direct interconnection with the B SP in order to retrieve the B user profile (using ENUM or non ENUM).

In this example, the B user profile that is IMS and ENUM Proxy (IPX B) will answer to ENUM proxy (IPX A) with URI domain prefixed with “ims”.

Finally, IPX A will route the SIP IMS messages to IPX B, in order to reach directly the final destination B.

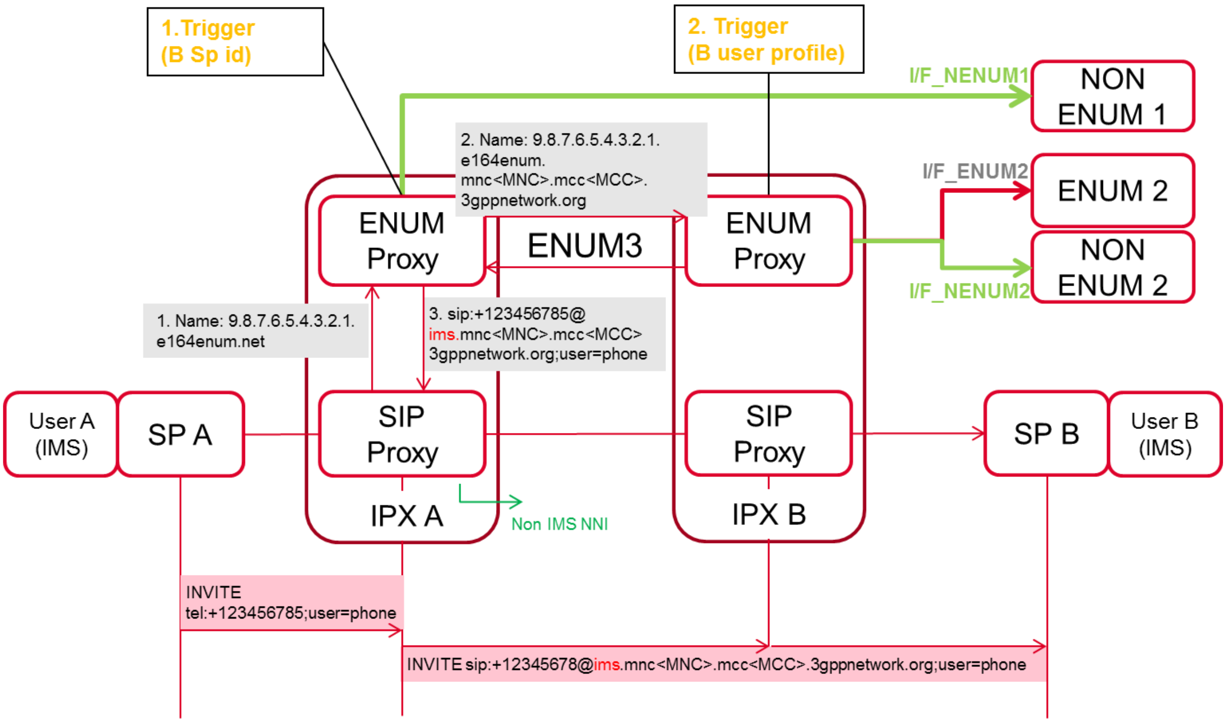


Figure 17 Use Case – multilateral with 2 IPX –ENUM delegation via ENUM3 for NP

5.1.5 IPX A retrieves SP id and User Profile via ENUM3

This use case is based on 2 IPX providers, interconnected by SIP and ENUM protocol.

The first IPX A will be not able to resolve the NP by querying the ENUM proxy. IPX A will then delegate via ENUM3 interface the ENUM query to another IPX B provider, having a direct interconnection with the B SP in order to resolve NP and retrieve the B user profile (using ENUM or non ENUM).

In this example, the B user profile that is IMS and ENUM Proxy (IPX B) will answer to the ENUM proxy (IPX A) with URI domain prefixed with “ims” including the MCC/MNC parameters adaptation.

Finally, IPX A will route the SIP IMS messages to IPX B, in order to reach directly the final destination B.

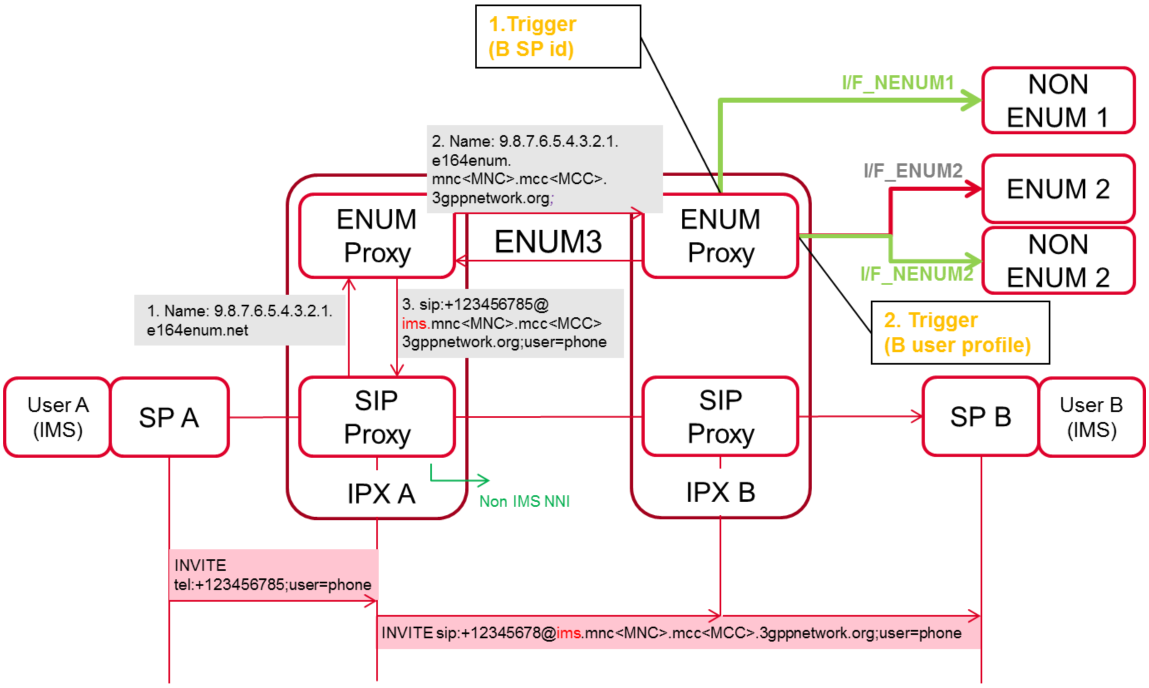


Figure 18 Use Case – multilateral with 2 IPX – ENUM delegation via ENUM3 for NP/user profile

5.1.6 SP A retrieves SP id to select the appropriate IPX provider

This use case is proposed to resolve the issue to select the appropriate IPX provider, when the SP A has several IPX providers.

