



**GSMA PRD IR.67 – "DNS/ENUM Guidelines for Service
Providers & GRX/IPX Providers"**

3.3

21 July 2009

This is a non-binding permanent reference document of the GSM Association.

Security Classification: Unrestricted

This document is subject to copyright protection. The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice. Access to and distribution of this document by the Association is made pursuant to the Regulations of the Association.

Copyright Notice

Copyright © 2009 GSM Association

GSM™ and the GSM Logo™ are registered and the property of the GSM Association.

Document History

Version	Date	Brief Description
0.1.0	14 October 2004	First draft – skeleton.
0.2.0	10 May 2005	Second draft, with most sections filled in, or at least with place holders.
0.2.1	11 May 2005	Changed the underlying Word template to the new one.
0.3.0	15 November 2005	Enhancements of ENUM section, including addition of Number Portability in ENUM, plus minor corrections and update of template.
0.9.0	16 December 2005	Final draft for publication; contains only minor corrections to formatting since previous version.
1.0	16 December 2005	Approved for publication.
1.1	26 January 2006	Minor formatting corrections.
1.2	4 April 2006	Moved in the DNS information from IR.34, ENUM section updated with the agreements made the ENUM adhoc, updated the list of domains to provide a list with those defined in and/or before 3GPP specification set Rel-6. This version of the present document is the first version to be classified as "Unrestricted".
1.3	9 August 2006	Clarification of references to 3GPP documents (to show which specific release is being referenced), addition of health warnings about the old MMS URI prefix and ENUMservice field values, addition of health warning about SIP URI provisioning and some general tidying-up/consolidation of text.
2.0	30 April 2007	Addition of the "No Root" ENUM architecture, plus some other miscellaneous corrections.
2.1	18 October 2007	Minor restructuring to move ENUM material into own section, clarification in GPRS section and MMS section on using iterative rather than recursive DNS queries, clarification in MMS section of DNS usage when utilising one or more MMS Hubs and direct interconnects, and renaming of "No Root" ENUM model to "Multiple Root".

Version	Date	Brief Description
2.2	14 April 2008	Addition of information on OMA's SUPL feature, including domain name used and a new section giving a brief overview of the feature (CR #10). Also, some minor corrections to the ENUM section are provided (CR #11). Finally, a global replacement of "MNO" to "Service Provider" has been done, in-line with IPX terminology.
3.0	26 September 2008	Includes new GSMA logo on coversheet, change of "Operators" to "Service Providers" in the spec title, and implementation of the following CRs: CR #12 (major): Implementation of the conclusion from the ENUM White Paper (EWP), plus other minor corrections/enhancements. This includes corrections to domain names in sub-sections of 5.7 CR #13 (minor): Addition of EPC and ICS specific sub-domains for .3gppnetwork.org. CR #14 (minor): Addition of new sub-section to ENUMservices section to specify the content of the ENUMservices field for services other than just those based on IMS/SIP and MMS. CR #15 (minor): Addition of information about domain names, including clearer indication of the current limitations of the GRX/IPX domain names currently supported. Some minor editorial, non-technical impacting corrections are also made.
3.1	8 December 2008	Corrections to footer, plus implementation of the following CRs: CR #16 (minor): Addition of the definition of the "user=phone" SIP URI parameter in URIs returned in IMS related ENUM responses. CR #17 (minor): Correction to 4.5.1 (IMS section) to state that support of NAPTR RRs are required in order to support SIP/IMS.
3.2	6 May 2009	Implementation of CR # 18 (minor): editorial enhancements to sections 1-4, and implementation of the recently approved sub-domains of 3gppnetwork.org (as requested by 3GPP and approved at Packet #37 and on email).

Version	Date	Brief Description
3.3	21 July 2009	<p>Implementation of the following CRs:</p> <p>CR #19 (minor): Add Internet assigned domain names to be used as a sub-domain under "3gppnetwork.org", in order to save all Service Providers connected to the IPX network to have to obtain an E.212 number range in order to be addressable. Also, the procedures section is updated to reflect this change, and also better describe the current state-of-the-art.</p> <p>CR #20 (minor): Add IR.33 (GPRS Roaming Guidelines) in the references section, add a new domain name to be used for naming of non-service specific nodes, add a new section on hostnames and domains (based on content from IR.33), provide extra detail on DNS Server software (also based on content from IR.33), add new section on DNS Server naming, add new section on Resource Record usage, and add references to IR.33 and the GTP spec (3GPP TS 29.060) in section 4.2 (GPRS). Also, some instances of "operator" are corrected to "Service Provider".</p>
<p>Changes Since Last Version See 3.3 above.</p>		

Other Information

Type	Description
Document Owner	GSMA IREG Packet
Revision Control	As required
Document editor/company	Nick Russell, Vodafone UK

Feedback

This document is intended for use by the members of GSMA. 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 <mailto:prd@gsm.org>. Your comments or suggestions are always welcome.

Table of Contents

1	OVERVIEW	9
1.1	Introduction.....	9
1.2	About this document.....	9
1.3	Scope	9
1.4	References	9
1.4.1	Normative References	9
1.4.2	Informative References	11
1.5	Acronyms & Abbreviations	11
1.6	Terminology.....	11
2	DNS AS USED ON THE GRX/IPX	12
2.1	Introduction.....	12
2.2	Architecture	12
2.3	Domains	15
2.3.1	Introduction	15
2.3.2	General	15
2.3.3	Domain names owned by GSMA that are used on the GRX/IPX DNS ..	16
2.3.4	Domain names owned by GSMA that are used on the Internet DNS	23
2.4	Non-service specific hostnames and domains	25
3	GENERAL DNS CONFIGURATION INFORMATION FOR SERVICE PROVIDERS.....	26
3.1	Introduction.....	26
3.2	DNS Server Hardware.....	26
3.3	DNS Server Software	26
3.4	DNS Server naming.....	26
3.5	Domain Caching.....	26
3.6	Reverse Mapping	27
3.7	Use of DNS Interrogation Modes.....	27
3.8	Use of the GRX/IPX Root DNS Server	27
3.9	Provisioning of Service Provider's DNS servers	28
3.10	Resource Records.....	28
4	DNS ASPECTS FOR STANDARDISED SERVICES	28
4.1	Introduction.....	28
4.2	General Packet Radio Service (GPRS)	28
4.2.1	Introduction	28
4.2.2	APN resolution in PDP Context activation	29
4.2.3	Inter-SGSN handovers for active PDP Contexts.....	31
4.3	Multi-media Messaging Service (MMS)	32
4.3.1	Introduction	32
4.3.2	MM delivery based on MSISDN for the Direct Interconnect model.....	33
4.3.3	MM delivery based on MSISDN for the Indirect Interconnect model	34
4.3.4	MM delivery based on NAI/e-mail address	35
4.4	WLAN Inter-working	35
4.4.1	Introduction	35
4.5	IP Multi-media core network Sub-system (IMS)	36
4.5.1	Introduction	36
4.5.2	SIP server configuration.....	37
4.5.2.1	Step 1.....	38
4.5.2.2	Step 2.....	38

4.5.2.3	Step 3.....	38
4.5.2.4	Step 4.....	38
4.5.3	Domain Names used.....	39
4.6	Generic Authentication Architecture (GAA)	39
4.6.1	Introduction	39
4.7	Generic Access Network (GAN)	39
4.7.1	Introduction	39
4.8	Secure User Plane Location (SUPL)	39
4.8.1	Introduction	39
4.9	Enhanced Packet Core (EPC)	39
4.9.1	Introduction	39
4.10	IMS Centralised Services (ICS)	40
4.10.1	Introduction	40
4.11	Access Network Discovery Support Function (ANDSF)	40
4.11.1	Introduction	40
5	E.164 NUMBER TRANSLATION (ENUM)	40
5.1	Introduction.....	40
5.2	ENUM FQDN Format	40
5.3	ENUM Tiers.....	41
5.4	Types of ENUM	41
5.5	Technical Requirements for Interworking	42
5.5.1	Domain name.....	42
5.5.2	URI formats	43
5.5.2.1	Introduction	43
5.5.2.2	IMS URI format	43
5.5.2.3	MMS URI format	43
5.5.3	When to provision numbers in the ENUM Database.....	44
5.5.4	Application of interconnection policy	44
5.5.5	ENUMservice field.....	45
5.5.5.1	Introduction	45
5.5.5.2	IMS.....	45
5.5.5.3	MMS.....	45
5.5.5.4	Other services.....	45
5.5.6	Example Data-fill	45
5.6	Structure and Delegation Model	46
5.6.1	Introduction	46
5.6.2	Architecture	47
5.6.3	Example resolution.....	48
5.6.4	Access to ENUM servers	49
5.7	Solving Number Portability in ENUM	49
5.7.1	Introduction	49
5.7.2	Option 1 – Central authoritative database.....	49
5.7.2.1	Description	49
5.7.2.2	Example Configuration.....	50
5.7.2.3	Advantages and Disadvantages	50
5.7.2.4	Suitability.....	50
5.7.3	Option 2 – Change of domain name in URIs/URLs in Tier-2	50
5.7.3.1	Description	50
5.7.3.2	Example	50
5.7.3.3	Advantages and Disadvantages	51
5.7.3.4	Suitability.....	51
5.7.4	Option 3 – Redirection at Tier 2	51
5.7.4.1	Description	51
5.7.4.2	Example	52
5.7.4.3	Advantages and Disadvantages	52

5.7.4.4	Suitability.....	53
5.7.5	Option 4 – Central re-direction database	53
5.7.5.1	Description	53
5.7.5.2	Example	53
5.7.5.3	Advantages and Disadvantages	54
5.7.5.4	Suitability.....	54
6	PROCESSES & PROCEDURES RELATING TO DNS	54
6.1	Introduction.....	54
6.2	Procedures Relating to Domain Names	54
6.2.1	Domains and their Allocation	54
7	ANNEX A: SAMPLE BIND DNS CONFIGURATION FOR GPRS.....	55
7.1	Introduction.....	55
7.2	The "named.conf" file	55
7.2.1	The "named.conf" file for a PLMN Master Nameserver	55
7.2.2	The "named.conf" file for a PLMN slave Nameserver	56
7.3	Zone Configuration Files	56
7.3.1	The "gprs.hint" file	56
7.3.2	The "0.0.127.in-addr.arpa" file	57
7.3.3	PLMN zone files	57
7.3.3.1	The "mnc091.mcc244.gprs" file	57
7.3.3.2	The "sonera.fi.gprs" file.....	57
7.3.4	The "hosts" file	57
7.3.5	The "168.192.in-addr.arpa" file	59
8	ANNEX B: ALTERNATIVE ENUM ARCHITECTURE: THE MULTIPLE ROOT MODEL.....	60
8.1	Introduction.....	60
8.2	Architecture	60
8.3	Resolution	62
8.4	Access to ENUM Servers	64
8.5	Interworking with the preferred model	64

1 OVERVIEW

1.1 Introduction

Inter-Service Provider IP communications are starting to evolve to support services other than GPRS Roaming. Many, if not all, of these services rely upon DNS. Therefore, it is of utmost importance for the interworking and stability of such services that Service Providers have all the necessary information to hand to ease configuration of their DNS servers upon which such services rely.

1.2 About this document

This document is intended to provide guidelines and technical information for those who need to set-up and/or maintain DNS servers for inter-Service Provider services. This document is not intended to provide a general education on DNS or ENUM. Thus, a reasonable level of technical competence in DNS, ENUM and DNS/ENUM server configuration is assumed through out this document.

1.3 Scope

This GSMA official document provides recommendations on DNS (including ENUM) to facilitate successful interworking of inter-Service Provider services. In particular, guidelines for general and service specific configuration of DNS/ENUM servers, GSMA processes and procedures relating to formats and usage of domain names and sub-domain names, updates to the GRX/IPX Root DNS Server and guidelines and recommendations on GSMA Carrier ENUM.

Particular attention is given to DNS/ENUM servers connected to the private, inter-Service Provider backbone network known as the "GRX" or "IPX", as described in GSMA PRD IR.34 [12].

Out of the scope of this document are vendor specific implementation/architecture options and configuration of DNS/ENUM servers used on the Internet (e.g. those DNS servers attached to the Internet for web site hosting). The only exception to this is the guidelines for sub-domains used for any standardised services that specifically use the Interneti.e. those that use the "pub.3gppnetwork.org" domain name.

Host name recommendations are also outside the scope of this document. They can be found in GSMA PRD IR.34 [12].

1.4 References

1.4.1 Normative References

The following are referenced in the body of the text in this permanent reference document (PRD):

- [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"
- [10] GSMA PRD IR.61: "WLAN Roaming Guidelines"
- [11] GSMA PRD IR.65: "IMS Roaming and Interworking Guidelines"
- [12] GSMA PRD IR.34: "Inter-PLMN Backbone Guidelines"
- [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)"
- [19] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture", version 6.9.0 or higher
- [20] 3GPP TS 43.318: "Generic Access to the A/Gb interface; Stage 2", version 6.6.0 or higher
- [21] 3GPP TS 44.318: "Generic Access (GA) to the A/Gb interface; Mobile GA interface layer 3 specification", version 6.5.0 or higher
- [22] 3GPP TS 23.236: "Intra Domain Connection of RAN Nodes to Multiple CN Nodes", version 6.3.0 or higher
- [23] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2", version 6.14.0 or higher
- [24] IETF RFC 3824: "Using E.164 numbers with the Session Initiation Protocol (SIP)"
- [25] IETF RFC 1032: "Domain administrators guide"
- [26] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface"
- [27] OMA OMA-AD-SUPL-V1_0-20070615-A "Secure User Plane Location Architecture; Approved Version 1.0 – 15 June 2007"
- [28] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"
- [29] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses"
- [30] 3GPP TS 23.292: "IP Multimedia System (IMS) centralized services; Stage 2"
- [31] GSMA PRD IN.12: "ENUM White Paper"
- [32] <http://www.iana.org/assignments/enum-services>: "ENUMservice Registrations"
- [33] IETF RFC 3764: "enumservice registration for Session Initiation Protocol (SIP) Addresses-of-Record"
- [34] IETF RFC 4355: "IANA Registration for Enumservices 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.
- [36] ITU-T Recommendation E.212: "The international identification plan for mobile terminals and mobile users"
- [37] ITU-T Recommendation E.164: "The international public telecommunication numbering plan"
- [38] IETF RFC 3261: "SIP: Session Initiation Protocol"

[39] GSMA PRD IR.33: "GPRS Roaming Guidelines"

1.4.2 Informative References

The following are not referenced in the body of the text in this PRD; however they give more insight into DNS specific functionality:

[i] IETF RFC 4282: "The Network Access Identifier"

1.5 Acronyms & Abbreviations

Term	Meaning
CC	Country Code
DNS	Domain Name System
ENUM	E.164 Number Mapping
ESP	ENUM Service Provider
FQDN	Fully Qualified Domain Name
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
IMS	IP Multimedia Sub-system
MCC	Mobile Country Code
MMS	Multimedia Messaging Service
MNC	Mobile Network Code
MNP	Mobile Number Portability
NAI	Network Access Identifier
NDC	National Destination Code
NP	Number Portability
SN	Subscriber Number
WLAN	Wireless LAN

1.6 Terminology

Delegation: When a part of a zone is maintained separately, it is delegated to a new nameserver that will have authority of that part of the domain namespace. The original zone will have the nameserver (NS) record for the delegated domain and the new sub-zone will have a new Start Of Authority (SOA) record.

DNS Client: See "DNS Resolver".

Domain Name: A Domain Name consists of two or more labels separated with a dot ('.') character. It starts from the least significant domain on the left, and ends with the most significant domain (or top-level domain) on the right. This naming convention naturally defines a hierarchy.

DNS Resolver: Also known as a "DNS Client", this is an entity that is attempting to resolve a given domain name to an address or vice versa. Usually the DNS Resolver is connected to a local DNS caching server that performs the DNS look-ups on behalf of the DNS Resolver. Application programs use function calls, such as 'gethostbyname', to find the IP address representing a domain name. The name may be specified either as a Fully Qualified Domain Name (FQDN) or only partially. In the

latter case, the DNS Resolver appends (a) configured local domain name(s) at the end of the name.

DNS Server: A DNS Server can be a Nameserver, a Local Caching DNS Server or both. It is common that all DNS Servers cache results from queries for a specific amount of time.

GRX/IPX: GPRS roaming eXchange/IP Packet eXchange. The GRX/IPX is an inter-operator IP backbone network that is transparent to subscribers. It is used for back-end routing/tunnelling purposes only.

