DNS Guidelines for Service Providers and GRX and IPX Providers

Version 19.0

23 November 2021

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

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

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.

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. Thus, a reasonable level of technical competence in DNS, and DNS server configuration is assumed throughout this document.

1.2 Scope

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

Particular attention is given to DNS 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 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 Internet i.e. those that use the "pub.3gppnetwork.org" domain name.

Note that ENUM is out-of-scope of this document and is addressed in [56].

1.3 Document Cross-References

Ref	Document Number	Title
1	IETF RFC 1034	"Domain Names - Concepts and Facilities"
2	IETF RFC 1035	"Domain Names - Implementation and Specification"
3	Void	No more used in current version of the document
4	Void	No more used in current version of the document
5	Void	No more used in current version of the document
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)"

Ref	Document Number	Title
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-Service Provider IP 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	Void	No more used in current version of the document
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	Void	No more used in current version of the document
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	Void	No more used in current version of the document
32	Void	No more used in current version of the document
33	Void	No more used in current version of the document

Ref	Document Number	Title
34	Void	No more used in current version of the document
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"
40	OMA OMA-TS-BCAST_Service_Guide-V1_1-20100111-D	"Service Guide for Mobile Broadcast Services"
41	Void	No more used in current version of the document
42	GSMA PRD IR.40	"Guidelines for IP Addressing and AS Numbering for GRX/IPX Network Infrastructure and User Terminals"
43	Void	No more used in current version of the document
44	IETF RFC 4825	"The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)"
45	3GPP TS24.623	"Extensible Markup Language (XML) Configuration Access Protocol (XCAP over the Ut interface for Manipulating Supplementary Services)"
46	GSMA PRD IR.92	"IMS Profile for Voice and SMS"
47	Void	No more used in current version of the document
48	GSMA PRD RCC.07	Rich Communication Suite - Advanced Communications Services and Client Specification
49	GSMA PRD IR.21	GSM Association Roaming Database, Structure and Updating Procedures
50	3GPP TS 32.501	Telecommunication management; Self-configuration of network elements; Concepts and requirements
51	3GPP TS 36.300	Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2
52	GSMA PRD IR.88	LTE and EPC Roaming Guidelines
53	3GPP TS 26.346	Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs
54	Void	No more used in current version of the document
55	3GPP TS 24.379	Mission Critical Push To Talk (MCPTT) call control; Protocol specification

Ref	Document Number	Title
56	GSMA NG.105	ENUM Guidelines for Service Providers and IPX Providers
57	3GPP TS 23.501	System architecture for the 5G System (5GS); Stage 2
58	GSMA PRD NG.102	IMS Profile for Converged IP Communications

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 "Secondary" Root DNS Servers (Formerly known as “Slave” Root DNS Server) and are commonly provisioned by that Service Provider's GRX/IPX. However, these Secondary Root DNS Servers can be provisioned by operators themselves if they so wish.

Each Secondary Root DNS Server is synchronised with a "Primary" Root DNS Server (Formerly known as “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' Secondary Root DNS Servers. The following diagram depicts this:

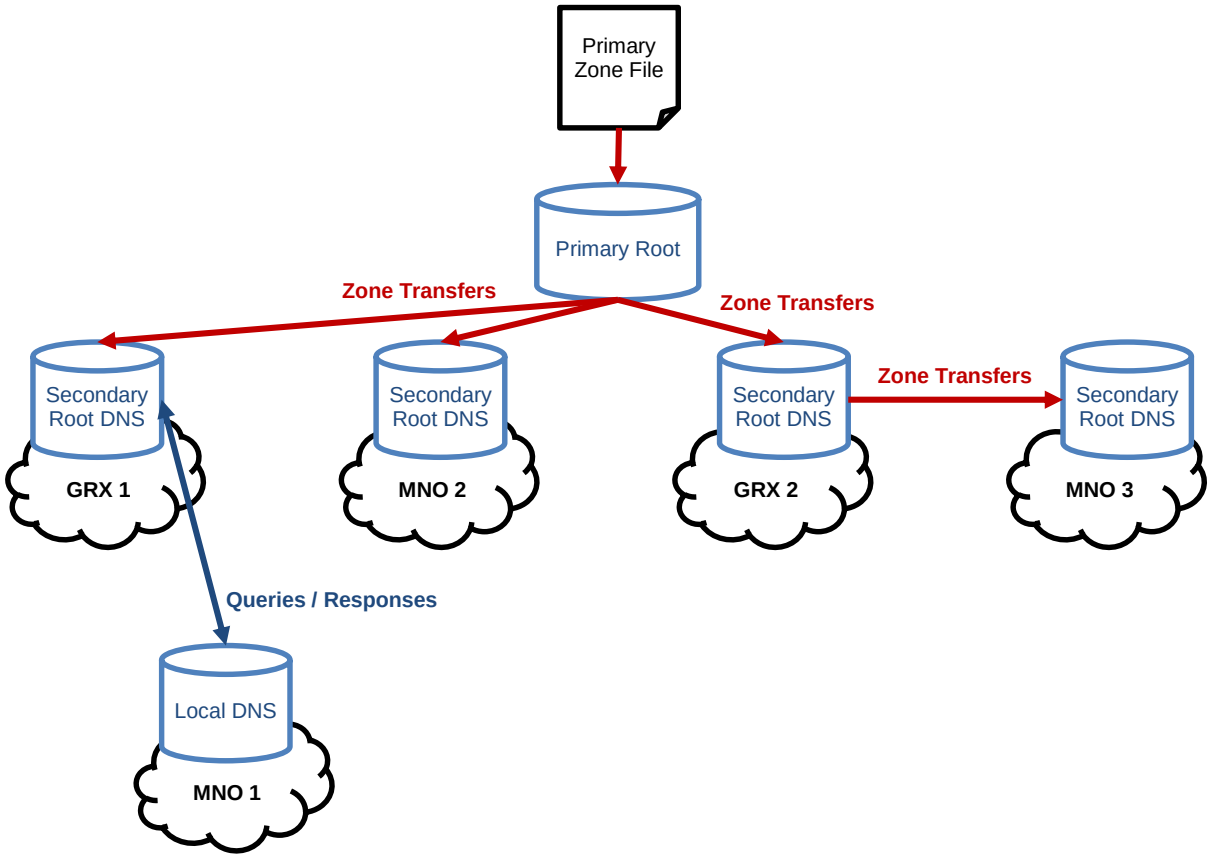

Figure 1: Backbone Architecture

The data in the Primary Root DNS Server is known as the Primary Zone File. The population of the data that goes into the Primary 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 Primary 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:

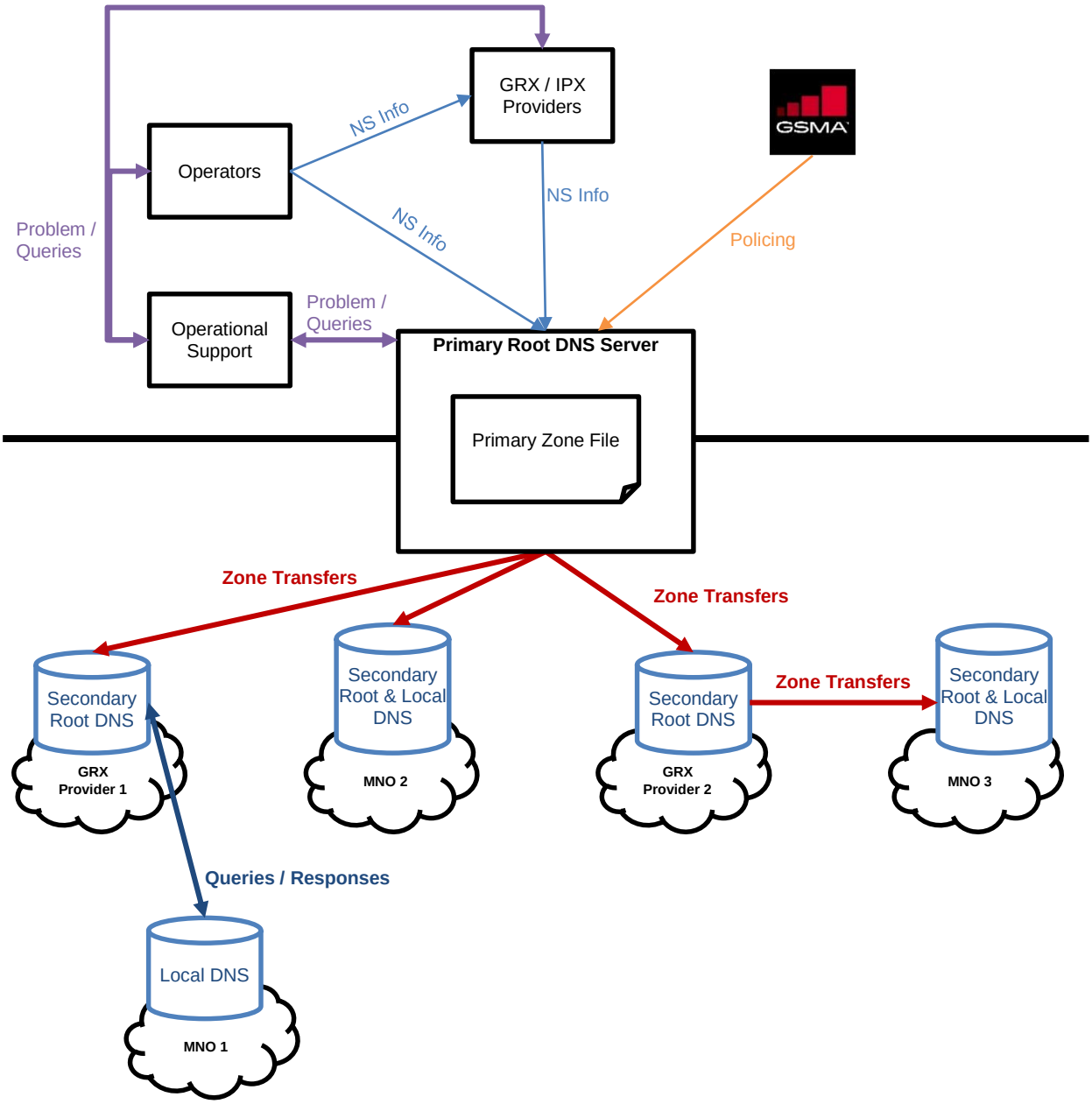

Figure 2: Overall Process Architecture

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:

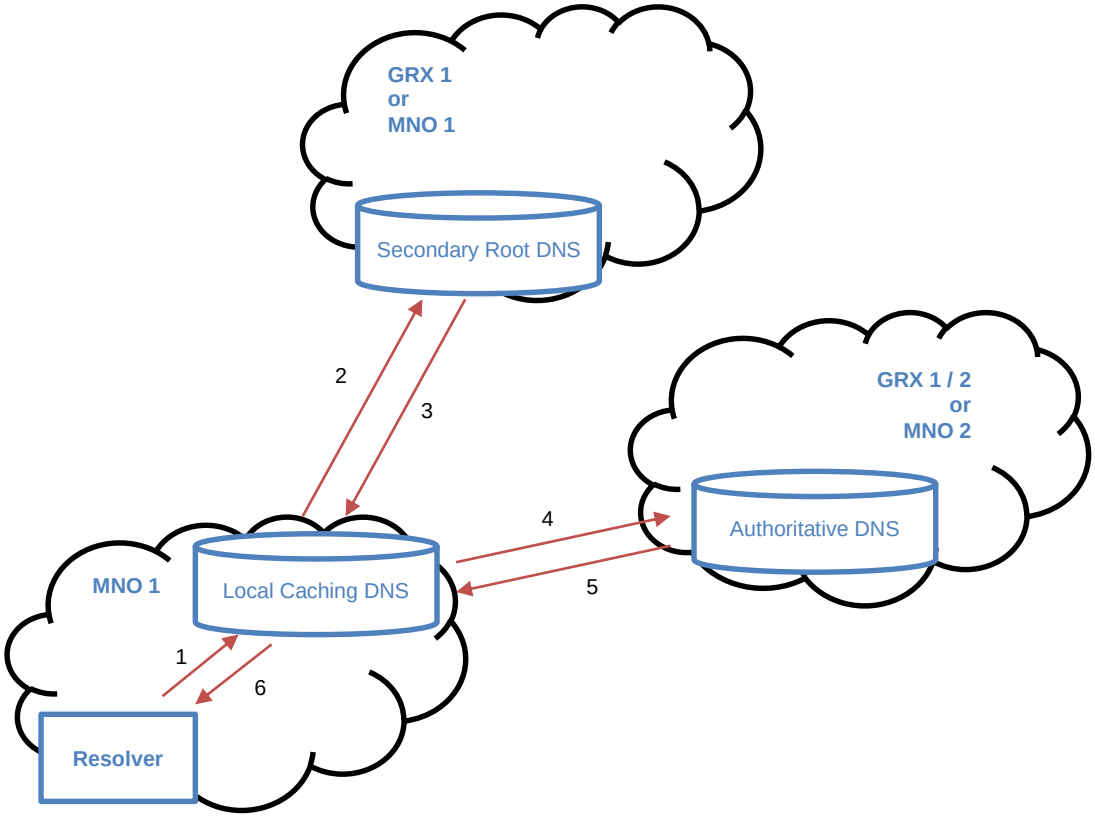

Figure 3: Resolver Architecture

1. The Resolver (for example an SGSN trying to find out the IP address of a GGSN) sends a query for the hostname (for example 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 the 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 (for example 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 1: The above shows only a typical message flow for the DNS resolving on the GRX/IPX. It may take extra queries when an MNO has Multiple levels of authoritative DNS servers (see example below and section 3.1). Please refer to section 4 for more detailed information for each service.

NOTE 2: In clause 7.11.21 (Section 17) of GSMA PRD IR.21 [49] provides for MNOs to directly exchange the IP addresses and DNS names of their authoritative DNS servers. This gives the option for an MNO who has received such information from another MNO to configure directly into their local caching servers the authoritative DNS servers IP addresses for the corresponding DNS names.
When this option is used, and a query matching a configured DNS name is received, the interaction with the Root DNS server specified in steps 2-4 above is bypassed. Instead the query is sent directly to the other operators authoritative DNS server, after which steps 5 and 6 follow. However, if the local caching DNS server has cached the answer to the query, the answer is sent directly as specified in step 2.

Instead of having a single Authoritative DNS, an Operator may choose to split the DNS into several levels of DNS for example a First Level DNS which may be authoritative for some of the domain names “owned” by the MNO, and one or more Second Level Authoritative DNSes, which may be authoritative for different “subdomainnames”, where for example a Second Level DNS may be outsourced to 3rd party service provider for a particular service.