In this example, the SP A will first query an ENUM proxy in order to resolve the NP. ENUM proxy will answer with the MCC/MNC parameters. The ENUM proxy could be implemented by an IPX provider or locally by the SP A.

Based on the destination SP information (MCC/MNC), SP A will then route the SIP messages to the appropriate IPX provider, having an interconnection with the B SP by filling correctly the SIP/IMS URI domain with the “MCC / MNC” parameters”. “tel” prefix is used at this stage because no B user information is available.

IPX provider will retrieve via the ENUM proxy, the B user profile (IMS), and route to the appropriate IMS NNI: the SIP/IMS URI domain will be prefixed with “ims”.

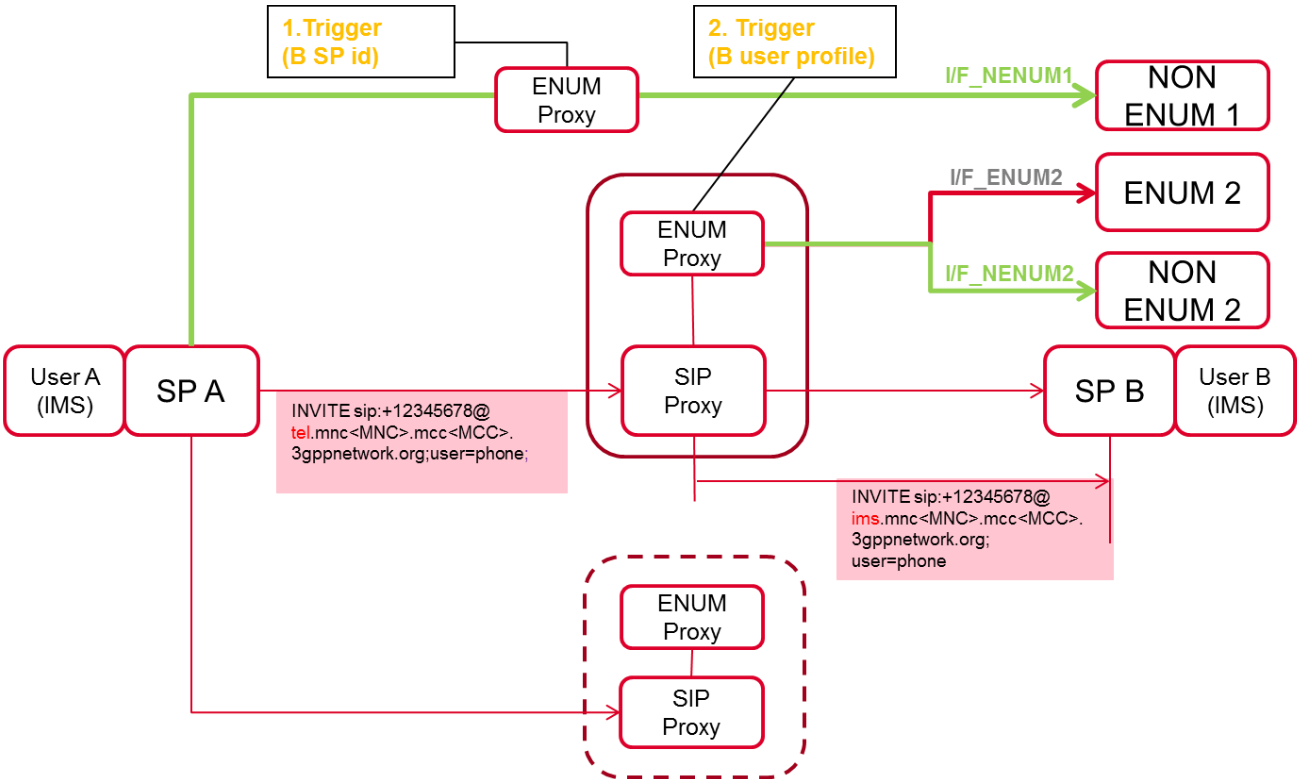


Figure 19 Use Case – multilateral – SP A selection for multi IPX providers

5.1.7 Operational networks

ENUM Framework could be introduced progressively in the operational networks on top of the existing SIP proxies:

- SIP proxies could be interconnected in order to perform IMS interconnection: non ported destination could be reached easily by routing SIP signalling to the Original Number Range Holder.
- ENUM proxy could be introduced progressively, providing additional routing capabilities related first to SP identity (to solve NP) and secondly to IMS user profile (when information is available). ENUM proxies could also be interconnected to enhance the database connection
- Databases connectivity could be added also progressively, using ENUM or non ENUM interfaces, depending on country availabilities.

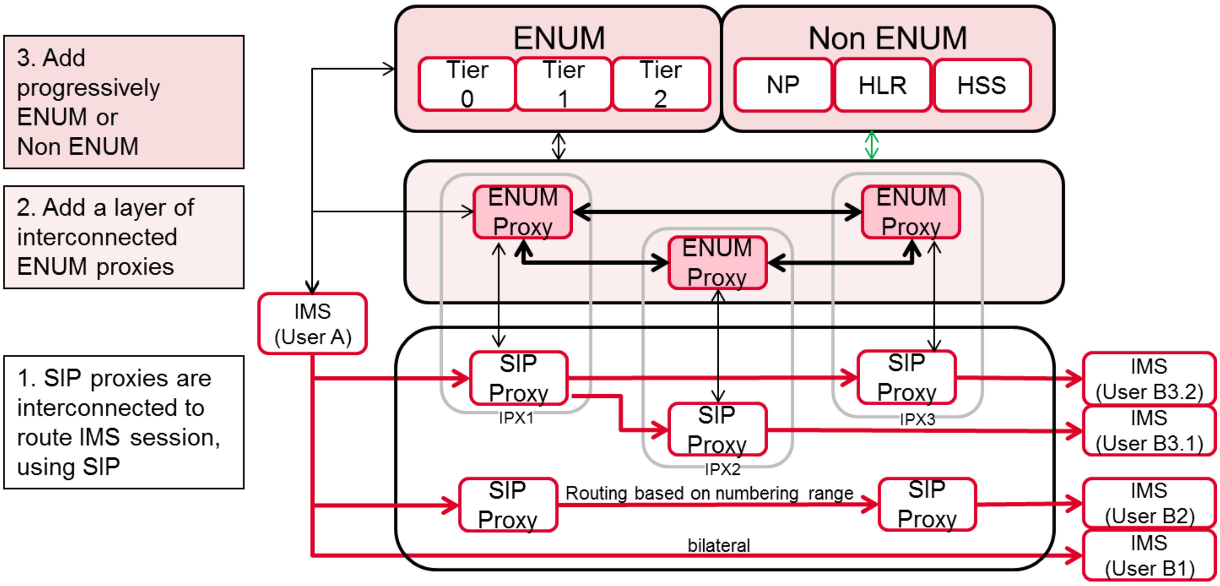


Figure 20 ENUM framework: deployment

In the ENUM framework, IMS A will be able to connect to various IMS B through several connection types:

a) IMS B1 in a bilateral mode, using ENUM hierarchical model or ENUM proxies to find the appropriate Bilateral destinationIMS B2 in a multilateral mode, using only number range routingIMS B3 in a multilateral mode, using ENUM proxy to resolve NP and discover the user profile