Nameserver: Takes care of DNS Queries sent by DNS Resolvers. The query is answered by using locally stored information (either configured locally or cached from a previous query result), by requesting the information from another DNS Server, or by providing the DNS Resolver with the details of another DNS Server to query. One Nameserver can serve (i.e. be authoritative for) several domains. There may also be several Nameservers serving one domain (usually one is the Primary, and the other/rest are Secondaries).

Zone: DNS is a distributed database that contains information of each domain name. Each DNS server maintains a part of the database called a zone. Usually a zone contains information of one domain. However, one zone may contain information about many (sub)domains. Each information element is stored in a record that contains at least a domain name and type (which includes type specific information).

2 DNS AS USED ON THE GRX/IPX

2.1 Introduction

The Domain Name System is critical to such services as GPRS roaming, inter-PLMN MMS delivery and IMS inter-working. DNS is defined in many IETF RFC documents; the most notable ones are IETF RFC 1034 [1] and IETF RFC 1035 [2].

2.2 Architecture

The DNS on the inter-PLMN IP backbone network (known as the "GRX/IPX") is completely separate from the DNS on the Internet. This is purposely done to add an extra layer of security to the GRX/IPX network, and the nodes within it. The GRX/IPX Root DNS Servers that network operators see are known as "Slave" Root DNS Servers and are commonly provisioned by that Service Provider's GRX/IPX Service Provider. However, these Slave Root DNS Servers can be provisioned by operators themselves if they so wish.

Each Slave Root DNS Server is synchronised with a "Master" Root DNS Server. This process of synchronisation is known as a "Zone Transfer" and ensures that the data is the same in all GRX/IPX Service Providers' and Operators' Slave Root DNS Servers. The following diagram depicts this:

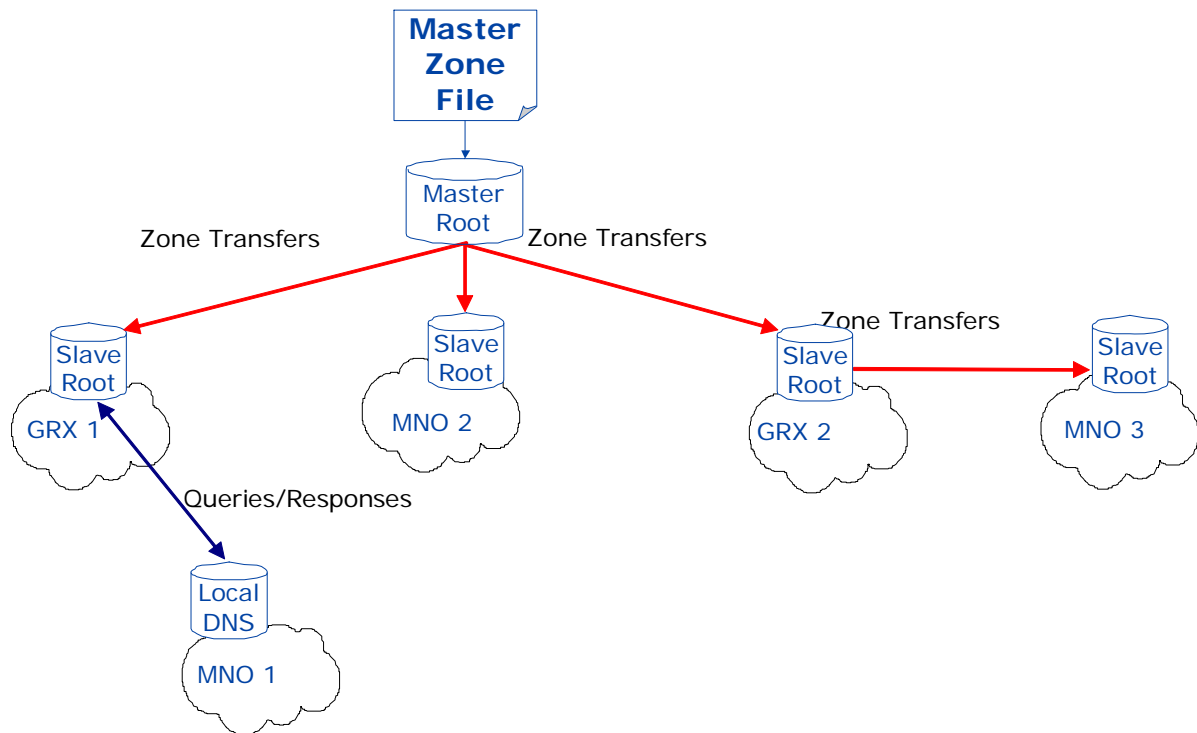


Figure 1: Backbone Architecture

The data in the Master Root DNS Server is known as the Master Zone File. The population of the data that goes into the Master Zone File has a number of sources, mainly Operators, GRX/IPX Providers and GRX/IPX Providers acting on behalf of Operators. It is also policed and validated by the Master Root DNS Server providers (under authority from GSMA) to ensure such things as correct sub-domain allocation and usage etc. The following diagram depicts this:

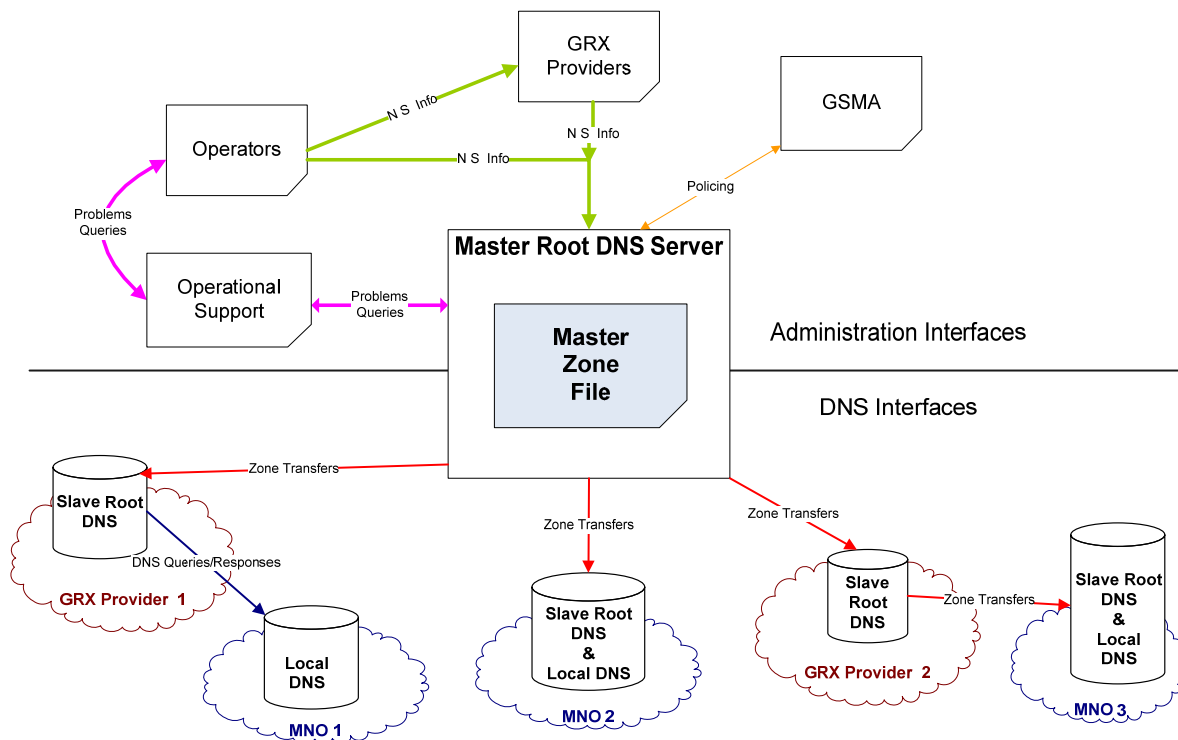


Figure 2: Overall Process Architecture

Finally, the following shows the architecture and the *typical* signalling involved in resolving hostnames to IP addresses or vice versa. The numbered steps below in the diagram correspond to the numbered message flows:

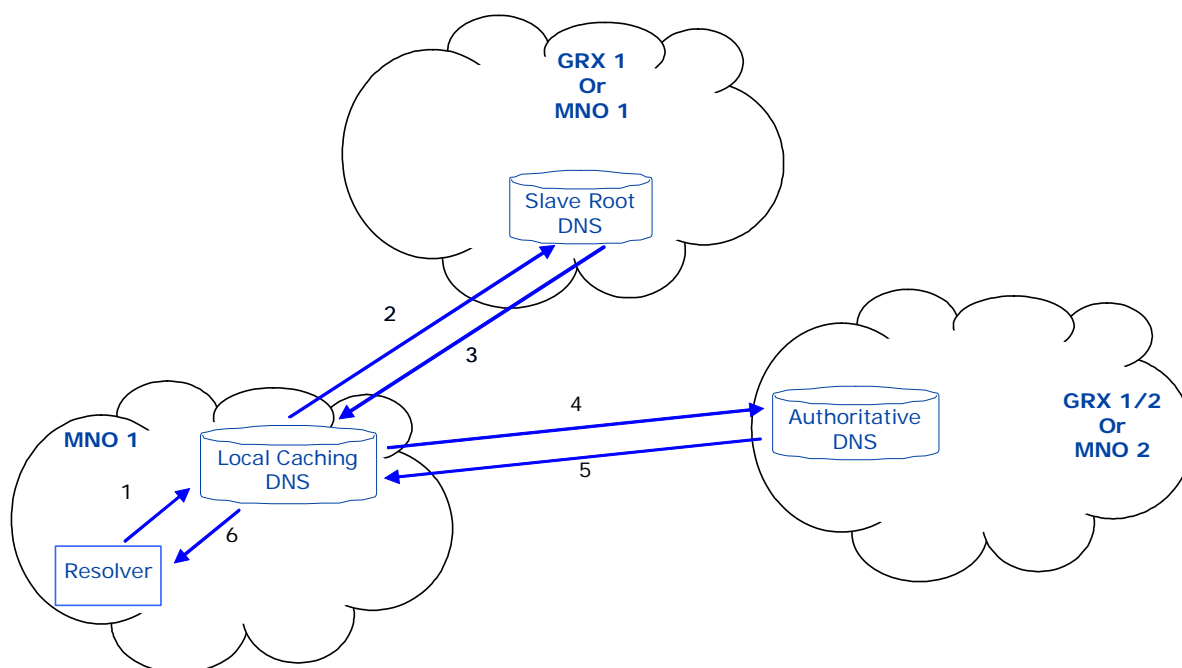


Figure 3: Resolver Architecture

- 1 The Resolver (e.g. an SGSN trying to find out the IP address of a GGSN) sends a query for the hostname (e.g. an APN) for which it wants the IP address, to its local caching DNS server.

- 2 The local caching DNS server checks to see if it has the answer to the query in its cache. If it does it answers immediately (with message 6). Otherwise, it forwards the query on to the Root DNS server. The Root DNS server may reside in Service Provider 1's network or it may reside in the GRX/IPX provider's network (GRX1). The address(es) of the Root DNS server may either be statically configured or be found by using Host Anycasting (see below).
- 3 The Root DNS server returns a referral to the DNS server which is authoritative for the queried domain name of the hostname (e.g. returns the authoritative server for "mnc015.mcc234.gprs").
- 4 The local caching DNS server caches the response for a specified amount of time (specified by the root DNS server) and then re sends the query but to the authoritative DNS server as specified by the Root DNS server. The authoritative DNS server may reside in the same GRX/IPX provider's network (GRX1), another GRX/IPX provider's network (GRX2) or the network of the destination Mobile Network Operator (Service Provider 2). (Indeed, it may even reside in the requesting Service Provider's network!)
- 5 The Authoritative DNS server responds to the query with the address of the hostname (or responds with a hostname, if a reverse lookup is being performed) to the Local Caching server in the requesting network (Service Provider 1).
- 6 The Local Caching Server caches the response for a specified amount of time (specified by the authoritative server) and forwards it on to the Resolver.

Note: The above shows only a typical message flow for DNS resolving on the GRX/IPX. It may take extra queries for such services/enablers as those that require ENUM. Please refer to section 4 for more detailed information for each service, and section 5 for more detailed information on ENUM.

2.3 Domains

2.3.1 Introduction

The following sub-sections detail the domain names that can and cannot be used on the GRX/IPX network.

In addition to this, the 3GPP have designated a specific sub domain for usage on the Internet's DNS to enable user equipment to locate a specific server on the Internet (terminals cannot see the GRX/IPX therefore a whole new sub domain had to be introduced). For more information on which domains used by 3GPP are intended for which network, see 3GPP TS 23.003 [8], Annex D.

2.3.2 General

Unlike the DNS on the Internet, the DNS on the GRX/IPX network is currently much "flatter". That is, there are not so many domains (and sub-domains of thereof), supported and provisioned in the GRX/IPX Root DNS Server. This inherently means that all domain names used by Service Providers and GRX/IPX Providers in any service that utilises the GRX/IPX network are limited to just the domain names detailed in section 2.3.3 below. **No other domain name formats are currently supported on the GRX/IPX network!** This effectively means a limitation of sub-domains of ".gprs" and ".3gppnetwork.org" at the higher level, and limited beneath to sub-domains of a format based on ITU-T recommendation E.212 [36] number ranges as well as so called "human friendly" sub-domains. The latter consists of simply an FQDN reserved in the Internet domain name space e.g. serviceprovider.fi, serviceprovider.co.uk. See section 2.3.3 below for more details.

More information on processes and procedures relating to domain names can be found in section 6.

2.3.3 Domain names owned by GSMA that are used on the GRX/IPX DNS

The following provides a summary of the domain names owned by GSMA that are used by Service Providers on private IP inter-connects and the GRX/IPX. These domain names are only resolvable by network equipment and not by end users.

For more detail about each domain name and/or sub-domain name, refer to the referenced documents.

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
.gprs	<p>Service Provider domains of the form: <Network Label>.mnc<MNC>.mcc<MCC>.gprs</p> <p>Where <Network Label> is the Network Label part of the Access Point Name (APN) as defined in 3GPP TS 23.003 [8] section 9, and <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in GPRS for the Operator ID in APNs. See section 4.2.1 and also 3GPP TS 23.003 [8], section 9 for more information.</p>	<p>Each Service Provider is allowed to use only sub-domains consisting of MNC(s) and MCC(s) that are allocated to them by ITU-T and their local national numbering authority.</p> <p>Service Providers should avoid using Network Labels consisting of any of the below defined sub-domains, in order to avoid clashes.</p>	<p>Domain needs to be resolvable by at least all GPRS/PS roaming partners.</p>
	<p>rac<RAC>.lac<LAC>.mnc<MNC>.mcc<MCC>.gprs</p> <p>Where <RAC> and <LAC> are the Routing Area Code and Location Area Code (respectively) represented in hexadecimal (base 16) form, and <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in inter-SGSN handovers (i.e. Routing Area Updates) by the new SGSN (possibly in a new PLMN) to route to the old SGSN (possibly in the old PLMN). See section 4.2.2 and also 3GPP TS 23.003 [8], Annex C.1, for more information.</p>	<p>Each Service Provider is allowed to use only sub-domains consisting of MNC(s) and MCC(s) that are allocated to them by ITU-T and their local national numbering authority.</p>	<p>Domains need to be resolvable by at least all SGSNs to which a UE can hand over (which may be in other networks, if inter network GPRS/PS handovers are supported in a Service Provider's network).</p>

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
	<p>nri<NRI>.rac<RAC>.lac<LAC>.mnc<MNC>.mcc<MCC>.gprs</p> <p>Where <NRI>, <RAC> and <LAC> are the Network Resource Identifier, Routing Area Code and Location Area Code (respectively) represented in hexadecimal (base 16) form, and <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in Routing Area Updates by the new SGSN (possibly in a new PLMN) to route to the old SGSN (possibly in the old PLMN), where Intra Domain Connection of RAN Nodes to Multiple CN Nodes (also known as "RAN flex" – see 3GPP TS 23.236 [22]) is applied. See section 4.2.2 and also 3GPP TS 23.003 [8], Annex C.1, for more information.</p>		
	<p>rnc<RNC>.mnc<MNC>.mcc<MCC>.gprs</p> <p>Where <RNC> is the RNC ID represented in hexadecimal (base 16) form, and <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in SRNS relocation to route to the target RNC in the new SGSN (possibly in a new PLMN). See section 4.2.2 and also 3GPP TS 23.003 [8], Annex C.3, for more information.</p>		
	<p>mms.mnc<MNC>.mcc<MCC>.gprs</p> <p>Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in MMS for the domain name part of the FQDN for MMSCs. See section 4.3 and also 3GPP TS 23.140 [15], section 8.4.5.1, for more information.</p>		<p>Domain needs to be resolvable by at least all directly connected MMS interworking partners/Service Providers and directly connected MMS Hub Providers.</p>

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
	<p><Internet_assigned_domain_name>.gprs</p> <p>Where <Internet_assigned_domain_name> is a domain name reserved by the Service Provider on the Internet. An example is "example.com.gprs"</p>	<p>Used as an alternative Operator ID in APNs (also known as "Human Readable APNs"). See 3GPP TS 23.003 [8], section 9 for more details.</p>	<p>The domain name(s) used must be owned by that Service Provider on the Internet. If the domain name(s) expire on the Internet, they also expire on the GRX/IPX. Care should be taken to ensure there is no clash with the other sub-domains for ".gprs" as defined above.</p>	<p>Domain needs to be resolvable by at least all GPRS/PS roaming partners.</p>
.3gppnetwork.org	<p>ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org</p> <p>Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in IMS in SIP addressing; specifically in the Private and Public Identities used in SIP registration. See 3GPP TS 23.003 [8] section 13 for more information.</p>	<p>Each Service Provider is allowed to use only sub-domains consisting of MNC(s) and MCC(s) that are allocated to them by ITU-T and their local national numbering authority.</p>	<p>Domain needs to be resolvable by at least all SIP/IMS based service inter working partners/Service Providers, as well as roaming partners where a visited P-CSCF is used.</p>
	<p>wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org</p> <p>Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in WLAN inter-working for NAI realms. See 3GPP TS 23.003 [8] section 14, for more information.</p>	<p>Sub-domains within the Service Provider's domain (i.e. mnc<MNC>.mcc<MCC>) are documented in 3GPP TS 23.003 [8]. It is recommended that</p>	<p>Since this is a realm, not a domain name, it does not necessarily have to be resolvable by external entities. The only time this is used in DNS is when Diameter is used and the next hop is determined by DNS rather than a look up table.</p>

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
	<p>gan.mnc<MNC>.mcc<MCC>.3gppnetwork.org</p> <p>Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in the Generic Access Network for Full Authentication NAI realms and Fast Re-authentication NAI realms. See 3GPP TS 23.003 [8] section 17.2, for more information.</p>	<p>Service Providers do not use other sub-domains that are not specified in 3GPP, OMA or in this PRD as this could potentially cause a clash of sub-domain usage in the future.</p>	<p>Since this is a realm, not a domain name, it does not necessarily have to be resolvable by external entities. The only time this is used in DNS is when Diameter is used and the next hop is determined by DNS rather than a look up table.</p>
	<p>epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org</p> <p>Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in the Enhanced Packet Core (EPC) architecture (previously known as Service Architecture Evolution – SAE) for NAIs and FQDNs of EPC related nodes. See 3GPP TS 23.003 [8] section 19 for more information.</p>		<p>Domain and sub-domains need to be resolvable by EPC/SAE roaming partners.</p>
	<p>ics.mnc<MNC>.mcc<MCC>.3gppnetwork.org</p> <p>Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in the IMS Centralised Services feature in SIP addressing. See 3GPP TS 23.003 [8] section 20 for more information.</p>		<p>Domain should only be resolvable for CS roaming partners where an MSC (Server) enhanced for ICS is allowed to be used in that visited partner's network.</p>

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
	node.mnc<MNC>.mcc<MCC>.3gppnetwork.org	Used by Service Providers to provide FQDNs to non-service specific nodes/hosts e.g. DNS/ENUM servers, routers, firewalls etc. See section 2.4 of this document for more information.	Each Service Provider is allowed to use only sub-domains consisting of MNC(s) and MCC(s) that are allocated to them by ITU-T and their local national numbering authority.	Domain needs to be resolvable by at least all roaming/interworking partners for the services used by this domain name.
	<Internet_assigned_domain_name>.3gppnetwork.org Where <Internet_assigned_domain_name> is a domain name reserved by the Service Provider on the Internet. An example is: "example.com.3gppnetwork.org". Further sub-domains under this are the responsibility of the owning Service Provider. However, it is recommended to use/reserve the sub-domains defined above for the MNC/MCC format.	Not used in any particular service, however, can be used by any Service Provider for any service they see fit. The main intention is to provide a domain name that Service Providers without an E.212 number range allocation can use when connecting to the IPX network.	The sub-domains used must be owned by that Service Provider on the Internet. If the sub-domains expire on the Internet, they also expire on the GRX/IPX DNS!	Domain needs to be resolvable by at least all roaming/interworking partners for the services used by this domain name.
	unreachable.3gppnetwork.org	Used in WLAN inter-working, specifically as a realm in the Alternative NAI. It's purpose is to enable the UE to retrieve a list of PLMNs behind an WLAN Access Point. See 3GPP TS 23.003 [8], sub-section 14.6 for more information.	Neither a Service Provider, a GRX/IPX Provider nor any other entity should use this domain name. It is simply reserved to never be used!	Intentionally not resolvable by any entity.

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
.e164enum.net	The sub-domains of this domain name correspond to reversed ITU-T E.164 numbers (as defined in ITU-T Recommendation E.164 [37]).	Used as the domain name for ENUM queries to the GRX/IPX Carrier ENUM as defined in section 5 of the present document.	Each Service Provider is allowed to use only sub-domains relating to their subscribers. See section 5 for more information.	See section 5 for more information.
.in-addr.arpa	The sub-domains of this domain name correspond to reversed IPv4 addresses that belong to the Service Provider.	Used for reverse lookups for IPv4 addresses i.e. mapping names to IPv4 addresses. This is useful when troubleshooting inter-PLMN connections. Due to available tools being pre-configured to use this hierarchy for reverse look-ups, it would not be feasible to use any different TLD.	Each Service Provider shall populate this domain for IP addresses assigned to them only (except with permission of the actual owner).	Domain should be resolvable by at least all interworking partners/Service Providers, roaming partners and directly connected GRX/IPX Providers.
.ip6.arpa	The sub-domains of this domain name correspond to reversed IPv6 addresses that belong to the Service Provider.	Used for reverse lookups for IPv6 addresses i.e. mapping names to IPv6 addresses. This is useful when troubleshooting inter-PLMN connections. Due to available tools using this hierarchy for reverse look-ups, it would not be feasible to use any different TLD.		

2.3.4 Domain names owned by GSMA that are used on the Internet DNS

The following provides a summary of the domain names owned by GSMA that are used by Service Providers on the Internet for 3GPP specific services. For more detail about each domain name and/or sub-domain name, refer to the referenced documents.

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
pub.3gppnetwork.org	<p>gan.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org</p> <p>Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in the Generic Access Network for home network domain names in node identifiers. See 3GPP TS 23.003 [8] section 17.3, for more information.</p>	<p>Each Service Provider is allowed to use only sub-domains consisting of MNC(s) and MCC(s) that are allocated to them by ITU-T and their local national numbering authority.</p> <p>The host names "psegw" and "pganc" under this sub-domain are reserved for special use, as detailed in 3GPP TS 23.003 [8], section 17.3</p>	Domains need to be resolvable on the Internet.
	<p>w-apn.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org</p> <p>Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in WLAN inter-working for PDG addressing. See 3GPP TS 23.003 [8] section 14, for more information.</p>	<p>Each Service Provider is allowed to use only sub-domains consisting of MNC(s) and MCC(s) that are allocated to them by ITU-T. The same rules apply for APN constructs, as defined in GSMA PRD IR.34.</p>	

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
	<p>h-slp.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org</p> <p>Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in the Secure User Plane Location feature for Home SUPL Location Platform addressing. See OMA-AD-SUPL-V1_0-20070615-A [27] section 7.2.2, for more information.</p>	<p>Each Service Provider is allowed to use only sub-domains consisting of MNC(s) and MCC(s) that are allocated to them by ITU-T and their local national numbering authority.</p>	
	<p>bsf.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org</p> <p>Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in the Generic Authentication Architecture for BSF addressing. See 3GPP TS 23.003 [8] section 16, for more information.</p>		
	<p>andsf.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org</p> <p>Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>		<p>Each Service Provider is allowed to use only sub-domains consisting of MNC(s) and MCC(s) that are allocated to them by ITU T. The same rules apply for APN constructs, as defined in GSMA PRD IR.34 [12].</p>	
	<p>ha-apn.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org</p> <p>Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form.</p>	<p>Used in EPC and WLAN inter working (3GPP Rel 8) home agent addressing. See 3GPP TS 23.003 [8] section 21, for more information.</p>		

2.4 Non-service specific hostnames and domains

Having a consistent naming convention makes it easier for tracing and trouble shooting as well as easing the maintenance of Service Provider's DNS. The following convention is recommended to achieve these goals. Although the usage of this naming methodology is highly recommended, it is not mandated.

Service Provider nodes should have names for each interface with the following format:
<city>-<type>-<nbr>

where:

<city> is the name, or shortened name, of the city/town (or closest, where applicable) where the node is located

<nbr> is a running number of similar devices at the same city (for DNS servers, use 0 to indicate the primary DNS Server)

<type> describes device type and should be one of the following for GRX/IPX connected hosts:

- dns - DNS/ENUM servers
- ggsn
- sgsn
- rtr - router
- fw - firewall

Additional values for the <type> parameter are for further study for the GRX/IPX. For example, the following are valid hostnames for interfaces on Service Provider nodes:

helsinki-ggsn-4

The domain name to append to hostnames for nodes belonging to Service Providers should be the following (see section 2.3 for more details on the domain name formats):

node.mnc<MNC>.mcc<MCC>.3gppnetwork.org

node.<Internet_assigned_domain_name>.3gppnetwork.org

A combination of the above domain names could be used by a Service Provider; however, for consistency it is better to use only one.

The following are thus example fully qualified domain names (FQDNs) for interfaces on Service Provider nodes:

helsinki-ggsn-4.node.mnc015.mcc234.3gppnetwork.org

london-dns-23.node.example.com.3gppnetwork.org

Note that usage of the above listed hostnames under "mnc<MNC>.mcc<MCC>.gprs" is now deprecated, and Service Providers are recommended to use either or both of the above domain names at their earliest convenience.

3 GENERAL DNS CONFIGURATION INFORMATION FOR SERVICE PROVIDERS

3.1 Introduction

This section gives some general information on DNS server configuration for operators. For information on configuring DNS servers for specific services, see sections 4 and 5.

3.2 DNS Server Hardware

It is recommended that operators have physically separate Primary and Secondary DNS servers. This helps provide the greatest service availability and allows for e.g. upgrading DNS Servers without any service interruption.

3.3 DNS Server Software

Most commonly ISC BIND (usually version 4 or version 9) is the chosen software supplied by equipment vendors with any new service equipment that utilises a DNS Nameserver. Service Providers and IPX Providers should ensure that only the most secure version is used in their live networks, and all security patches are applied. Note that no particular version of BIND is recommended, because to do so here would provide potentially out of date information to the reader.

Use of ISC BIND is fine for services which do not necessarily have a large data-fil (for example: GPRS, MMS) but for services such as ENUM where the data-fil can run into thousands, if not millions of resource records, a commercial DNS Nameserver product should be used.

Such commercial DNS Nameserver solutions can also support legacy DNS data-fil (for example, that used for GPRS roaming), thereby consolidating all operator DNS needs. Note that it is out of the scope of this document, and the GSMA, to provide any recommendations on commercial DNS Nameservers. In fact, diversity of DNS software used by Service Providers and IPX Providers gives a better overall robustness of the DNS on GRX/IPX network.

3.4 DNS Server naming

All DNS servers need to have an FQDN assigned to them. For Service Provider DNS servers connected to the GRX/IPX, the naming conventions as specified in section 2.4 shall be used.

3.5 Domain Caching

Since each service (e.g. GPRS, MMS etc) has its own domain, a separate TTL value can be set per service.

When setting the TTL value for a zone, careful consideration must be taken to ensure that the right trade-off is made between performance and consistency. A small TTL value results in a greater signalling overhead, greater processing overhead for the authoritative name server(s) and greater time for a returning a result (an example: GPRS PDP Context set-up time), but the data will be more up-to-date therefore allowing updates to propagate much more quickly. A large TTL value results in a smaller signalling overhead, smaller processor overhead for the authoritative name server(s) and usually shorter time for returning a result to the requesting entity, but the data will be more likely to be out of date and therefore resulting in updates taking longer to propagate.

It is highly recommended that negative caching is also used (available in ISC BIND versions 4.9, 8.x and 9.x and should be available in most commercial DNS solutions). Again, careful consideration should be taken, considering factors such as the frequency of updates, signalling overhead and processing overhead of the authoritative DNS server for the domain.

3.6 Reverse Mapping

Each operator is strongly recommended to provide reverse mapping of all FQDNs that they use e.g. for APNs, MMSC addresses etc. This is not mandatory for inter-working to be successful, but rather, it aids in trouble shooting/debugging activities such as performing a "traceroute".

3.7 Use of DNS Interrogation Modes

Two interrogation modes are defined in the DNS specifications: iterative and recursive. In Iterative mode, a DNS server interrogates each DNS server in the hierarchy itself, in order to resolve the requested domain name. In Recursive Mode, a DNS server interrogates only the next DNS server in the DNS hierarchy. That DNS Server then takes on responsibility for resolving the requested domain name and provides a final answer back to the original requesting DNS server. Figure 3 below depicts both iterative and recursive queries:

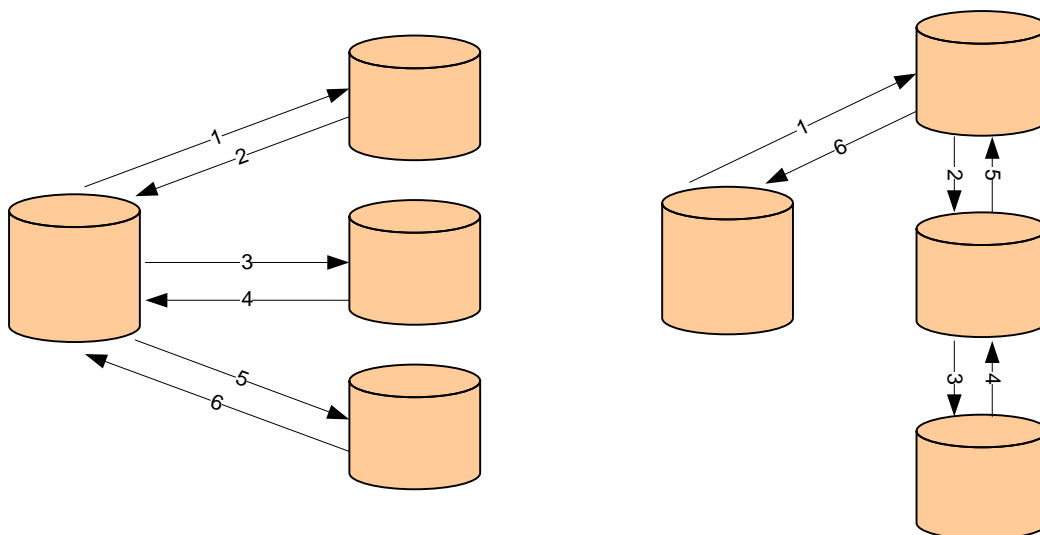


Figure 3 - Iterative (left) and Recursive (Right) modes of DNS querying

Only Iterative DNS queries shall be used within the GRX/IPX. This not only saves on DNS Server load but also to enables visibility of the source of the original request at the destination, which is lost when using recursive queries.

If any recursive DNS queries are received by a DNS Server then they should be ignored. The only elements that should issue recursive DNS queries are service nodes issuing DNS requests to their Local Caching DNS Servers e.g. an SGSN querying its Local Caching DNS Server for an APN (see sub-section 4.2 for more information on GPRS, including APN resolution).

3.8 Use of the GRX/IPX Root DNS Server

There are two possibilities to arrange DNS hierarchy. The first is for each Service Provider to configure their own authoritative DNS Server for each domain name that needs to be

resolved for all inter-working and roaming partner Service Providers. The draw back of this approach is that it is not scalable because every time a new inter-working and/or roaming partner agreement is made, or even any existing inter-working and/or roaming partner's DNS Server details change, the aforementioned authoritative DNS Server must be updated accordingly. Thus, a potential operational intensive task, and most likely a frequent source for inter-working and roaming problems. This alternative may be fine for small Service Providers with few interworking and/or roaming partners, but is not recommended due to the reasons stated. Therefore, this alternative is not further detailed in the present document.

Another alternative is to use the common GRX/IPX Root DNS Server, as provided for by the GRX/IPX service provider (see section 2.2 for more detail on this architecture). Using the GRX/IPX Root DNS Server enables modified DNS Server details for a Service Provider to automatically propagate to all interworking and roaming partners (subject to caching time). This alternative is the recommended one, and is thus the assumed deployment of authoritative DNS Servers in the rest of the present document.