6 For Further Study

The following items are for further study:

- DNS process to get information in ENUM servers (missing in GSMA IR.67)
- GSMA IR.21 DB defined in [49] to be fill in with the list of PMN ENUM, (public mobile network ENUM) server IP addresses and names
- Editorial: references could be sort by categories (IETF, GSMA, ITU, 3GPP, …)

Annex A Input documents to build this new PRD

		IN.16	IN.12	IN.16 CR1002	IR.67	ENUM Framework
1	Introduction					
1.1.	Overview					
1.2.	Definitions		3.2			
1.3.	Abbreviation		3.2			
1.4.	References				1.5	1.4
2	Requirements		5	3.1		
3	ENUM technology		6		5.1 & 5.2	
4	Architecture					
4.1	Hierarchical model	4.3.1	7.1		5.3	
4.2	ENUM interface definition				5.4	
4.3	ENUM proxy					2
5	Implementation aspects					3
A	Annexes					
A.1	MNP in ENUM hierarchical model				C	

Table 3 Input Documents Table

Annex B GSMA PathFinder

GSMA has launched a GSMA Carrier ENUM solution through PathFinder. PathFinder implements the common root directory, Tier-0, which allows global navigation of the distributed databases. Tier-0 records, allow the authority to be identified for each number block and may identify a national T1 operated by a national authority hosted by PathFinder or an individual operator. This provides the flexibility to handle multiple different regulatory models. PathFinder also includes Tier-1 and Tier-2 functionality, and it will be the operators wish to use one or another. GSMA Carrier ENUM is a practical solution to the MNP issues raised in this white paper today.

To provide routing solutions in the absence of ENUM data widely populated by operators, Pathfinder proposes Pathfinder NPD (Number Portability Discovery Service). With PathFinder NPD has acquired feeds to traditional NP information sources which can also be used to obtain the identity of the Recipient network, and as a last resort, it has also the possibility to query the HLR to obtain the identity of the Recipient Network (see Figure 7).

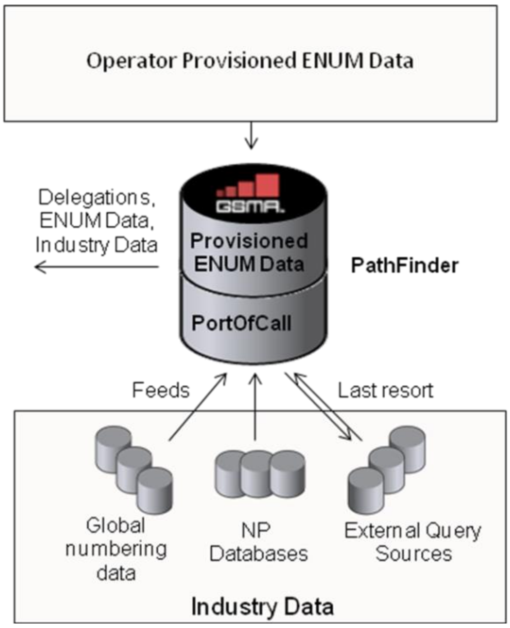


Figure 21 GSMA PathFinder

In this way the party requesting information can see who the record of the operator is for any particular number. If that operator has populated data, the party requesting information is given the gateway addresses for the desired services. This feature enables a smooth migration path towards GSMA Carrier ENUM.

Annex C Solving Number Portability in ENUM

C.1 Introduction

This section describes and analyses different approaches for provisioning ENUM in countries where NP exists. The approach provided will depend on the NP solution used in the local country for the hosted number ranges.

The different approaches can be categorized based on at which Tier the knowledge about ported users is available which could be at a centralized Tier-1 ENUM DNS server or decentralized at the Tier-2 ENUM DNS servers

C.2 Options based on Number Portability knowledge at a central ENUM server

C.2.1 Option 1 – Central authoritative database

C.2.1.1 Description

This option consists on combining the Tier-1 and Tier-2 ENUM tiers and having the country level ENUM DNS server authoritative for all subscribers. This means that all URIs and/or URLs for subscribers are centrally located and managed.