3.9 Provisioning of Service Provider's DNS servers

Service Providers should take care to share all appropriate data to enable all roaming/inter-working partners routing to an authoritative DNS Server, i.e. a DNS Server where their own domain names can be resolved by others. GSMA IR.21 (PRD or GSMA InfoCentre database) and the GRX/IPX Root DNS should be used to ease such sharing of data, wherever possible.

Service Providers can provision authoritative DNS Servers themselves or outsource to another entity e.g. their GRX/IPX Provider.

3.10 Resource Records

Service Providers and IPX Providers should take care to provision only the DNS Resource Records (RRs) that are absolutely necessary.

4 DNS ASPECTS FOR STANDARDISED SERVICES

4.1 Introduction

This section describes the DNS aspects of standardised services that utilise DNS. Recommendations are made, where appropriate, beyond what is defined in the referenced specifications in order to promote easier service interworking for Service Providers. The list of services below is not exhaustive and other services that utilise DNS on the GRX/IPX can be used.

If there are discrepancies between the description of the services and the referenced specifications in the following sub-sections, what is stated in the referenced specifications shall prevail.

4.2 General Packet Radio Service (GPRS)

4.2.1 Introduction

GPRS provides for a packet switched bearer in GSM/UMTS networks. Packets are tunnelled between core network nodes that may or may not be in different PLMNs, using the GPRS Tunnelling Protocol (GTP) as defined in 3GPP TS 29.060 [24].

Note that in UMTS, GPRS is referred to as "Packet Switched" access, however, this is just a naming convention, and the mechanism remains the same.

For more information on GPRS/Packet Switched access, see GSMA PRD IR.33 [39], 3GPP TS 23.060 [26], and 3GPP TS 29.060 [24].

4.2.2 APN resolution in PDP Context activation

PDP Context activations occur between the SGSN and the GGSN. PDP Contexts are activated to an Access Point Name either provided by the MS, or derived by the network (such as when the MS instructs the SGSN to use a "default" APN). It is the APN that determines to which interface on which GGSN the PDP Context is to be established. See sub-section 2.3 for the format of APNs. Further details on the APN can be found in GSMA PRD IR.33 [39].

An SGSN and a GGSN can be located in either the HPLMN or VPLMN. Both are in the same network when the subscriber is in the HPLMN and also when the subscriber is roaming in a VPLMN and is using a GGSN in the VPLMN (vGGSN). However, the SGSN and GGSN are in different networks when the subscriber is roaming but using a GGSN in the HPLMN (hGGSN).

GPRS roaming means the extension of packet switched services offered in the Home PLMN to Visited PLMNs with which the HPLMN has a predefined commercial roaming agreement.

The necessary DNS queries for resolving an APN in order to activate a PDP Context are described below. Note that the Authoritative DNS Server is usually located in the same PLMN as the GGSN, but can be located elsewhere, for example, in the HPLMN's GRX/IPX provider's network (due to the HPLMN outsourcing the Authoritative DNS Server).

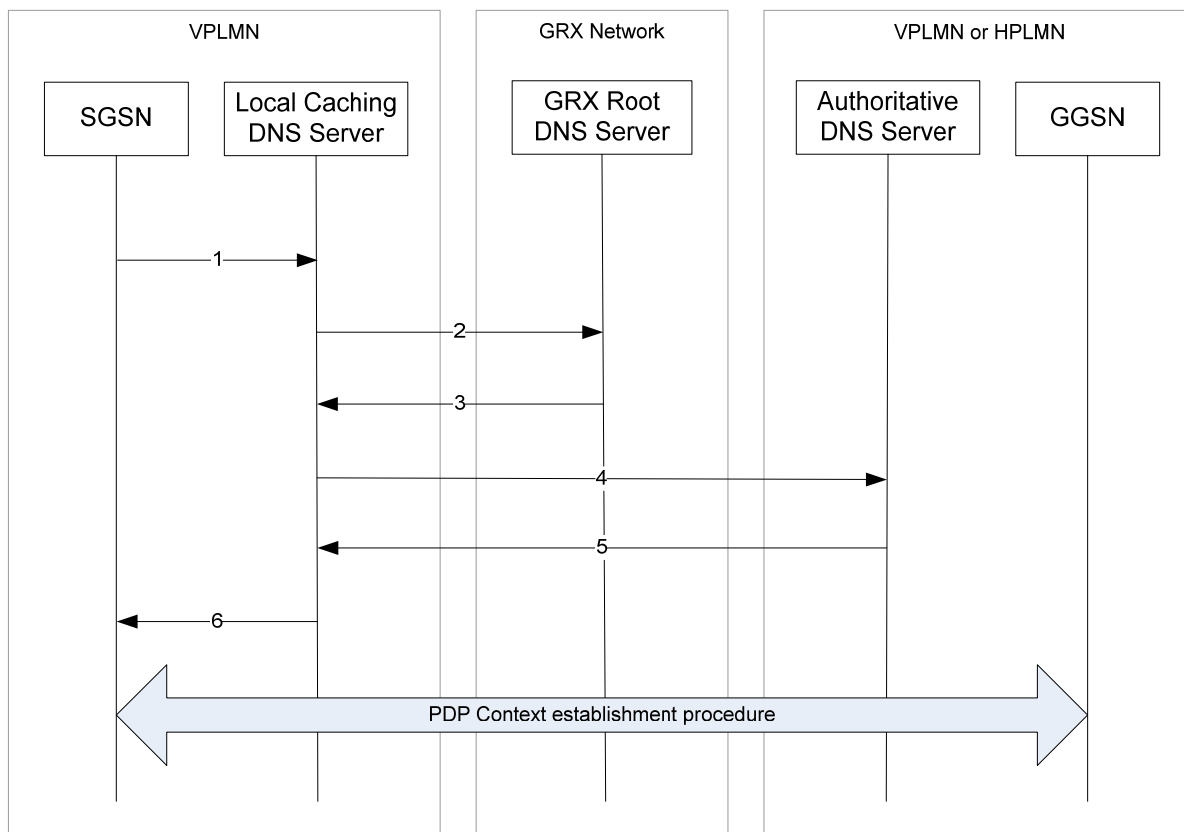


Figure 4: DNS message flow for PDP Context activations

- 1 Upon receiving a "PDP Context Activation" message from the MS, the SGSN checks the APN (if one was provided) against the user subscription record it previously obtained from the HLR when the MS attached, and then sends a recursive DNS Query to the DNS Local Caching DNS server.
- 2 The Local Caching DNS Server checks its local cache for the IP address of the requested FQDN. If it has this, processing skips to step 6. Otherwise, the Local Caching DNS Server checks its local cache for the IP address of the Authoritative DNS Server. If it does not already have this IP address, it then issues an iterative DNS Query to the Root DNS Server otherwise, processing skips to step 4.
- 3 The Root DNS Server replies to the DNS Query received from the Local Caching DNS with the details of the Authoritative DNS Server (for example, the FQDN and/or IP address(es)).
- 4 The Local Caching DNS Server sends an iterative DNS Query to the Authoritative DNS Server (which will reside in the VPLMN, for vGGSN connection, and will reside in the HPLMN for hGGSN connection).
- 5 The Authoritative DNS Server replies to DNS Query received from the Local Caching DNS Server with the IP address of the GGSN.
- 6 The Local Caching DNS Server replies to the DNS Query received from the SGSN (in step 1) with the result obtained from the Authoritative DNS Server. The SGSN then commences GTP tunnel establishment and, all being well, data flow starts.

As can be seen in the above steps, there are less DNS queries for a subscriber using a GGSN in the VPLMN as the Root DNS Server is not interrogated.

Note also that the Local Caching DNS Server could also be the Authoritative DNS Server for the requested FQDN, in which case a final result can be given immediately to the SGSN.

4.2.3 Inter-SGSN handovers for active PDP Contexts

When an MS has one or more PDP Contexts activated and moves to a new Routing Area that is serviced by a new SGSN, the new SGSN needs to connect to the old SGSN in order to download the PDP Context information and any data that is still to be delivered to the MS. It can do this by either using a mapping table which has SGSN addresses against a finite set of Routing Areas, or it can translate the old Routing Area Code (as received from the MS) into a FQDN upon which to resolve to an IP address using DNS.

The former method is most commonly used for intra-PLMN SGSN handovers, and the latter is used for inter-PLMN SGSN handovers. However, both methods can be used for both types of handovers.

The latter of the two aforementioned methods is depicted below for inter- and intra-PLMN SGSN handovers. The FQDN created by the SGSN depends upon whether the SGSN handover is a Routing Area Update, Routing Area Update in a network which has Intra Domain Connection of RAN Nodes to Multiple CN Nodes or is an SRNS Relocation (see 3GPP TS 23.060 [23] section 6.9 for more information).

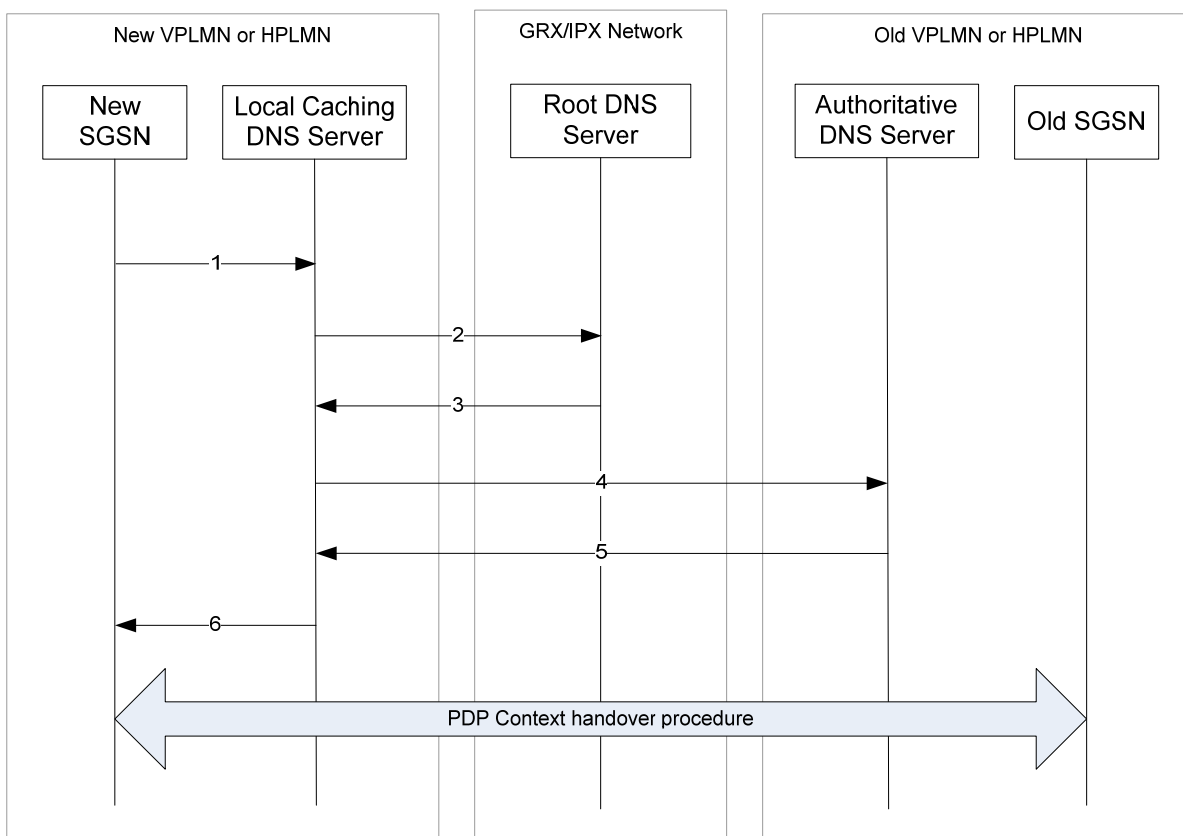


Figure 5: DNS message flow for PDP Context handovers between SGSNs

- 1 The new SGSN creates an FQDN using the old Routing Area Code (and the Network Resource Identifier, if available) or the old RNC ID and then issues a recursive DNS Query to the DNS server address configured in the SGSN (Local Caching DNS server).
- 2 The Local Caching DNS Server checks its local cache for the IP address of the requested FQDN. If it has this, processing skips to step 6. Otherwise, the Local Caching DNS Server checks its local cache for the IP address of the Authoritative DNS

- Server. If it does not already have this IP address, it then issues an iterative DNS Query to the Root DNS Server, otherwise, processing skips to step 4.
- 3 The Root DNS Server replies to the DNS Query received from the Local Caching DNS with the details of the Authoritative DNS Server (for example, the FQDN and/or IP address(es)).
 - 4 The Local Caching DNS Server sends an iterative DNS Query to the Authoritative DNS Server (which will reside in the VPLMN, for inter-PLMN handover, and will reside in the HPLMN for intra-PLMN handover).
 - 5 The Authoritative DNS Server replies to DNS Query received from the Local Caching DNS Server with the IP address of the old SGSN.
 - 6 The Local Caching DNS Server replies to the DNS Query received from the SGSN (in step 1) with the result obtained from the Authoritative DNS Server. The New SGSN then commences handover with the Old SGSN.

As can be seen in the above steps, there are less DNS queries for an intra-PLMN SGSN handover as the Root DNS Server is not interrogated.

Note also that the Local Caching DNS Server could also be the Authoritative DNS Server for the requested FQDN, in which case a final result can be given immediately to the New SGSN.

4.3 Multi-media Messaging Service (MMS)

4.3.1 Introduction

MMS inter-working is where a subscriber of one operator has the ability to send and receive Multimedia Messages (MMs) to and from a subscriber of another operator. Unlike SMS inter-working, the MM is always sent to the user via his "home" service centre. This means that in all MMS inter-working scenarios, the MM is always transferred from the source operator's MMSC to the destination operator's MMSC. Thus, MMS interworking requires use of a standardised inter-MMSC protocol. This protocol is defined as SMTP (defined in IETF RFC 2821[13]) as profiled in the MMS specification 3GPP TS 23.140 [15].

DNS is used in MMS in order for the source MMSC to resolve the destination MMSC/SMTP server. DNS MX Resource Records, as defined in IETF RFC 1035 [2], are required for SMTP based Multimedia Message routing and relaying. It should be noted that GSMA PRD IR.34 [12] recommends that the ".gprs" TLD should be used when utilising the GRX/IPX network as the interworking network between MMSCs. This format of FQDN, including allowed sub-domains, is defined in sub-section 2.3.1 of the present document.

The selection of a DNS tree/hierarchy to use (e.g. Internet or GRX/IPX) ultimately depends on the interconnection network used. The interconnection network used can in turn depend on where the MM is to be sent e.g. Internet for when delivering to an e-mail user, GRX/IPX network for when delivering to another MMS subscriber. Thus, the resolution process may differ depending on whether the MM is addressed to an MSISDN/E.164 number or to an NAI/e-mail address.

There are also different commercial models for MMS inter-working between Operators. These are essentially the "Direct Interconnect" model, where MMs are sent from Operator A to Operator B directly, and the "Indirect Interconnect Model", where MMs are sent from Operator A to an MMS Hub (and the MMS Hub then takes care of delivering the MM to Operator B).

More information on MMS interworking can be found in GSMA PRD IR.52 [9].

4.3.2 MM delivery based on MSISDN for the Direct Interconnect model

The following figure and associated numbered steps describe the direct interconnect only scenario for MMS inter-working of MMs addressed to an MSISDN/E.164 number:

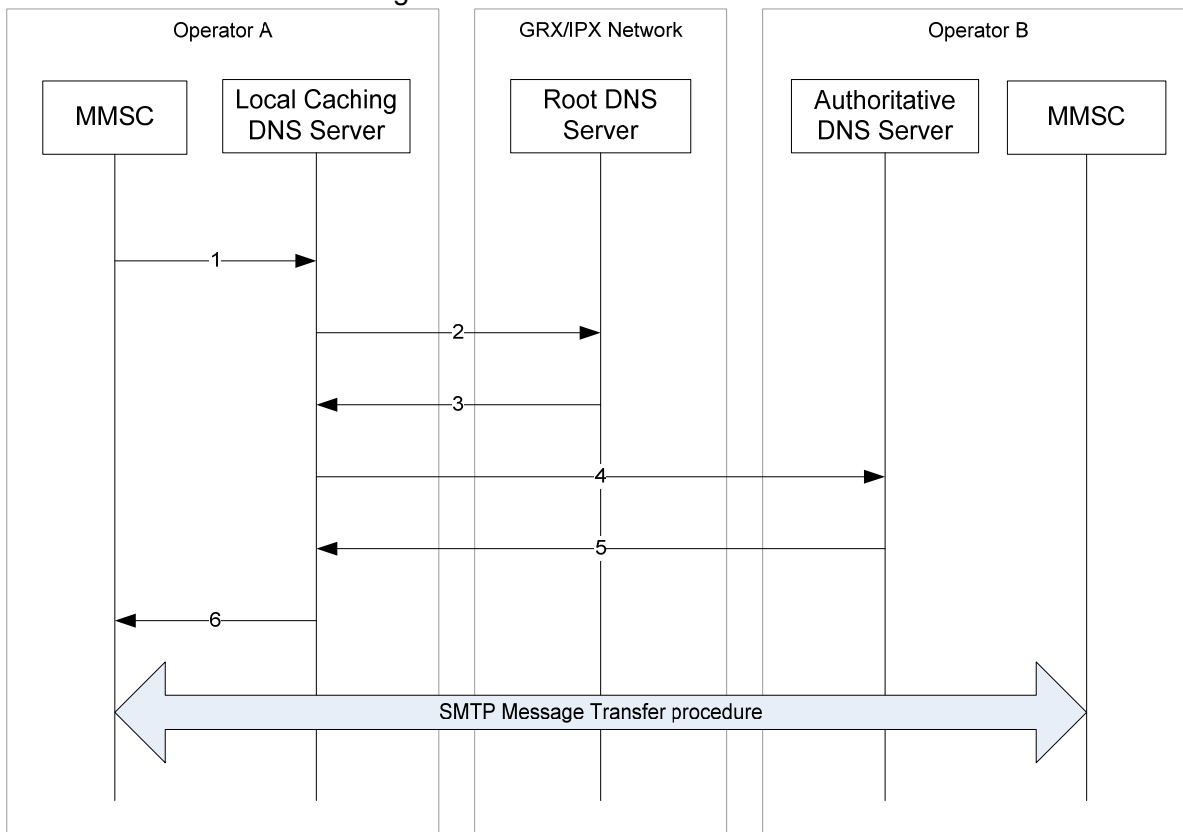


Figure 6: MMS Direct Inter-network Delivery

- 1 Upon receiving a Multimedia Message (MM) from the MS, the MMSC converts the destination MSISDN to an MMS FQDN (commonly of the form "mms.mnc<MNC>.mcc<MCC>.gprs") by using one of the following methods:
 An HLR look-up using e.g. the MAP_SRI_For_SM operation. This returns the IMSI, of which the MNC and MCC are extracted to create the MMS FQDN.
 An ENUM look-up (see section 6 for more details).
 The MMSC then sends a recursive DNS query for the derived FQDN to the Local Caching DNS Server.
- 2 The Local Caching DNS Server checks its local cache for the IP address of the requested FQDN. If it has this, processing skips to step 6. Otherwise, the Local Caching DNS Server checks its local cache for the IP address of the Authoritative DNS Server. If it does not already have this IP address, it then issues an iterative DNS Query to the Root DNS Server, otherwise processing skips to step 4.
- 3 The Root DNS Server replies to the DNS Query received from the Local Caching DNS Server with the details of the Authoritative DNS Server (for example, the FQDN and/or IP address(es)).
- 4 The Local Caching DNS Server sends an iterative DNS Query to the Authoritative DNS Server.

- 5 The Authoritative DNS Server replies to the DNS Query received from the Local Caching DNS Server with the IP address of the MMSC, or, a list of FQDNs and/or IP addresses if the query was for an MX record.
- 6 The Local Caching DNS Server replies to the DNS Query received from the MMSC (in step 1) with the result obtained from the Authoritative DNS Server. The MMSC then commences an SMTP session with Operator B's MMSC to transfer the MM.

Note that the Local Caching DNS Server could also be the Authoritative DNS Server for the requested FQDN, in which case a final result can be given immediately to the MMSC.

4.3.3 MM delivery based on MSISDN for the Indirect Interconnect model

The following figure and associated numbered steps describe the MMS hub model of interconnect for MMS inter-working of MMs addressed to an MSISDN/E.164 number:

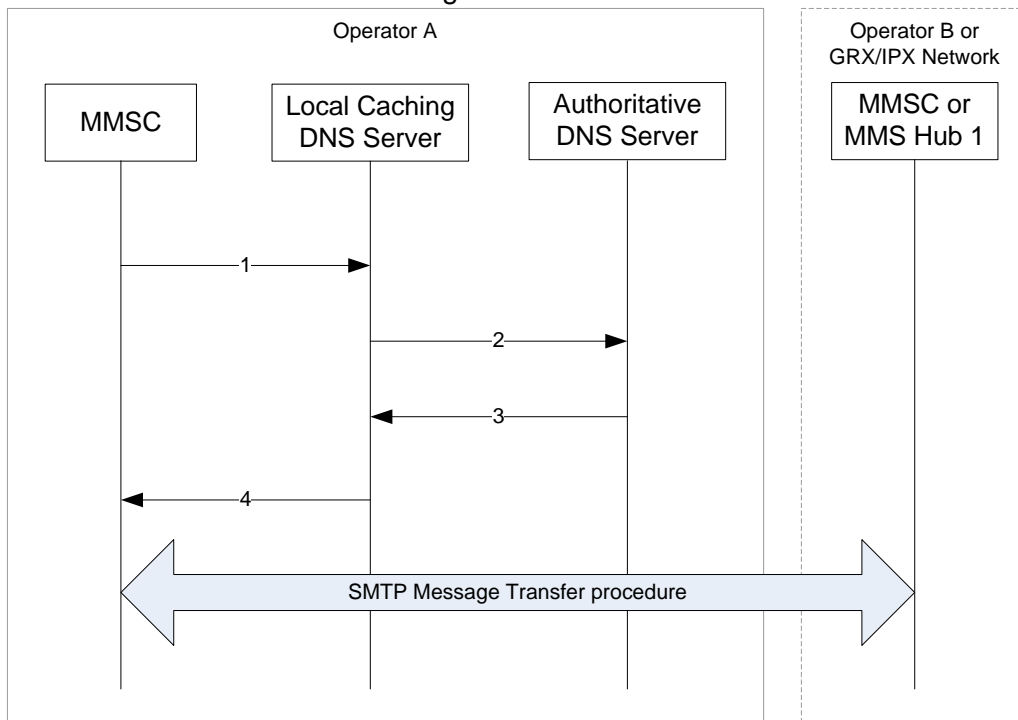


Figure 6a: MMS Inter-operator Delivery

- 1 Upon receiving a Multimedia Message (MM) from the MS, the MMSC converts the destination MSISDN to an MMS FQDN (commonly of the form "mms.mnc<MNC>.mcc<MCC>.gprs") by using one of the following methods:
 An HLR look-up using e.g. the MAP_SRI_For_SM operation. This returns the IMSI, of which the MNC and MCC are extracted to create the MMS FQDN.
 An ENUM look-up (see section 6 for more details).
 The MMSC then sends a recursive DNS query for the derived FQDN to the Local Caching DNS Server.
- 2 The Local Caching DNS Server checks its local cache for the IP address of the requested FQDN. If it has this, processing skips to step 4. Otherwise, the Local Caching DNS Server checks its local cache for the IP address of the Authoritative DNS Server. In this model, the Authoritative DNS Server is always known.
- 3 The Authoritative DNS Server replies to the DNS Query received from the Local Caching DNS Server with either the IP address of the MMS Hub to use or the

destination MMSC, or, a list of FQDNs and/or IP addresses if the query was for an MX record.

- 4 The Local Caching DNS Server replies to the DNS Query received from the MMSC (in step 1) with the result obtained from the Authoritative DNS Server. The MMSC then commences an SMTP session either with Operator B's MMSC, or, to an identified MMS Hub, to transfer the MM.

Note that there is more flexibility in the MMS Hub architecture than shown above, depending on the MMS Hub provider used e.g. some Hub providers offer MSISDN/E.164 number conversion/resolving, some offer complete hosting of the MMSC, and so on. See GSMA PRD IR.52 [9] for more information on MM delivery using an MMS Hub, including a more full description of the flexibility available in the architecture.

Note also that the Local Caching DNS Server could also be the Authoritative DNS Server for the requested FQDN, in which case a final result can be given immediately to the MMSC.

4.3.4 MM delivery based on NAI/e-mail address

For MMs addressed to an NAI/e-mail address (as defined in IETF RFC 2822 [15]), the message flow is the same as in Figure 6 except that the Internet's root DNS servers and authoritative DNS servers are used, possibly with the use of referral DNS servers too.

4.4 WLAN Inter-working

4.4.1 Introduction

Figure 7 shows how local login and roaming login differ; it also demonstrates how Roaming Partners actually connect to each other via inter-operator network. Case 1 is an example of normal local login in the hot spot of Visited PLMN, where the user inserts his username & password and is authenticated in the Visited PLMN. In this case, the RADIUS Roaming Network is not utilised.

Case 2 in Figure 7 refers to a roaming login, where the user inserts his username (with realm) and password in the hot spot of the Visited PLMN and authentication and request is sent by way of a proxy to Home PLMN. The User is then authenticated in the Home PLMN. Necessary RADIUS messages are transferred between RADIUS Roaming Proxies using the IP based Inter-PLMN network, that is, the GRX/IPX.

Figure 7 shows also in principle the difference between the following two authentication methods:

- 1 Web Based Authentication
- 2 SIM Based Authentication

Web Based (that is, using username/password) authentication is considered as an existing first phase solution for the WLAN authentication. However, in the future there will be a target solution utilising EAP solutions, where the Home PLMN HLR is involved.

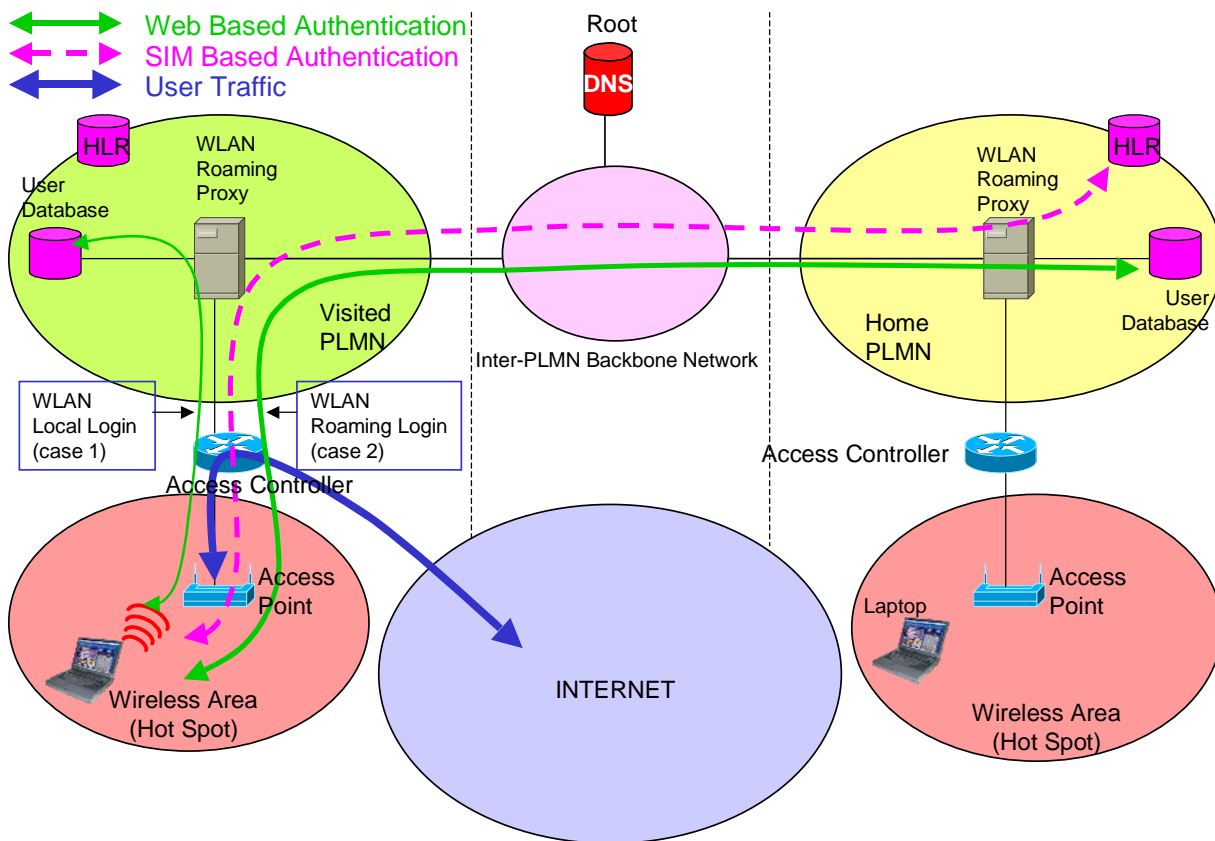


Figure 7: WLAN user authentication mechanism

The GRX/IPX network is used for transporting RADIUS authentication and accounting messages for WLAN roaming services only, WLAN user data is *not* carried over GRX/IPX.

The IP address of the WLAN Roaming Proxy must be reachable via the GRX/IPX. Please note that the first phase of WLAN roaming will not use the GRX/IPX Root DNS at all since the IP addresses of the Home PLMN RADIUS server is statically configured in the Visited PLMNs RADIUS server (the "next hop" list). In fact, RADIUS does not provide for a DNS type solution for realm to AAA entity mapping. The utilising of Root DNS may be required in future WLAN roaming solutions where Diameter instead of RADIUS is used, as Diameter does provide for an optional realm to AAA entity mapping.

More information on WLAN roaming can be found in GSMA PRD IR.61 [10].

4.5 IP Multi-media core network Sub-system (IMS)

4.5.1 Introduction

The IP Multi-media core network Sub-system (IMS) provides a standardised architecture for providing feature rich, multimedia services/applications, such as speech communication, real-time and turn-based gaming, shared online whiteboards etc. IMS services/applications rely on sessions managed by the Session Initiation Protocol (SIP), as defined in IETF RFC 3261 [38], and profiled in 3GPP TS 24.229 [35] (which includes a set of standardised extensions) for use by 3GPP operators.

In order to improve performance/session establishment time, use of explicit IP addresses instead of FQDNs eliminates the need for some DNS lookups and retains compatibility with existing standards. However, using IP addresses instead of FQDNs is more restrictive.

4.5.2.1 Step 1

This is the ENUM related step and is performed only for cases where the service has been addressed to an E.164 number. An IMS call to a user using the format bob@example.com would not require this step. Example of DNS data for a particular SIP URI and its servers can be found in sub-section 4.6.5.6.

4.5.2.2 Step 2

Having obtained the destination domain name the DNS is asked to provide matching SIP Server Location Information. One or more NAPTR records may be retrieved and the calling application examines these records to find the best match based on priorities and the desired SIP protocol variant:

```
mnc001.mcc234.3gppnetwork.org. IN NAPTR 50 100 "s" "SIP+D2U" "" _sip._udp.example.com.  
mnc001.mcc234.3gppnetwork.org. IN NAPTR 90 100 "s" "SIP+D2T" "" _sip._tcp.example.com.  
mnc001.mcc234.3gppnetwork.org. IN NAPTR 90 100 "s" "SIPS+D2T" "" _sips._tcp.example.com.
```

In the above example, "D2U" indicates UDP-based SIP, "D2T" indicates TCP-based SIP, and "SIPS+D2T" indicates UDP-based unencrypted SIP.

The presence of these fields indicates what variations of SIP are supported on a given SIP server.

The "s" flag means the next stage is to look up an "SRV" record

4.5.2.3 Step 3

An example set of SIP server SRV records is as follows:

```
_sip._tcp.example.com. SRV 0 1 5060 sipsevr1.example.com.  
_sip._tcp.example.com. SRV 0 2 5060 sipsevr2.example.com.  
_sip._udp.example.com. SRV 0 1 5060 sipsevr1.example.com.  
_sip._udp.example.com. SRV 0 2 5060 sipsevr2.example.com.  
_sips._tcp.example.com. SRV 0 1 5060 sipsevr3.example.com.  
_sips._tcp.example.com. SRV 0 2 5060 sipsevr4.example.com.
```

For each of the variations of the SIP protocols supported the SRV records describe:

- name of the server;

- which port number SIP uses; and

- where there are multiple servers, the weights & priorities to allow rough load balancing.

The calling network asks the DNS for a SRV record for the host corresponding to the specific service/protocol/domain combination that was returned in Step 2

If there are multiple records with the same service/protocol/domain combination, the caller must sort the records based on which has the lowest priority. If there is more than one record with the same priority, the record with the highest weight is chosen.

From the SRV record get the corresponding server name.

There is potential flexibility in this step for the destination operator to receive the SIP traffic on different servers depending on the desired variation of the SIP protocol – TCP, UDP, encrypted, unencrypted.