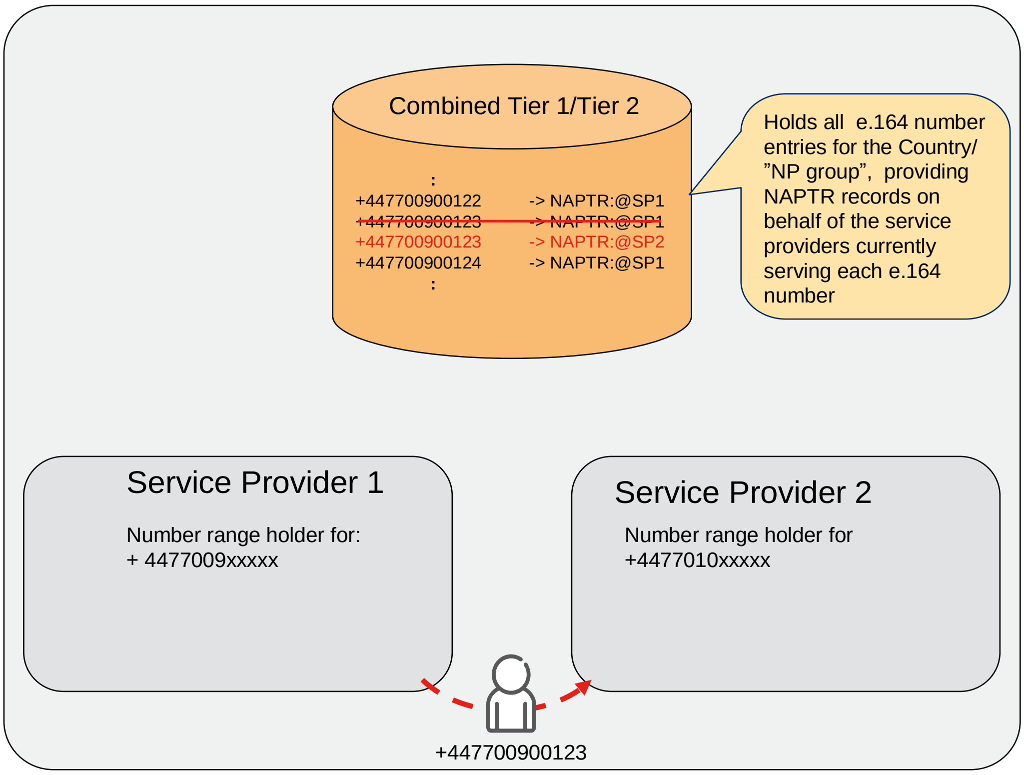


Figure 22 Central Authoritative database

C.2.1.2 Example Configuration

If the subscriber whose E.164 number is +44-7700-900123 is a subscriber of SP 1 in the UK, his SIP URI (for IMS) could be "SIP:+447700900123@ims.mnc001.mcc234.3gppnetwork.org;user=phone" and would be provisioned in his ENUM record in the central database as follows:

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
       3.2.1.0.0.9 NAPTR 10 10 "u" "E2U+SIP"
       "!^.*$!sip:+447700900123@ims.mnc001.mcc234.3gppnetwork.org;user=phone!" .
```

If this subscriber is moved/ported to SP 2 in the UK, then this SIP URI in the central database would simply be modified to be "SIP:+447700900123@ims.mnc002.mcc234.3gppnetwork.org;user=phone" thus:

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
       3.2.1.0.0.9 NAPTR 10 10 "u" "E2U+SIP"
       "!^.*$!sip:+447700900123@ims.mnc002.mcc234.3gppnetwork.org;user=phone!" .
```

C.2.1.3 Advantages and Disadvantages

The obvious disadvantage of this option is that the data-fill for such a combined Tier-1/2 could be very large. The widely used, freely available ISC BIND DNS server application won't probably be able to cope with such data-fill for this solution. However, there are high capacity ENUM/DNS solutions commercially available.

This option, however, does have the advantage that all subscriber numbers are stored centrally and so can be centrally controlled and administered, possibly by one O&M (operation and maintenance) facility. It also has the advantage in that it reduces the number of DNS requests that an ENUM/DNS resolver has to perform by one DNS Request therefore the extra time taken to search through a larger set of zone files to return the NAPTR records may in some circumstances actually be quicker than the DNS resolver having to perform a further DNS look-up to a separate Tier-2.

C.2.1.4 Suitability

This option is possibly more suited to countries having a central ENUM Tier-1 server and where their MNPs are already solved using a central (M)NP database.

C.2.2 Option 2 – Central redirection database

C.2.2.1 Description

This option consists of combining the Tier-1 and Tier-2 ENUM tiers but instead of having the country level ENUM DNS server store the URIs and/or URLs for subscribers, each subscriber record contains a special redirection indicator for all incoming look-ups. The indicator provides a pointer to the subscribed network. This "capture all" redirection can be realised using a single NS record. This NS record redirects the ENUM/DNS Resolver to the newly subscribed network's ENUM/DNS server by returning a new DNS server to query. This means that all URIs and/or URLs for subscribers are located and managed by the actual subscribed network of each number, and not by the number range owning network of each number.

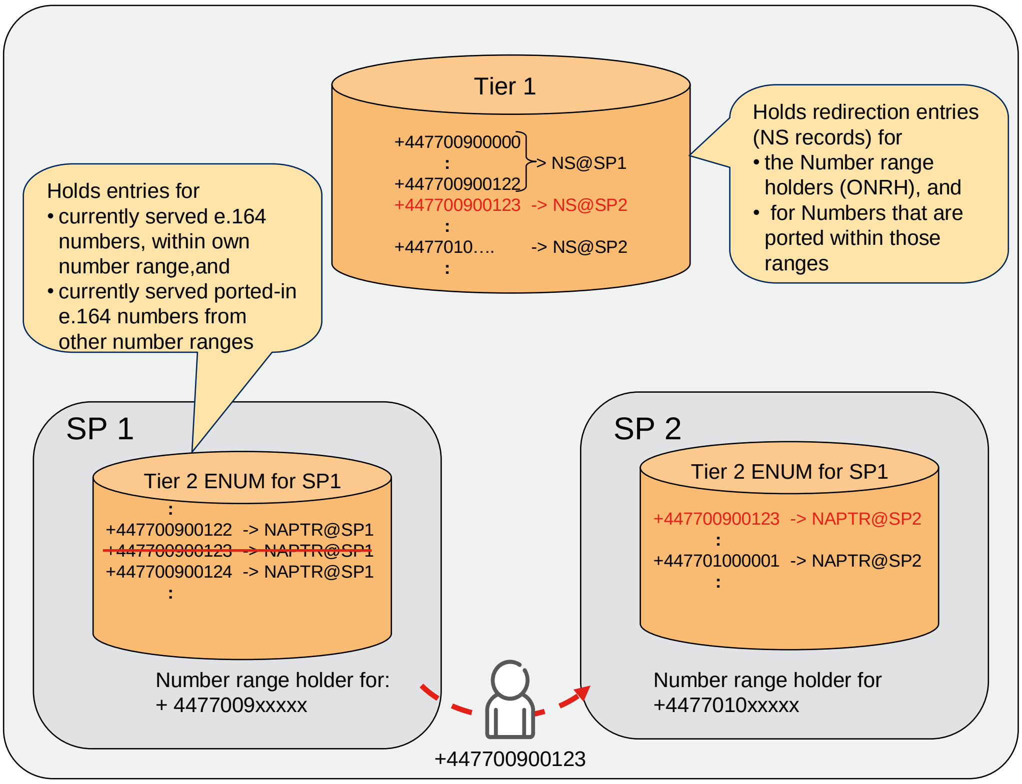


Figure 23 Central redirection database

C.2.2.2 Example

If the subscriber whose E.164 number is +44-7700-900123, and is also a subscriber of SP 1 in the UK, his record in the Central Database would be as follows:

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
       3.2.1.0.0.9 IN NS dns1.mnc001.mcc234.3gppnetwork.org
```

And would be reflected in SP 1's DNS server (called "dns1.mnc001.mcc234.3gppnetwork.org") as follows:

```
$ORIGIN 3.2.1.0.0.9.0.0.7.7.4.4.e164enum.net.
       NAPTR 10 10 "u" "E2U+SIP"
       "!^.*$!sip:+447700900123@ims.mnc001.mcc234.3gppnetwork.org;user=phone!" .
```

If this subscriber then moves over to SP 2 in the UK, then the ENUM record stored in the Central Database would be modified to the following:

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
       3.2.1.0.0.9 IN NS dns1.mnc002.mcc234.3gppnetwork.org
```

And hence, SP 2's DNS server (called "dns1.mnc002.mcc234.3gppnetwork.org") would be:

```
$ORIGIN 3.2.1.0.0.9.0.0.7.7.4.4.e164enum.net.
       NAPTR 10 10 "u" "E2U+SIP"
       "!^.*$!sip:+447700900123@ims.mnc002.mcc234.3gppnetwork.org;user=phone!" .
```

C.2.2.3 Advantages and Disadvantages

The main advantage of this option is that it puts the subscribed operator in full control of the URIs/URLs returned for a particular Tel URI. An explicit advantage over option 3 is that the newly subscribed network is *not* reliant upon the number range owning network to make any updates in their ENUM DNS server, instead just the Tier-1 is.