4.5.2.4 Step 4

For the server name returned in Step 3, do a standard DNS lookup to find its IP address
This is a normal "A" (address) record lookup

```
sipserv1.example.com.      IN A    101.1.2.3  
sipserv2.example.com.      IN A    101.1.2.4
```

4.5.3 Domain Names used

The domain names used for IMS based services are SIP Server names, however, there are no restrictions in the standards as to what these domain names shall be (other than the normal FQDN rules, as specified in the likes of IETF RFC 1034 [1] and IETF RFC 1035 [2]). However, for service providers interconnecting across the GRX/IPX network, it is recommended to use an MCC/MNC sub domain of ".3gppnetwork.org" as this is supported already on the GRX/IPX DNS and also allows for SIP URIs returned using ENUM on the GRX/IPX as specified in section 5.

It should be noted that right now, more "user friendly" domain names are not yet directly supported on the GRX/IPX DNS. Work on supporting a much wider set of domain names is ongoing.

4.6 Generic Authentication Architecture (GAA)

4.6.1 Introduction

The Generic Authentication Architecture is defined in 3GPP TS 33.220 [19]. It is a standardised mechanism for securely distributing shared keys for later use by applications on the UE.

4.7 Generic Access Network (GAN)

4.7.1 Introduction

The Generic Access Network is defined in 3GPP TS 43.318 [20] and 3GPP TS 44.318 [21]. It provides for using unlicensed radio spectrum for accessing the GSM core network in order to provide normal GSM services including both CS and PS. It was based on the work done by the UMA forum.

4.8 Secure User Plane Location (SUPL)

4.8.1 Introduction

The Secure User Plane Location feature is defined in OMA OMA-AD-SUPL-V1_0-20070615-A [27]. It provides a mechanism for carrying location information between a user's SUPL Enabled Terminal (SET) and SUPL Location Platform (SLP) in a Service Provider's network, in a way that does not rely on modifications to any network interfaces or elements between the SET and SLP. This information can then be used by the Service Provider to calculate the SET's location.

4.9 Enhanced Packet Core (EPC)

4.9.1 Introduction

The Enhanced Packet Core is defined in 3GPP TS 23.401 [28] and 3GPP TS 23.402 [29]. It provides for a new and much more efficient PS core network to support E-UTRAN and serves as part of the Enhanced Packet System (EPS).

It should be noted that EPC used to be known as SAE (Service Architecture Evolution) and E-UTRAN used to be known as LTE (Long Term Evolution) RAN.

4.10 IMS Centralised Services (ICS)

4.10.1 Introduction

The IMS Centralised Services feature is defined in 3GPP TS 23.292 [30]. It enables the provisioning of Supplementary Services and value added services (such as those offered today via CAMEL) to the CS domain from IMS.

4.11 Access Network Discovery Support Function (ANDSF)

4.11.1 Introduction

The Access Network Discovery Support Function (ANDSF) is defined in 3GPP TS 23.402 [29]. It contains data management and control functionality necessary to provide network discovery and selection assistance data according to Service Provider policy. The ANDSF responds to requests from the UE for access network discovery information and may be able to initiate data transfer to the UE, based on network triggers.

5 E.164 NUMBER TRANSLATION (ENUM)

5.1 Introduction

Telephone numbers compliant with E.164 that identify subscribers (known as "MSISDNs" in GSM/UMTS) cannot be used on their own for addressing in IP based networks. The Internet Engineering Task Force have defined a mechanism for converting E.164 numbers to an "IP friendly" address relevant to the service which the user wishes to use. IETF RFC 3761 [3] defines storing E.164 numbers and services related to a particular number using DNS. This mechanism is known as ENUM.

The services which need ENUM are currently MMS and IMS/SIP based services. The definitions in this section take account of both these services and can be extended in the future when new services emerge.

5.2 ENUM FQDN Format

Through translating E.164 numbers into DNS names, the ENUM mechanism can take advantage of existing DNS functionality such as infrastructure, delegation and caching. The algorithm for converting any E.164 number to an ENUM domain consists of the following:

Ensure that the E.164 number is written in its full form, including the country code.

- Example: +44-7700-900123

Remove all non-digit characters with the exception of the leading '+'.

- Example: +447700900123

Remove all characters with the exception of the digits.

- Example: 447700900123

Put dots (".") between each digit.

- Example: 4.4.7.7.0.0.9.0.0.1.2.3

Reverse the order of the digits.

- Example: 3.2.1.0.0.9.0.0.7.7.4.4

Append a top level domain name to the end (example: ".e164.arpa" for Public ENUM, or "e164enum.net" for Carrier ENUM on the GRX/IPX).

- Example: 3.2.1.0.0.9.0.0.7.7.4.4.e164enum.net

The final answer identifies the destination operator for the given E.164 number.

5.3 ENUM Tiers

To ensure proper distribution and scalability of the DNS structures, ENUM uses a tier system. There are commonly 3 tiers that consist of the following:

Tier 0 – Global level (e.g. Root DNS server)

- Authoritative for the top level domain ("e164.arpa").
- Under this domain are pointers to the Tier 1 authoritative servers.

Tier 1 – Country level (CC)

- Authoritative for country code (e.g. "4.4.e164.arpa" for country code +44)
- Under this domain are pointers to the Tier 2 authoritative servers.

Tier 2 – Operator level (NDC)

- Authoritative for National Destination Codes ("0.0.7.7.4.4.e164.arpa").
- Under this domain are the individual Subscriber Numbers each with one or more NAPTR records.

Note: ENUM Tiers can be combined or even expanded, that is further Tiers may be prevalent in some networks and/or countries for number portability realisations (see sub clause 4.6.12 for more information on Number Portability).

If the E.164 number is in a national format, it must first be converted to an international format. This may also apply to short codes; however, short code support in ENUM is currently not specified.

Services that are related to particular E.164 numbers are stored and described in NAPTR records. NAPTR records are defined in IETF RFC 3403 [6] and can be used for mechanisms other than ENUM. However, in the ENUM context, NAPTR records provide a powerful mechanism of matching against E.164 numbers using regular expressions and outputting one or more URIs as a result. Outputted URIs then point to those services that belong to a resolved E.164 number. For example, returned SIP URIs can be used in IMS inter working.

5.4 Types of ENUM

There are two types of ENUM: Public ENUM and Private ENUM. There are a number of different terms used in the Telecomms 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 DNS infrastructure on the Internet
- Data can be read by anyone
- Uses the "e164.arpa" top level domain
- Intention is to provide an on-line directory service for end users
- Data populated by end users who choose to opt-in
- Data 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 on the GRX/IPX
- Intention is to provide a routing enabling technology that is transparent to the end user
- Not reachable by end users or Internet users
- Uses the "e164enum.net" top level domain to avoid any detrimental effects caused by unintended leakage to the Internet caused by mis-configuration in an operator's network
- Data can be read only by those connected to the GRX/IPX (examples: operators, MMS hub providers)
- Data populated by operators
- Data must be kept up-to-date by the owning operator otherwise calls and services will fail.
- Does not contain "personal" data, only data required for call and service routing

5.5 Technical Requirements for Interworking

The implementation of Carrier ENUM on the GRX/IPX is currently in the process of being rolled out. The following sections specify the agreed implementation details for ENUM on the GRX/IPX network so that it is fully interoperable between all network entities.

5.5.1 Domain name

The domain name "e164enum.net" shall be used for Carrier ENUM on the GRX/IPX.

This domain name has been chosen for a number of 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 and standards groups
- Has an indication of its purpose i.e. 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.*

5.5.2 URI formats

5.5.2.1 Introduction

The domain name part of URIs returned in NAPTRs shall be in the format detailed in section 2.3 of the present document, to enable routing through the GRX/IPX network using the current GRX/IPX DNS.

5.5.2.2 IMS URI format

The IMS ENUM URI domain 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 allocated to the Service Provider.

"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 in the future with sub domains allocated 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 only for IMS subscribers, the SIP URI parameter "user=phone" could be excluded so long as their HSS knows that the user part contains an E.164 number with the leading "+". For operators that provision the SIP URI for both IMS and non-IMS subscribers, they should always include the SIP URI parameter "user=phone" in the SIP URI.

The following examples are all acceptable 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@imsnetwork.mnc001.mcc234.3gppnetwork.org  
sip:+447700900123@mnc001.mcc234.3gppnetwork.org;user=phone  
sip:+447700900123@ims.mnc001.mcc234.3gppnetwork.org;user=phone  
sip:+447700900123@imsnetwork.mnc001.mcc234.3gppnetwork.org;user=phone
```

5.5.2.3 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 Service Provider.

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, 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/TYP=PLMN@mms.mnc001.mcc234.gprs
```

5.5.3 When to provision numbers in the ENUM Database

Once an operator begins to use ENUM for a service they have options on how to provision information in the ENUM database. They could either:

- Provision just the E.164 numbers of customers who have taken up that service

- Provision all the E.164 numbers belonging to that operator, that is, all those numbers that can be allocated to customers whether or not they have taken up that service

At the time of writing it is expected that the two main services using ENUM will be IMS/SIP based services and MMS although the timescales for these will probably be different. Most operators will at some point be using ENUM for one service and not the other.

For operators who offer MMS it is recommended that, where possible, all of that operator's subscribers should be provisioned with an MMS URI. This allows for all MMS interconnecting operators to utilise ENUM instead of MAP in order to determine the destination operator and thereby reduce load on that operator's HLR.

For operators who offer IMS based services it is recommended that, where possible, all of that operator's subscribers should be provisioned with a SIP URI. However, operators should be warned that if a subscriber who does not have an HSS entry is provisioned with a SIP URI without the SIP URI parameter "user=phone", this results in SIP sessions/calls failing indefinitely (as the I-CSCF handling the incoming session will not be able to assign an S-CSCF and to attempt request routing using the E.164 number derived from the SIP URI), as opposed to the session/call being alternatively delivered via the PSTN by the originating operator (which is defined in 3GPP IMS standards to occur only upon an ENUM look-up failure by the originating network).

It is recommended that an operator should always include the SIP URI parameter "user=phone" in the SIP URI and configure and set the I-CSCF to support the "local configuration option" to attempt request routing using the E.164 number derived from the SIP URI as is 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.

It is accepted that the optimal approach in any country depends on the way Number Portability has been implemented. The overall recommendation here is that neither approach is *mandatory* and operators are free to choose whichever approach they wish.

5.5.4 Application of interconnection policy

In some instances, it is possible to resolve an E.164 number to a URI, even though there is no interconnection agreement (commercial or technical) with the target operator for the identified service. This may happen to an originating operator 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 operator, but for a different service e.g. 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 section 4.6.6.3.

- Automatic derivation of the URI from the E.164 number e.g. MAP_SRI_For_SM look-up (also known as an "IMSI look-up"), back-end connection to a number range database (e.g. MNP database), static look-up table of E.164 number block data assignment. For examples of architectures, see sub-section 4.6.6.3.

In such a case, extra analysis needs to be performed by the originating operator on the derived URI to check local policies on interconnection with regards to 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 in routing the service.

Policy checking can take place in the service node e.g. MMSC, S-CSCF, AS, or it can take place in the local DNS caching server that is taking care of the ENUM resolution. In both cases, there are commercially available solutions for both.

5.5.5 ENUMservice field

5.5.5.1 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 5.5.6 for an example. The following are recommended values to be used for different services defined by 3GPP.

5.5.5.2 IMS

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

5.5.5.3 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].

5.5.5.4 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 registration process defined in IETF RFC 3761 [3]).

5.5.6 Example Data-fill

The following shows an example of the E.164 number +447700900123 that supports both IMS and MMS, in a Service Provider'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@mnc001.mcc234.3gppnetwork.org;user=phone!" .  
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 rest of the NAPTR is a Regular Expression. The querying application substitutes the relevant fields into the regular expression to get the result which is a SIP URI.

5.6 Structure and Delegation Model

5.6.1 Introduction

There are three principles which any Carrier ENUM model should support. First, there should be a competitive environment, where more than one vendor or service bureau offers Carrier ENUM functionality. Second, equal accessibility is required, such that the ENUM data fill is available to all entities who need it. Third, accuracy is critical, which means that there exist authoritative databases with the required information. Note that a competitive environment is dependent upon the open connectivity and accessibility of the ENUM data.

The following details the GSMA recommended structure and delegation model of Carrier ENUM on the GRX/IPX network. An alternative model is described in Annex B. Analysis on the appropriateness and viability of each model (including how they can both co-exist) is provided in IN.12 [31].

In the following architecture model, a strict hierarchy is followed. DNS is designed to have a hierarchical structure allowing different organisations to have control of different parts of the overall structure. E.164 numbers also have a hierarchical structure and this can be mapped onto the DNS structure on the GRX/IPX network.

When one country has solved the provisioning of their ENUM Tier-1 and in certain cases service providers have established their Tier-2 information, all service providers are able to use the data for interworking scenarios, if agreements and all needed firewall openings are done.

5.6.2 Architecture

The architecture for this model is depicted in the diagram below:

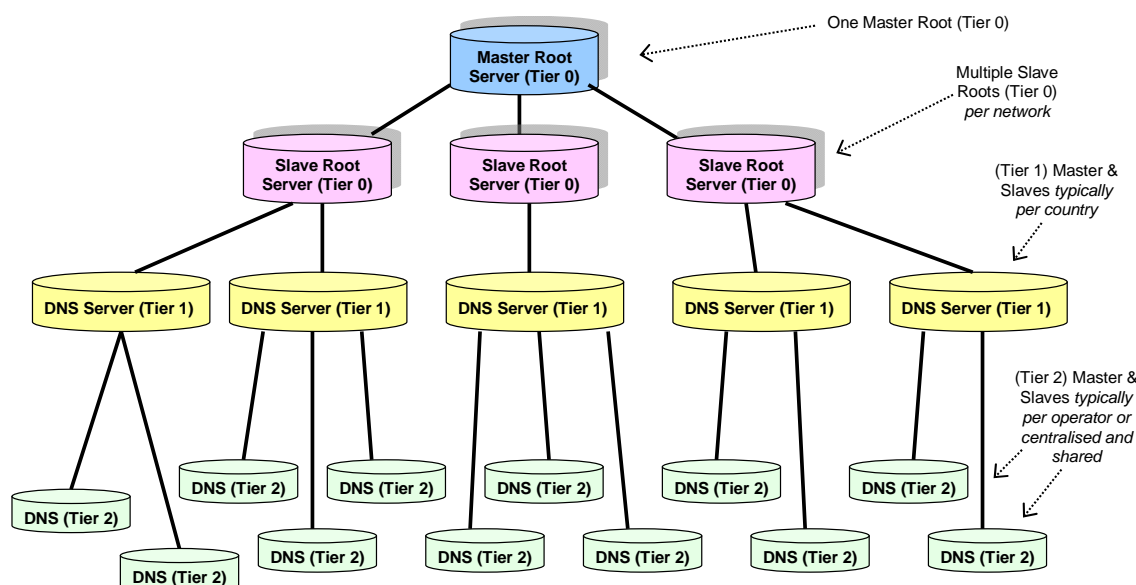


Figure 9: ENUM DNS hierarchy

It should be noted that what is represented in the above figure are logical entities and thus one or more of those logical entities can be offered by one physical server.

Tier-0: Delegates E.164 numbers for a specific country code to a country-defined Tier-1 server. "Where can I get information about E.164 numbers for a given country code?". This Tier-0 will be handled by some authority in GSMA. It could be the same server provider who offers the Root DNS database in GRX/IPX environment, or it could be another provider altogether.

Tier-1: Delegates E.164 numbers for a particular NDC to a carrier-defined Tier-2 server. "Where can I get information about a particular E.164 number or block of numbers?" Tier-1 is basically country level i.e. every single country needs to have their own ENUM Tier-1 server.

The ENUM Tier-1 server provider can be country regulator, one operator in a country, or a designated third party, who has access to the GRX/IPX network. The ENUM Tier-1 server could be shared between multiple Service Providers. In some instances the ENUM Tier-1 server provider can even be the same provider who provides the ENUM Tier-0 server.

Tier-2: Returns NAPTR records for an E.164 number. "What services can this E.164 number support and what are the URIs to be able to contact it?". Tier-2 is basically operator level.

The ENUM Tier-2 servers of operators under a country code could be combined with the ENUM Tier-1 server. Such a server could be "owned" by one Service Provider or shared between multiple Service Providers. Typically the ENUM Tier-2 server providers are either operators themselves or the same providers who offer Tier-0 or Tier-1 servers.

It is also possible to run mixed mode, i.e. where part of the delegations are done in Tier-1 (e.g. centralized (M)NP numbers), and rest is done in Tier-2.

In practice there are many considerations relating to DNS delegation. Who has control of particular servers and number ranges is a matter of concern to telecomm carriers, especially in countries where numbers are portable between mobile and fixed carriers 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.