An explicit disadvantage over option 1 is that the DNS Resolver may have to perform one additional ENUM DNS look-up to the Tier-2 ENUM DNS server.

The obvious disadvantage of this option is that the data-fill for the Tier-1 could be very large! The widely used, freely available ISC BIND DNS server application would more than likely not be able to cope with such a data-fill for this solution. However, there are high capacity ENUM/DNS solutions commercially available.

C.2.2.4 Suitability

This option is possibly more suited to countries having a central ENUM Tier-1 server and where their MNP is already solved using a central MNP database.

C.3 Options based on Number Portability knowledge at Service Provider Tier-2 ENUM server

These options have in common that the Tier-1 ENUM/DNS server redirects to the Tier-2 ENUM/DNS of the SP originally owning the number range.

A common disadvantage for these options compared to the centralized server options is that, to work properly, all SP within an NP Group should have a Tier-2 ENUM DNS server.

Potential methods and measures to deal with the problem of not all SPs having an ENUM/DNS server are discussed in section C3.5.

An advantage with this option over the centralized server approaches is that it is does not require centralized server per country. In countries where there are problems to establish such a Tier-1 server, the decentralized options 3 to 6 described below can still be applied when the Tier-1 functionality to redirect to the number range owner’s ENUM DNS server can be hosted on the Tier-0 server.

C.3.1 3 – Change of domain name in URIs/URLs in Tier-2

C.3.1.1 Description

This option is similar to the previous one and consists of simply changing the domain name in all URIs and/or URLs under individual E.164 number entries to the identity of the newly subscribed network. However, the Tier-1 and Tier-2 are not combined but kept separated.

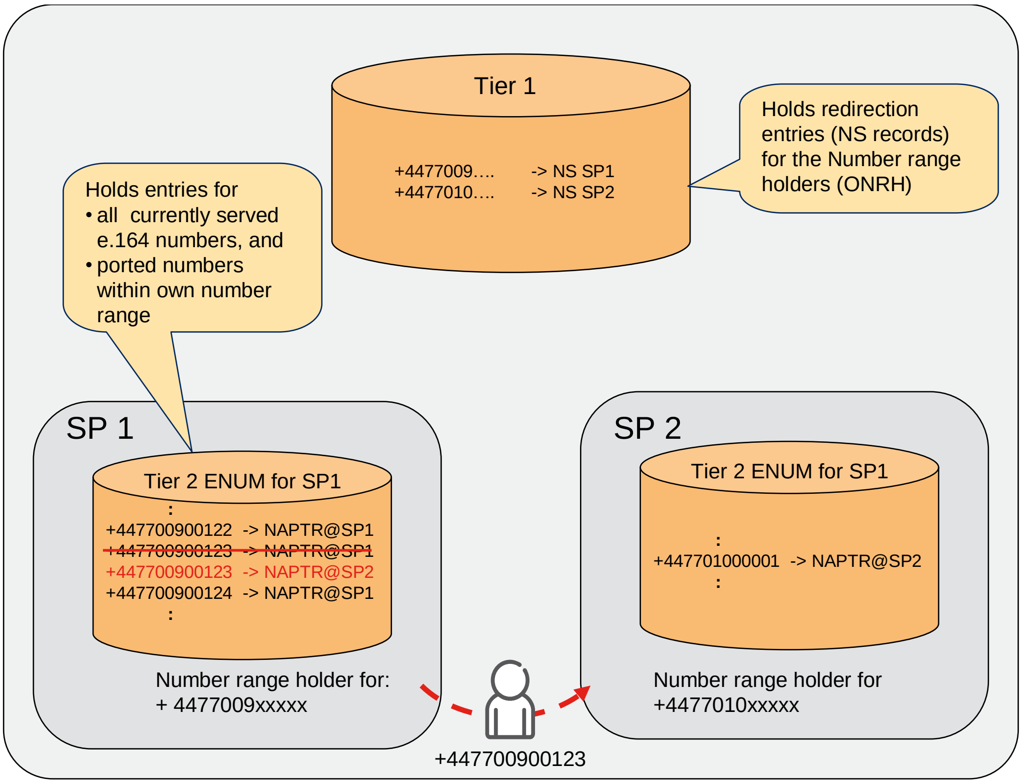


Figure 24 Change of Domain Names of URI/URLs in Tier-2

C.3.1.2 Example

If the subscriber whose E.164 number is +44-7700-900123 is a subscriber of SP 1 in the UK, his SIP URI (for IMS) could be "SIP:+447700900123@ims.mnc001.mcc234.3gppnetwork.org" and would be provisioned in his ENUM record in SP 1's Tier-2 DNS server as follows:

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
      3.2.1.0.0.9 NAPTR 10 10 "u" "E2U+SIP"
      "!^.*$!sip:+447700900123@ims.mnc001.mcc234.3gppnetwork.org!" .
```

If this subscriber then moved/ported over to SP 2 in the UK, then this SIP URI would be modified in SP 1's Tier-2 DNS server to be "SIP:+447700900123@ims.mnc002.mcc234.3gppnetwork.org" thus:

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
      3.2.1.0.0.9 NAPTR 10 10 "u" "E2U+SIP"
      "!^.*$!sip:+447700900123@ims.mnc002.mcc234.3gppnetwork.org!" .
```

C.3.1.3 Advantages and Disadvantages

A disadvantage of this option is that the newly subscribed network is reliant upon the number range owning network to not only make the changes at the time of porting, but to also support later additions and modifications to URIs and/or URLs; possibly related to services that may not be offered by the number range owning network. For example, if SP 2 rolled-out an IP based service (that uses ENUM) before SP 1, then SP 1 will have to provision in their Tier-2 DNS all the ENUM records for those subscribers who have ported to

SP 2 with the new URI(s) and/or URL(s). SP 1 may also not be able to do this in a time period that is satisfactory to SP 2's launch of the new service.

C.3.1.4 Suitability

This option is suited to countries where their MNP is not solved using a central MNP database. It may also be suitable for countries having no central Tier-1 ENUM server, but where the Tier-1 functionality is hosted by the Tier-0.