This document does not attempt to describe arrangements for DNS & ENUM delegation, control and administration. The scope is restricted to describing technical details.

5.6.3 Example resolution

The following depicts an example ENUM resolution:

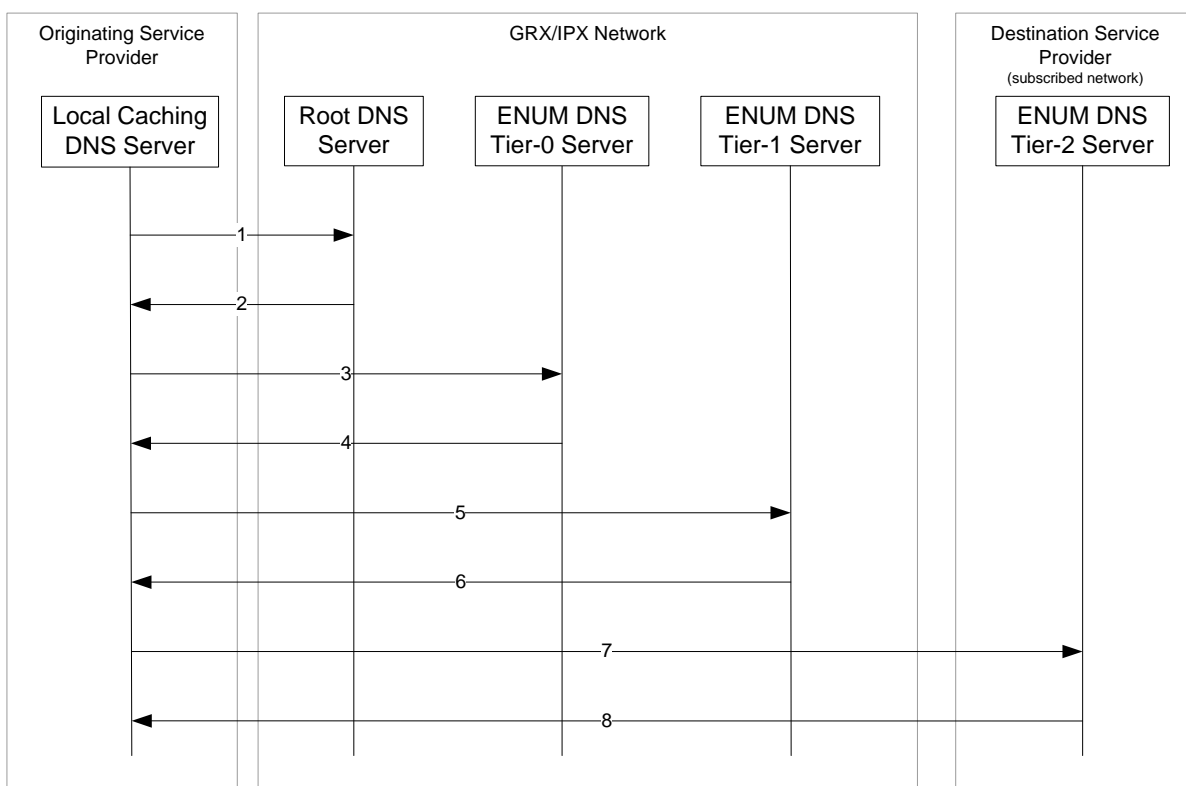


Figure 10: Example ENUM resolution for an IMS session establishment

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

- 1 Service Provider's Local Caching DNS Server sends the DNS query to the Root DNS Server (which is essentially a DNS server that is authoritative for "e164enum.net").
- 2 Root DNS Server replies with the NS record for the ENUM DNS Tier-0 Server.
- 3 Service Provider re-sends the DNS query, but to the ENUM DNS Tier-0 Server.
- 4 ENUM DNS Tier-0 Server replies with the NS record for the ENUM DNS Tier-1 Server.
- 5 Service Provider re-sends the DNS query, but to the ENUM DNS Tier-1 Server.
- 6 ENUM DNS Tier-1 Server replies with the NS record for the ENUM DNS Tier-2 Server.
- 7 Service Provider re-sends the DNS query, but to the ENUM DNS Tier-2 Server.

- 8 ENUM DNS Tier-2 Server replies with a list of URIs/URLs associated with the given E.164 number in NAPTR records, or an error of NXDOMAIN e.g. if the subscriber does not exist or if the Destination Service Provider's optional policy check has decreed that there is no inter-working agreement with the Originating Service Provider.

Note 1: As per normal DNS procedures, each reply an Service Provider receives is cached for a certain amount of time, therefore, negating the need of every message shown always having to be sent.

Note 2: Each ENUM DNS Tier Server may be combined e.g. combined Tier-1 and Tier2.

Note 3: The Originating Service Provider apply an optional policy check upon receiving any response.

5.6.4 Access to ENUM servers

It is assumed that all Service Providers connected to the GRX/IPX network have access to all ENUM servers at all Tiers, and such servers service all queries sent to them by Service Providers. If any servers require commercial agreements and/or charge for access, then this will seriously hamper the ability for Service Providers to resolve queries and may lead to adverse resolution times due to DNS query timeouts.

5.7 Solving Number Portability in ENUM

5.7.1 Introduction

Many countries now mandate that when a subscriber leaves an operator and goes to another that they be able to take their number with them. This is known as "Number Portability". In some countries Number Portability applies only to mobile operators ("Mobile Number Portability") however, more countries are now mandating that this apply also to both fixed line and mobile operators.

Number Portability applies only at the country level; there are currently no portability requirements between networks of different countries, only networks of the same country.

Number Portability implementation differs from country to country and there is no single solution that suits all countries. However, implementations can be categorised as those that use a central database (be it centrally located, or copies of it distributed to Service Providers) and those who do not. The following four sub-clauses describe how Number Portability can be implemented by countries in either of these categories, and concentrates on the Single Root Model architecture (see sub-section 4.6.6.2).

For the "Multiple Root Model", the implications on tiers at, and above, Tier-1 are non-existent, and should therefore be ignored. The ENUM Service Provider takes care of all portability requirements at such Tier levels. Further impacts of the Multiple Root Model architecture are FFS in a future version of the present document.

5.7.2 Option 1 – Central authoritative database

5.7.2.1 Description

This option consists of 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.

5.7.2.2 Example Configuration

If the subscriber whose E.164 number is +44-7700-900123 is a subscriber of Service Provider 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 then moved/ported over to Service Provider 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!" .
```

5.7.2.3 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 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.

This option does have the advantage though that all subscriber numbers are stored centrally and so can be centrally controlled and administered, possibly by one O&M 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.

5.7.2.4 Suitability

This option is possibly more suited to countries where their MNPs are already realised using a central (M)NP database.

5.7.3 Option 2 – Change of domain name in URIs/URLs in Tier-2

5.7.3.1 Description

This option is similar to the previous one in that it 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 separate.

5.7.3.2 Example

If the subscriber whose E.164 number is +44-7700-900123 is a subscriber of Service Provider 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 Service Provider 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 Service Provider 2 in the UK, then this SIP URI would be modified in Service Provider 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!" .
```

5.7.3.3 *Advantages and Disadvantages*

The main disadvantage of this option is that *ALL* network operators within the MNP group need to have launched their ENUM DNS server. Also, if MNP groups are extended (example: to include fixed line portability), any new operators (example: fixed line only operators) will have to launch their own ENUM DNS server before any porting to/from the newly added NDCs can be performed.

Another disadvantage 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 relating to services that may not be offered by the number range owning network. For example, if Service Provider 2 rolled-out an IP based service (that uses ENUM) before Service Provider 1, then Service Provider 1 would have to provision in their Tier-2 DNS all the ENUM records for those subscribers who have ported to Service Provider 2 with the new URI(s) and/or URL(s). Service Provider 1 may also not be able to do this in a time period that is satisfactory to Service Provider 2's launch of the new service.

5.7.3.4 *Suitability*

This option is suited to countries where their MNP is not realised using a central MNP database.

5.7.4 **Option 3 – Redirection at Tier 2**

5.7.4.1 *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.

Such functionality could also be realised using non-terminal NAPTR records. Non-Terminal NAPTR records have been possible since the very first specification of NAPTR records in IETF RFC 2915 [16] (which is now rendered obsolete by IETF RFC 3401 [4], IETF RFC 3402 [5], IETF RFC 3403 [6] and IETF RFC 3404 [7]). However, support for non-terminal NAPTR records in real world implementations of ENUM resolvers is not always present; some support only one NAPTR record in a single resolution procedure, some don't even support them at all! Therefore, the use of NS records instead of non-terminal NAPTR records is recommended.

Note: The option of using NS records and whether or not there are any issues with authority is FFS.

In order to reduce the potential number of DNS look-ups, it is recommended that the FQDN of the ported to DNS server consist of a domain which may already be cached by the DNS Resolver due to similar previous look-ups. This can be realised by always using the same

FQDN for all subscribers ported to one network and by setting a large TTL for such a domain name (in the example below, this would be the FQDN "dns1.mnc002.mcc234.e164enum.net").

5.7.4.2 Example

If the subscriber whose E.164 number is +44-7700-900123 is a subscriber of Service Provider 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 Service Provider 2 in the UK, then the ENUM record stored in Service Provider 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 Service Provider 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 already "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 said DNS Server's FQDN's TTL (which is achievable as today operators change the IP addresses of their DNS servers very infrequently). So in the common case, this solution will involve one extra DNS look-up, and in the worst case involve two extra DNS look-ups.

5.7.4.3 Advantages and Disadvantages

As with Option 2, a disadvantage of this option is that *ALL* network operators within the MNP group need to have launched their ENUM DNS server. Also, if MNP groups are extended (example: to include fixed line portability), any new operators (example: fixed line only operators) will have to launch their own ENUM DNS server before any porting to/from the newly added NDCs can be performed.

Another disadvantage 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 2, the update is only minor, only has to be done once (or at least, only when the subscriber changes/ports networks) and encompasses *all* services relating to ENUM; whether they are supported by the number range owning network or not!

An explicit disadvantage over option 2 though is that the DNS Resolver may have to perform either one or two additional DNS look-ups to resolve the new FQDN returned. As stated above, the exact number of additional look-ups depends on the cache of the DNS Resolver.

An advantage of using NS records for this solution as opposed to using non-terminal NAPTR records is that calls to the ported-in subscriber originating from that same, ported-to

network operator, can be resolved much more quickly as the first ENUM/DNS interrogated will (assuming correct configuration in the local DNS) be the one that is actually authoritative for the ported-in subscriber's number.

5.7.4.4 Suitability

As with Option 2, this option is more suited to countries where their MNPs are not realised using a central MNP database.

5.7.5 Option 4 – Central re-direction database

5.7.5.1 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 as specified in Option 3 (see section 5.3.1 for more detail). This means that all URIs and/or URLs for subscribers are located and managed by the actual subscribed network of each number, rather than the number range owning network of each number.

5.7.5.2 Example

If the subscriber whose E.164 number is +44-7700-900123, and is also a subscriber of Service Provider 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 Service Provider 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 moved over to Service Provider 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, Service Provider 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!" .
```

More so than in Option 3, in this option the DNS resolver will more than likely already "know" the IP address for the DNS server "dns1.mnc001.mcc234.3gppnetwork.org" or "dns1.mnc002.mcc234.3gppnetwork.org" due to previous look-ups. At the very least, it will know the authoritative server for the domain "e164enum.net" from the current set of look-ups! This can be controlled further by increasing the DNS Server's FQDN's TTL (which is achievable as today operators change the IP addresses of their DNS servers very infrequently). So in the common case, this solution will involve one extra DNS look-up exactly like that which occurs in a "normal" Tier-1/Tier-2 architecture within a country, and in the worst case involve two extra DNS look-ups (but the chances of the occurrence of the second DNS look-up in this option are less than the chance of the occurrence of the second DNS look-up in Option 3).

5.7.5.3 *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, only the Tier-1.

An explicit disadvantage over option 2 though is that the DNS Resolver may have to perform either one additional DNS look-up to resolve the new FQDN returned. As stated above, the exact number of additional look-ups depends on the cache of the DNS Resolver.

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.

5.7.5.4 *Suitability*

This option is possibly more suited to countries where their MNP is already realised using a central MNP database.

6 PROCESSES & PROCEDURES RELATING TO DNS

6.1 Introduction

This section describes the processes and procedures relating to DNS that apply to Service Providers and GRX/IPX Providers.

6.2 Procedures Relating to Domain Names

6.2.1 Domains and their Allocation

The domain names for use by Service Providers on the GRX/IPX network are the following:

- .gprs
- .3gppnetwork.org
- .e164enum.net

Only the sub-domains listed in section 2.3.3 for each of the above domains should be used.

The domain name ".e164enum.net" is used only for Carrier ENUM on the GRX/IPX; see section 5 for more information.

The domain names for use by GRX/IPX Providers on the GRX/IPX are the same as those above, when a GRX/IPX Provider is hosting services on behalf of a Service Provider. For all other services and also for GRX/IPX network equipment (e.g. routers, MMS Hubs, etc), use of the ".grx" domain name is commonly used, with a sub-domain that uniquely identifies the GRX/IPX Provider. These sub domains are agreed amongst other GRX/IPX Providers in order to guarantee uniqueness.

7 ANNEX A: SAMPLE BIND DNS CONFIGURATION FOR GPRS

7.1 Introduction

All sample configurations of this annex are in valid syntactical format for the ISC BIND DNS server software. However, the samples are not from actual DNS configuration and contain only example information, including sample IP addresses which are not valid. They are provided for illustration purposes only. It is therefore highly recommended NOT to use these samples in live networks! The GSM Association takes no responsibility of the usage of these configurations in any operators DNS servers and/or live networks.

7.2 The "named.conf" file

The "named.conf" file has configuration information for BIND software. Following is only the necessary configuration to get DNS running. There are many more options that may also be useful, but which are not shown here, simply for making the examples as simple as possible.

7.2.1 The "named.conf" file for a PLMN Master Nameserver

```
options {
    directory "/var/named";
}; // where the files reside

zone "." in {
    type hint;
    file "gprs.hint";
}; // gprs root servers

zone "0.0.127.in-addr.arpa" in {
    type master;
    notify no;
    file "master/0.0.127.in-addr.arpa";
}; // only contains information about localhost.

/*
 * PLMN domain information
 */

zone "mnc091.mcc244.gprs" in {
    type master;
    file "master/mnc091.mcc244.gprs";
};

zone "sonera.fi.gprs" in {
    type master;
    file "master/sonera.fi.gprs";
}; // human readable operator id

zone "168.192.in-addr.arpa" in {
    type master;
    file "master/168.192.in-addr.arpa";
};
```

7.2.2 The "named.conf" file for a PLMN slave Nameserver

```

options {
    directory "/var/named";
}; // where the files reside

zone "." in {
    type hint;
    file "gprs.hint";
}; // gprs root servers

zone "0.0.127.in-addr.arpa" in {
    type master;
    notify no;
    file "master/0.0.127.in-addr.arpa";
}; // only contains information about localhost.

/*
 * PLMN domain information
 */

zone "mnc091.mcc244.gprs" in {
    type slave;
    file "slave/mnc091.mcc244.gprs";
    masters {192.168.1.2;} // address of master nameserver
};

zone "sonera.fi.gprs" in {
    type master;
    file "slave/sonera.fi.gprs";
    masters {192.168.1.2;} // address of master nameserver
}; // human readable operator id;

zone "168.192.in-addr.arpa" in {
    type slave;
    file "slave/168.192.in-addr.arpa";
    masters {192.168.1.2;} // address of master nameserver
};
  
```

7.3 Zone Configuration Files

Recommended values for SOA records are as specified in ripe-203.

7.3.1 The "gprs.hint" file

This file contains ".gprs" root nameservers needed to initialise cache of ".gprs" nameservers. Note that the "." character is indeed significant.

.	518400	IN	NS	dns0.root.gprs.
	dns0.root.gprs.	IN	A	172.22.1.5
.	518400	IN	NS	dns1.root.gprs.
	dns1.root.gprs.	IN	A	10.254.243.7
.	518400	IN	NS	dns2.root.gprs.
	dns2.root.gprs.	IN	A	192.168.17.232

7.3.2 The "0.0.127.in-addr.arpa" file

This file contains only information about localhost i.e. 127.0.0.1

```
$TTL 172800
@    IN      SOA      localhost.. hostmaster.localhost. (
      2000030701 ; serial (YYYYMMDDvv)
      86400      ; refresh (24 hours)
      7200       ; retry (2 hours)
      3600000    ; expire (1000 hours)
      172800 )   ; minimum time to live (2 days)
1    IN      PTR     localhost.
```

7.3.3 PLMN zone files

PLMN may configure both mnc.mcc.gprs and operaror.cc.gprs type domains that will share exactly the same host information. In addition, early versions of GTPv0 did not have leading zeroes to make mnc code always 3 digits long. In order to minimise both configuration work and possible errors, zone files may include a common hosts configuration.

7.3.3.1 The "mnc091.mcc244.gprs" file

```
$TTL 172800
@    IN      SOA      mnc091.mcc244.gprs. hostmaster.mnc091.mcc244.gprs. (
      2000030701 ; serial (YYYYMMDDvv)
      86000      ; refresh (24 hours)
      7200       ; retry (2 hours)
      3600000    ; expire (1000 hours)
      172800 )   ; minimum time to live (2 days)
      IN      NS      dns0
      IN      NS      dns1
$INCLUDE master/hosts
```

7.3.3.2 The "sonera.fi.gprs" file

```
$TTL 172800
@    IN      SOA      sonera.fi.gprs. hostmaster.sonera.fi.gprs. (
      2000030701 ; serial (YYYYMMDDvv)
      86400      ; refresh (24 hours)
      7200       ; retry (2 hours)
      3600000    ; expire (1000 hours)
      172800 )   ; minimum time to live (2 days)
      IN      NS      dns0
      IN      NS      dns1
$INCLUDE master/hosts
```

7.3.4 The "hosts" file

This file contains IP address records for all hosts in the PLMN. The origin changes depending on which file includes the contents i.e. after the names not ending at dot, the current domain name is appended automatically.

Load balancing may be performed configuring same access point with several IP addresses that actually are on different GGSNs. In this case, addresses are used in round-robin fashion. However, DNS information is cached and a new query is performed only when the

TTL (time-to-live) has expired. Therefore TTL of 0 seconds is configured for load balanced access points.