C.3.2 Option 4 – Redirection at Tier-2

C.3.2.1 Description

This option consists of having a "normal" Tier-1 and Tier-2 however, the number range owning network's Tier-2 DNS server storing for each ported-out subscriber, a special redirection indicator for all incoming look-ups (effectively creating an extra "Tier-3" for all ported out subscribers). The indicator provides a pointer to the subscribed network. This "capture all" redirection is realised using a single NS record. This NS record redirects the ENUM/DNS Resolver to the newly subscribed network's ENUM/DNS server by returning a new DNS server to query.

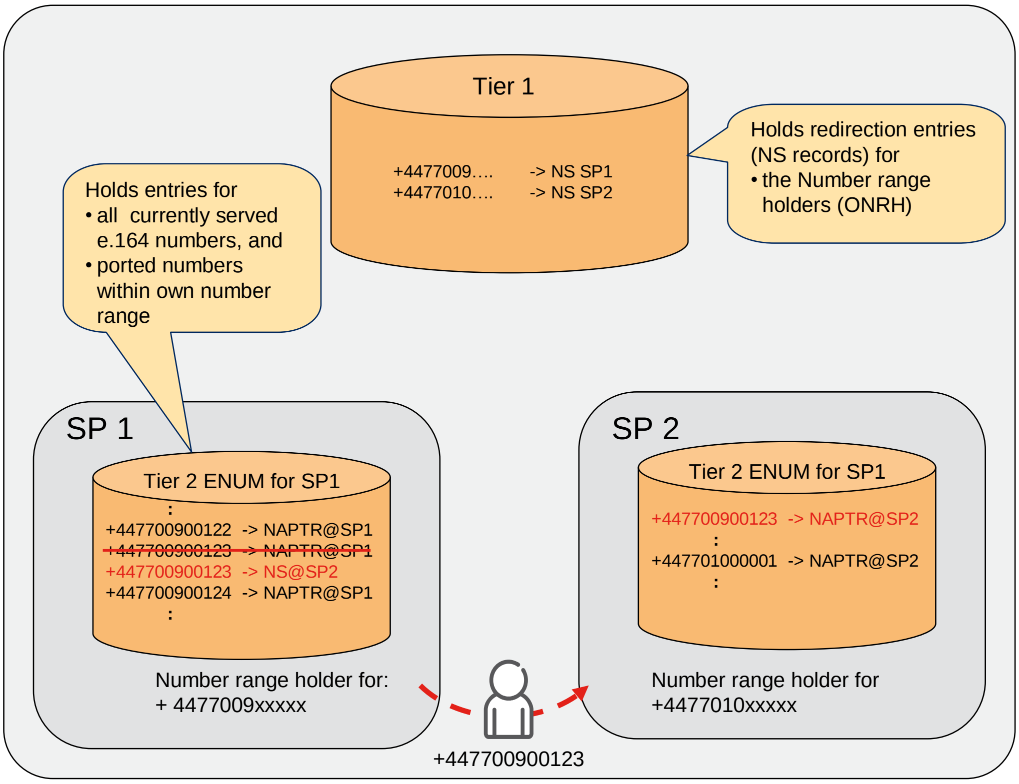


Figure 25 Redirection at Tier-2

C.3.2.2 Example

If the subscriber whose E.164 number is +44-7700-900123 is a subscriber of SP 1 in the UK, their SIP URI (for IMS) could be "SIP:+447700900123@ims.mnc001.mcc234.3gppnetwork.org" and would be reflected in their ENUM record as standard, thus:

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
       3.2.1.0.0.9 NAPTR 10 10 "u" "E2U+SIP"
       "!^.*$!sip:+447700900123@ims.mnc001.mcc234.3gppnetwork.org;user=phone!" .
```

If this subscriber then moves over to SP 2 in the UK, then the ENUM record stored in SP 1's Tier-2 DNS server would be something like the following:

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
       3.2.1.0.0.9 IN NS dns1.mnc002.mcc234.3gppnetwork.org
```

In SP 2's DNS server, called "dns1.mnc002.mcc234.3gppnetwork.org", would be needed something like the following:

```
$ORIGIN 3.2.1.0.0.9.0.0.7.7.4.4.e164enum.net.
       NAPTR 10 10 "u" "E2U+SIP"
       "!^.*$!sip:+447700900123@ims.mnc002.mcc234.3gppnetwork.org;user=phone!" .
```

The DNS resolver will more than likely "know" the IP address for the DNS server "dns1.mnc002.mcc234.3gppnetwork.org" due to previous look-ups. At the very least, it will know the authoritative server for the domain "3gppnetwork.org" from the current set of look-ups. This can be controlled further by increasing the DNS Server's FQDN's TTL (time to live), which is achievable as generally operators do not change the IP addresses of their DNS servers frequently. Therefore, this solution will involve one extra DNS look-up, possibly two extra DNS look-ups.

C.3.2.3 Advantages and Disadvantages

The main advantage of this option is that it puts the subscribed operator in full control of the URIs/URLs returned for a particular Tel URI, in the same manner as for option 2.

A disadvantage of this option is that the newly subscribed network is still reliant upon the number range owning network to make updates in their ENUM Tier-2 DNS server. However, unlike Option 3, the update is only minor, and has to be done once (or at least, only when the subscriber changes/ports networks) and encompasses *all* services related to ENUM; whether they are supported by the number range owning network or not.

An explicit disadvantage over option 3 is that the DNS Resolver may have to perform one additional ENUM DNS look-up to resolve ported numbers.

C.3.2.4 Suitability

As with Option 3, this option is more suited to countries where their MNPs are not solved using a central MNP database, and it is also suitable to countries where the Tier-1 functionality is hosted by the Tier-0.

C.3.3 Option 5 – Redirection at Tier-2 based on interaction with Legacy NP systems

C.3.3.1 Description

This option consists of having a "normal" Tier-1 and Tier-2. However, for numbers where the Tier-2 servers do not have a corresponding ENUM record, the Tier-2 Interacts with a legacy

NP system and based on legacy NP information, it determines the currently serving SP, and creates a NS response to redirect to that SP. The legacy NP information used to identify the serving SP can for example be the IMSI, when available, or SS7 routing information used by ISUP (ISDN user part).

That information can be used to point to the appropriate NS record to use.

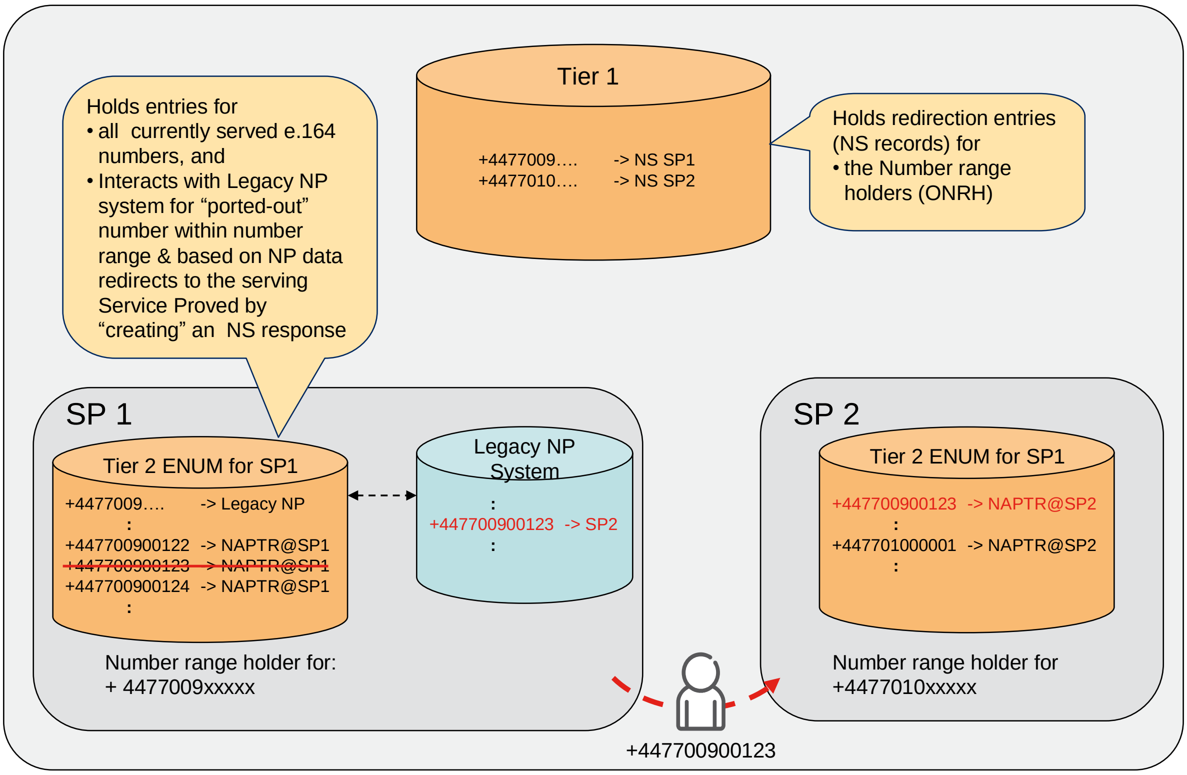


Figure 26 Redirection at Tier-2 based on Legacy NP system interaction

C.3.3.2 Example

If the subscriber whose E.164 number is +44-7700-900123 is a subscriber of SP 1 in the UK, his SIP URI (for IMS) could be "SIP:+447700900123@ims.mnc001.mcc234.3gppnetwork.org" and would be provisioned in his ENUM record in SP 1's Tier-2 DNS server as follows:

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
       3.2.1.0.0.9 NAPTR 10 10 "u" "E2U+SIP"
       "!^.*$!sip:+447700900123@ims.mnc001.mcc234.3gppnetwork.org;user=phone!" .
```

If this subscriber then moves over to SP 2 in the UK, then the ENUM record stored in SP 1's Tier-2 DNS server would be removed, and when a query for this number is received, then SP 1's Tier-2 DNS server would interact with the Legacy NP system using for example an INAP (intelligent network application protocol) or MAP query.

The response from the legacy NP system, informs that the number is now supported by SP 2, and something like the following would be created.

```
$ ORIGIN 0.0.7.7.4.4.e164enum.net.
       3.2.1.0.0.9 IN NS dns1.mnc002.mcc234.3gppnetwork.org
```

In SP 2's DNS server, called "dns1.mnc002.mcc234.3gppnetwork.org", would be needed something like the following:

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
       3.2.1.0.0.9 NAPTR 10 10 "u" "E2U+SIP"
       "!^.*$!sip:+447700900123@ims.mnc002.mcc234.3gppnetwork.org!" .
```

In SP 2's DNS server, called "dns1.mnc002.mcc234.3gppnetwork.org", would be needed something like the following:

```
$ORIGIN 3.2.1.0.0.9.0.0.7.7.4.4.e164enum.net.
       NAPTR 10 10 "u" "E2U+SIP"
       "!^.*$!sip:+447700900123@ims.mnc002.mcc234.3gppnetwork.org;user=phone!" .
```

C.3.3.3 Advantages and Disadvantages

A disadvantage with this option is the need for interaction with the legacy NP system. At a minimum this interaction can be compared with performing an additional query in recursive mode.

Compared to alternative 4, this option does not require any updates to the number range owner’s ENUM/DNS server when a number is ported. In fact, the E.164 entry for the ported number needs to be removed from the Number range owning SP’s Tier-2 server. The information on how to translate the legacy NP information to an NS record pointing to the other SP’s ENUM DNS server needs to be configured. However, this needs only to be introduced once, and not for every ported number.

The main advantage of this option is that it puts the subscribed operator in full control of the URIs/URLs returned for a particular Tel URI, in the same manner as for option 4. An explicit advantage over option 4 is that the newly subscribed network is *not* reliant upon the number range owning network to make any updates in their ENUM DNS server, as the newly subscribed network is identified from the Legacy NP system.

C.3.3.4 Suitability

This option is possibly more suited in for countries with no Tier-1 server and the Tier-1 functionality is hosted by the Tier-1, and where all SPs have access to full NP information,

C.3.4 Option 6 – Non-Authoritative response based on Legacy NP system interaction

C.3.4.1 Description

This option consists on having a "normal" Tier-1 and Tier-2. However, for Numbers where the Tier-2 servers do not have a corresponding ENUM record, the Tier-2 may utilize legacy NP information. Based on that information a non-authoritative final response, where for example the legacy NP routing information (for example IMSI or routing number, and so on) can be used to create the domain name to be used in for example a SIP URI, could be created.