```
dns0                IN      A      192.168.1.2
dns1                IN      A      192.168.2.2
;
;   router
helsinki-rtr-1-fe-0-0    IN      A      192.168.1.254
helsinki- rtr-1-fe-0-1    IN      A      192.168.2.254
helsinki- rtr-1-fe-0-2    IN      A      192.168.3.254
helsinki- rtr-1-s-1-0    IN      A      172.22.5.6
;
;   access point
ibm.com              IN      A      192.168.1.5
;
;   load balanced access point
compaq.com 0          IN      A      192.168.1.5
              0          IN      A      192.168.2.5
;
;   service access point
internet             IN      A      192.168.2.2
;
;   GGSN
helsinki-ggsn-15     IN      A      192.168.1.5
helsinki- ggsn-25     IN      A      192.168.2.5
helsinki- ggsn-22     IN      A      192.168.2.2
;
;   SGSN
helsinki-sgsn-1      IN      A      192.168.3.3
;   SGSN with RAI
racF1.lac12EF        IN      A      192.168.3.3
```

7.3.5 The "168.192.in-addr.arpa" file

There may be several PTR records so that each name associated with an address may have reverse mapping also. Note that IP address is reversed in in-addr.arpa domain i.e. 192.168.1.254 will be 254.1.168.192.in-addr.arpa.

```

$TTL 172800
@   IN      SOA   dns0.sonera.fi.gprs. hostmaster.sonera.fi.gprs. (
      2000030701 ; serial (YYYYMMDDvv)
      86400      ; refresh (24 hours)
      7200       ; retry (2 hours)
      3600000    ; expire (1000 hours)
      172800    ) ; minimum time to live (2 days)

      IN      NS   dns0.sonera.fi.gprs.
      IN      NS   dns1.sonera.fi.gprs.

5.1   IN      PTR   ibm.com.sonera.fi.gprs.
      PTR   ibm.com.mnc091.mcc244.gprs.
      PTR   compaq.com.sonera.fi.gprs.
      PTR   compaq.com.mnc091.mcc244.gprs.
      PTR   helsinki-ggsn-15.sonera.fi.gprs.
      PTR   helsinki-ggsn-15.mnc091.mcc244.gprs.

254.1 IN      PTR   helsinki-rtr-1-fe-0-0.sonera.fi.gprs.
      PTR   helsinki-rtr-1-fe-0-0.mnc091.mcc244.gprs.

2.2   IN      PTR   internet.sonera.fi.gprs.
      PTR   internet.mnc091.mcc244.gprs.
      PTR   helsinki-ggsn-2.sonera.fi.gprs.
      PTR   helsinki-ggsn-2.mnc091.mcc244.gprs.

5.2   IN      PTR   compaq.com.sonera.fi.gprs.
      PTR   compaq.com.mnc091.mcc244.gprs.
      PTR   helsinki-ggsn-25.sonera.fi.gprs.
      PTR   helsinki-ggsn-25.mnc091.mcc244.gprs.

254.2 IN      PTR   helsinki-rtr-1-fe-0-1.sonera.fi.gprs.
      PTR   helsinki-rtr-1-fe-0-1.mnc091.mcc244.gprs.

3.3   IN      PTR   helsinki-sgsn-1-fe.sonera.fi.gprs.
      PTR   helsinki-sgsn-1-fe.mnc091.mcc244.gprs.
      PTR   racF1.lac12EF.sonera.fi.gprs.
      PTR   racF1.lac12EF.mnc091.mcc244.gprs.

254.3 IN      PTR   helsinki-rtr-1-fe-0-2.sonera.fi.gprs.
      PTR   helsinki-rtr-1-fe-0-2.mnc091.mcc244.gprs.
  
```

8 ANNEX B: ALTERNATIVE ENUM ARCHITECTURE: THE MULTIPLE ROOT MODEL

8.1 Introduction

This Annex describes an alternative to the preferred ENUM architecture model described in section 5. As per the preferred ENUM architecture model, the following model utilises the technical requirements as detailed in section 4.6.5 "Technical Requirements for Interworking", allowing full interoperability between Service Provider and different ENUM Service Providers (ESPs).

In this architecture model, a common root DNS server is not utilised. Instead, the root node functionality along with the ENUM Tier 0 and possibly also the Tier 1 are provisioned by an authoritative database either within the operator's network or outside the operator's network via a service bureau. In essence, this means that connection to the GRX/IPX Carrier ENUM is not a requirement, although, the GRX/IPX may be used to interconnect the end user service. It also means that an operator implementing this option does not necessarily have to wait for roll out of an ENUM Tier 1 server for the destination operator.

Operators who implement this option need to also apply a policy to the derived URI, as discussed in sub section 4.6.5.4, to avoid late session-establishment-failure or even worse, session-connection-timeout for their subscribers.

8.2 Architecture

The architecture for this model has many Authoritative Database provisioning options. This means that Service Providers have flexibility and may choose how to provision their ENUM databases depending on their network and market or regulatory environment. This has an advantage in that it allows Service Providers to choose the best option for their environment, based on such factors as local numbering policy, number portability solution, etc.

What remains the same though is that the Tier-2 server for the destination operator is identified.

The architecture for this model is depicted in the following figure:

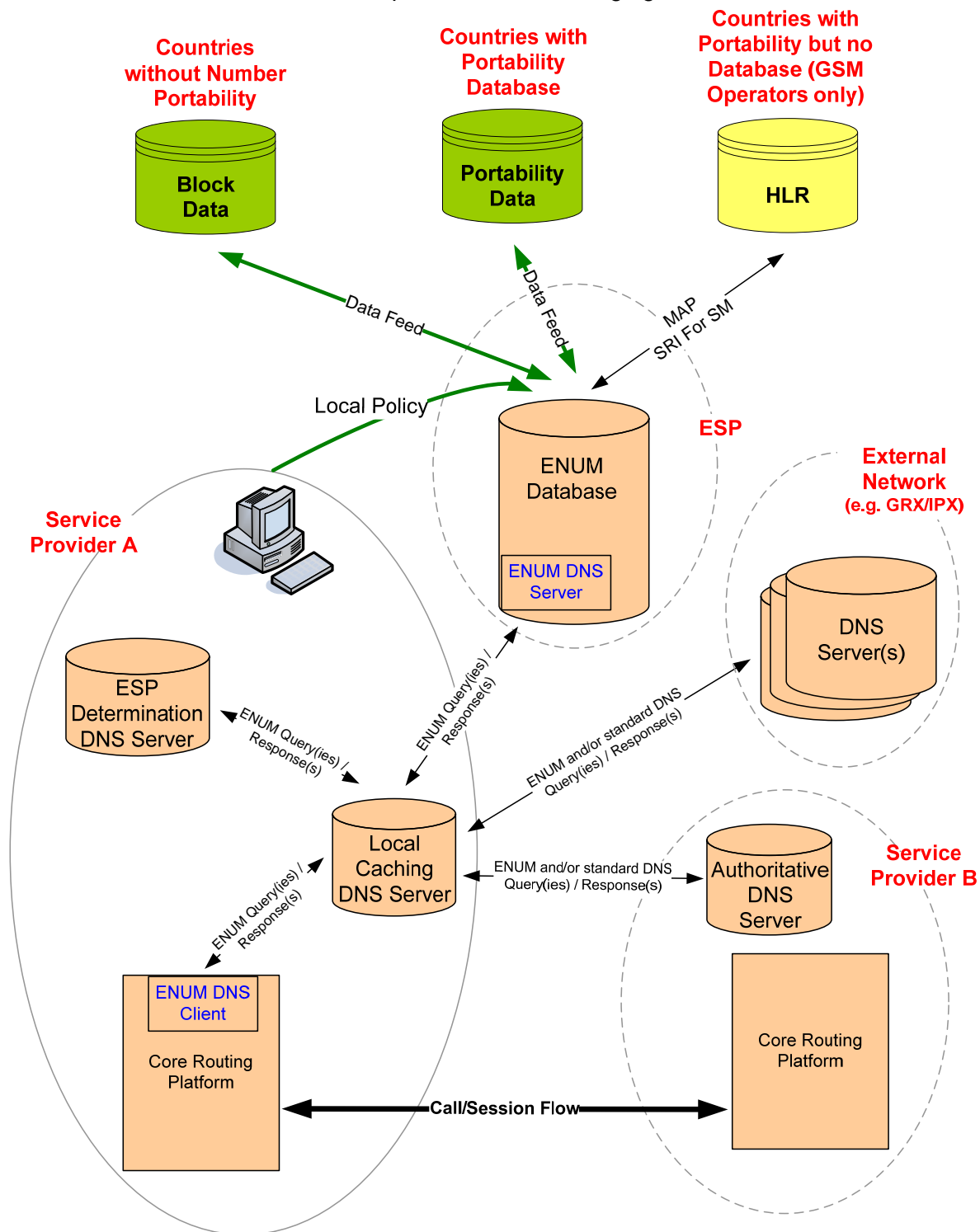


Figure 11: Architecture for the Multiple Root Model

It is an implementation option as to when a Service Provider provisions their own ENUM Server or utilises an ENUM Server in an ESP for destination numbers.

ENUM requests to an external network (e.g. GRX/IPX) and consequently to an authoritative DNS server in Service Provider B, is optional and occurs only when the ENUM Server does not return a final answer.

The ESP Determination DNS Server is used by the Service Provider to utilise multiple ENUM Servers (residing in their own network and/or in one or more ESPs) or, one or more ENUM Servers and the Single Root architecture model (further specification on interworking between the two architectural models is FFS in a future version of the present document). The Local Caching DNS Server needs to be preconfigured to forward DNS requests for domains ending in "e164enum.net" to the ESP Determination DNS Server. Alternatively, the two nodes/features can be provisioned on the same platform.

As shown above, there are three different implementation models that leverage existing industry sources of number-assignment data:

Number portability database: ENUM server or ESP utilizes an existing authoritative number portability database to determine the destination carrier for a given dialled number. The operator originating the query uses local policy information to provision an appropriate entry-point address for each of its interconnect partners as shown below.

Number-block database: ENUM server or ESP utilizes an existing authoritative number-block assignment database to determine the destination carrier for a given dialled number. This model works in any country that does not support number-portability.

MAP SRI for SM query: ENUM server or ESP utilizes existing HLR databases to discover the destination carrier for GSM networks around the world.

8.3 Resolution

The address resolution process in this model breaks down into the following logical steps:

- 1 Identify the ESP to use (given the dialled number);
- 2 Identify the Subscribed Network (using the determined ESP).

Local policy should be applied either at the ESP or in the Service Provider network, as detailed in sub-section 4.6.5.4.

The following figure depicts an example ENUM resolution for this model, after the Core Routing Platform has sent the necessary ENUM query to its local caching DNS server:

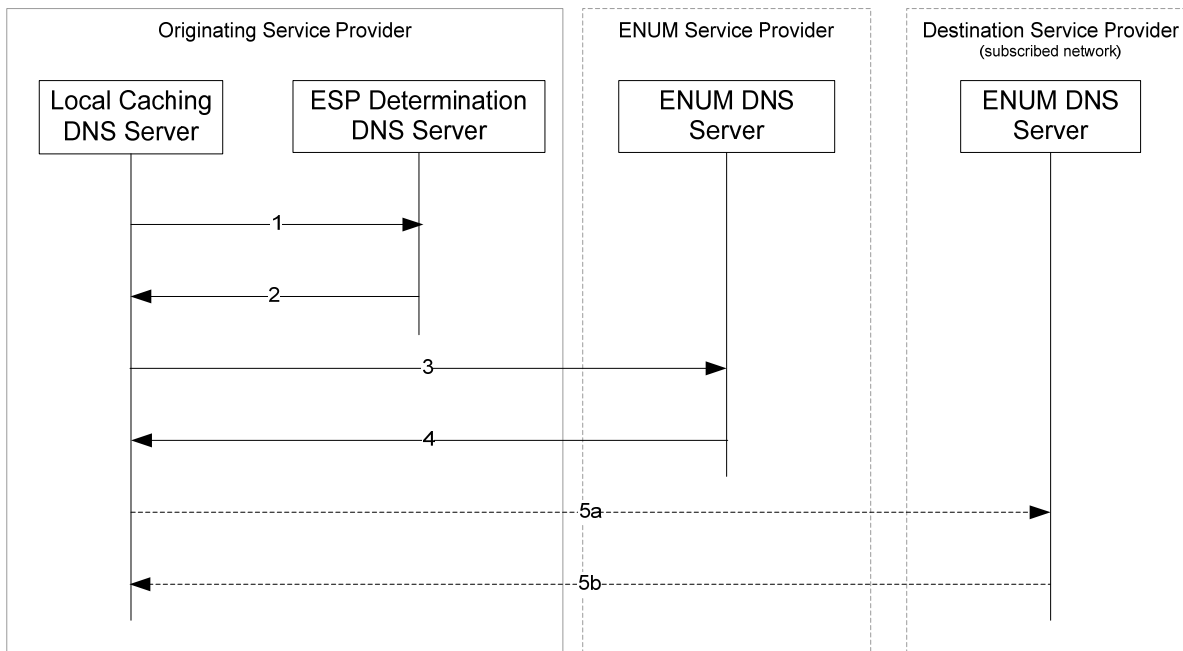


Figure 12: Example ENUM resolution in the Multiple Root Model

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

- 1 Service Provider's Local Caching DNS Server sends the DNS query to its own ESP Determination DNS Server (which is essentially a DNS server that is authoritative for "e164enum.net").
- 2 ESP Determination DNS Server analyses the queried ENUM FQDN. It then replies with the NS record for the Service Provider's chosen ESP for that domain (based on pre-configuration).
- 3 Service Provider re-sends the DNS query, but to the Special ENUM DNS Server in the ESP.
- 4 The ESP looks-up the E.164 number by using connections to existing ENUM servers, referencing number block data, querying (M)NP databases and/or by issuing a MAP_SRI_For_SM to the target network's HLR. It then replies with a list of URIs/URLs associated with the given E.164 number in NAPTR records, or the NS record(s) of the subscribed network's authoritative DNS server.
- 5 If the ESP replied with (an) NS record(s), then:
 - a) The Service Provider re-sends the query, but to the subscribed network's authoritative DNS server.
 - b) The subscribed network replies with a list of URIs/URLs associated with the given E.164 number in NAPTR records.

Note: As per normal DNS procedures, each reply a Service Provider receives is cached for a certain amount of time, therefore, negating the need of every message shown always having to be sent.

8.4 Access to ENUM Servers

In this model, the ENUM Service Provider takes care of all commercial agreements and any charges incurred for access to the sources of its back-end data used to service queries from Service Providers. The Service Provider typically will have a commercial agreement with an ENUM Service Provider (of which may include charges). Access to Service Provider Tier-2 servers is still required though.

8.5 Interworking with the preferred model

Service Providers who utilise this model still have to provide ENUM DNS Tier-1 and Tier-2 servers to enable other Service Providers utilising the preferred model (as described in sub-clause 5.6) to be able to resolve their queries. Such provisioning is implementation dependent, and no recommendations are made in the present document.