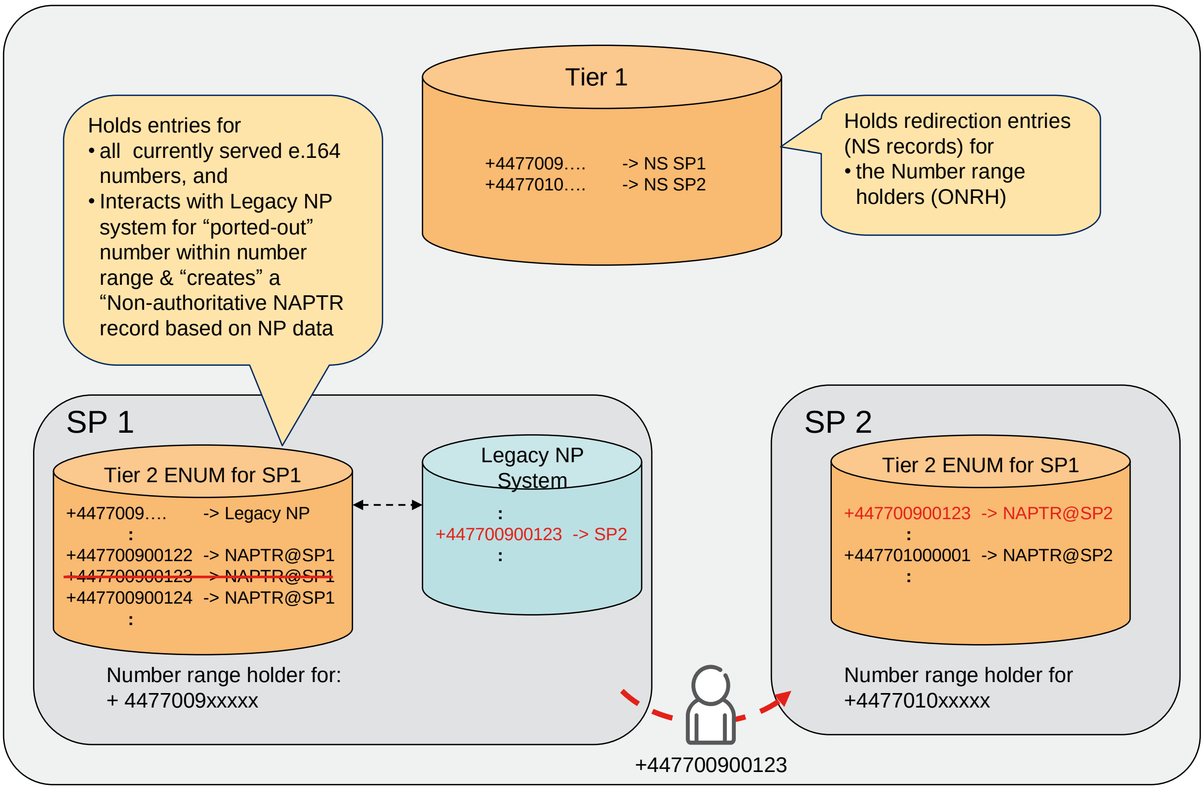


Figure 27 Non-authoritative NAPTR response based on Legacy NP system Interactions

C.3.4.2 Example

If the subscriber whose E.164 number is +44-7700-900123 is a subscriber of SP 1 in the UK, his SIP URI (for IMS) could be "SIP:+447700900123@ims.mnc001.mcc234.3gppnetwork.org" and would be reflected in his ENUM record as standard, thus:

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
      3.2.1.0.0.9 NAPTR 10 10 "u" "E2U+SIP"
      "!^.*$!sip:+447700900123@ims.mnc001.mcc234.3gppnetwork.org;user=phone
!" .
```

If this subscriber then moved over to SP 2 in the UK, then the ENUM record stored in SP 1's Tier-2 DNS server would be removed, and when a query for this number is received SP 1's Tier-2 DNS server would interact with the Legacy NP system using for example an INAP or MAP query.

The response from the legacy NP system, informs that the number is now supported by SP 2, and something like the following would be created.

```
$ORIGIN 0.0.7.7.4.4.e164enum.net.
      3.2.1.0.0.9 NAPTR 10 10 "u" "E2U+SIP"
      "!^.*$!sip:+447700900123@ims.mnc002.mcc234.3gppnetwork.org;user=phone
!" .
```

The NAPTR RR record returned in this case may be considered as Non-authoritative. If it is even provided based on consent by SP 2, it would be created based on legacy NP information. In difference to Option 3, SP 2 does not have the possibility to individualize the NAPTR records per E.164 number.

C.3.4.3 Advantages and Disadvantages

A disadvantage with this option is the need for interaction with the legacy NP system. At a minimum this interaction can be compared with performing an additional query in recursive mode.

Another important disadvantage is that the currently serving SP cannot decide for which of its Ported-in numbers it wants a NAPTR Record returned. If the serving SP only wants to populate its ENUM DNS server for numbers having an IMS service, this information may not be available in the Legacy NP system and with the achieved results, the NAPTR records it will be returned also for numbers that for example only are served on CS (circuit switch).

C.3.4.4 Suitability

This option is possibly more suited in for countries where no Tier-1 server and the Tier-1 functionality is hosted by the Tier-1, and where all SPs have access to full NP information,

C.3.5 Considerations when not all Service Provider have a Tier-2 ENUM DNS server

As mentioned, there may be problems with a decentralized NP solution if not all SPs have a Tier-2 ENUM DNS server.

In case one SP does not have an ENUM/DNS server, there is no Tier-2 ENUM/DNS server that would hold NAPTR or NS records for the numbers that have been ported out to other SPs.

To allow a SP who wants to be able to provide ENUM entries for all served E.164 numbers, including ported-in numbers when a decentralized solution is used, there are a number of methods that may help overcome the problem when not all SPs have a Tier-2, proposed below.

C.3.5.1 Hosting of Ported-in numbers at the Tier-1

Although the Options 3, 4, 5 and 6 are decentralized in nature, and the Tier-1 only should make redirects to the Number Range Holders, SPs make arrangements with the Tier-1 (or Tier-0 if it hosts the Tier-1 functionality) ENUM/DNS server to host entries for numbers ported from a SP not having a Tier-2 ENUM/DNS server.

This alternative can be used for all decentralized options.

C.3.5.2 Tier-1 redirects to alternative Service Provider Tier-2 server

For Options 5 and 6 which rely on information from Legacy NP systems, to determine the currently serving SP, one or more of the Tier-2 SPs could agree to access the legacy NP system not only for his own Number ranges but also for Number ranges held by a SP that does not have an ENUM DNS server.

The Tier-1 (or Tier-0 for countries where the Tier-1 is hosted by the Tier-0 server) could then refer to the Alternative SP’s ENUM/DNS server when the number range owner does not have a Tier-2.

If several or all Tier-2 SP agree to do the same to share the cost and load, the Tier-1 server, can provide multiple NS records with the same priority, one for each of the “participating” Tier-2 SP’s ENUM/DNS servers.

DNS resolvers could then randomize which “participating” Tier-2 SP’s DNS server they would access to resolve the number.

Annex D Document Management

D.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	20/03/2017	Official release of first version	PMSC	Marc Balon / Orange

D.2 Other Information

Type	Description
Document Owner	Networks / Packet
Editor / Company	Marc Balon / Orange

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.