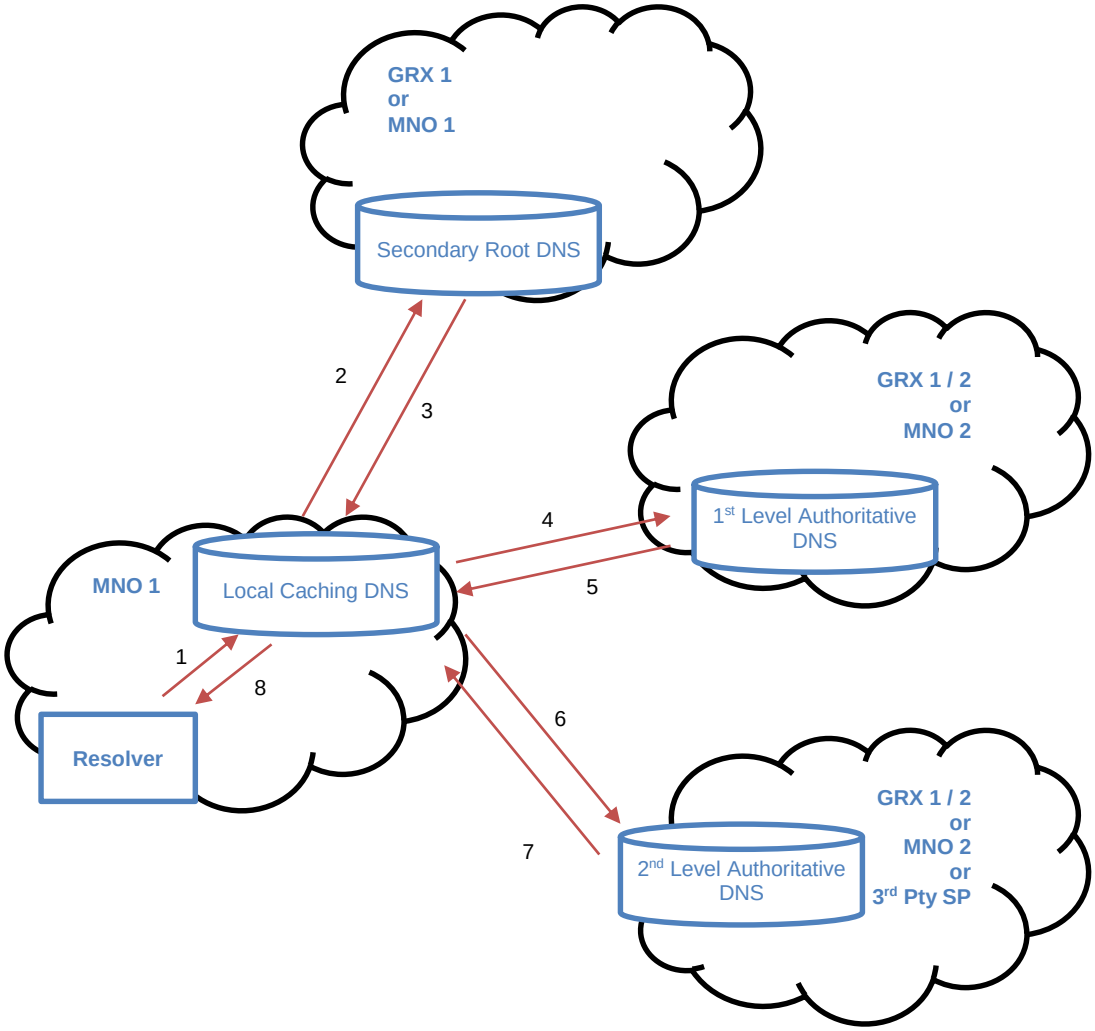

Figure 4: Resolver Architecture with multiple levels of Authoritative DNS

1. Same as step 1 in the example above
2. Same as step 2 in the example above
3. Same as step 3 in the example above
4. Same as step 4 in the example above
5. The First Level Authoritative DNS server may be authoritative for the queried domain name, in which case it 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). In this case the following step process continues with step 8.
   Alternatively for certain “subdomain names”, a second level DNS may be authoritative. In this case The First Level Authoritative DNS server returns a referral to the Second Level DNS server which is authoritative for the queried domain name of the hostname (for example returns the authoritative server for "<subdomainname>.mnc015.mcc234.gprs")

6. The local caching DNS server caches the response for a specified amount of time (specified by the First Level Authoritative DNS server) and then re - sends the query to the Second Level Authoritative DNS server as specified by the First Level Authoritative DNS server. The 2nd Level Authoritative DNS server may reside in the same GRX/IPX provider's network (GRX1), another GRX/IPX provider's network (GRX2), the network of the destination Mobile Network Operator (Service Provider 2), or in a 3rd Party Service Providers Network.
7. The Second Level Authoritative DNS server may respond 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).
8. 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 3: It is recommended that no more than two Levels of Authoritative DNS (that is First Level and Second Level) are provisioned in a resolution "chain".

NOTE 4: In case the option to directly configure the IP address of another operators DNS server is used as discussed in NOTE 2 above, only IP addresses of First Level Authoritative DNS Server should be configured.

Some IPX services are offered on different network segments (VLANs) that are application aware and that may not provide end-to-end IP connectivity, i.e. as shown in Fig 4 below, MNO2 can either be an On-net MNO or an Off-net via IPX2. The DNS architecture is required to take this into account. (See GSMA PRD IR.34 [12]). A resolver architecture where the DNS service is “fronted” with a DNS cache/forwarder is required.

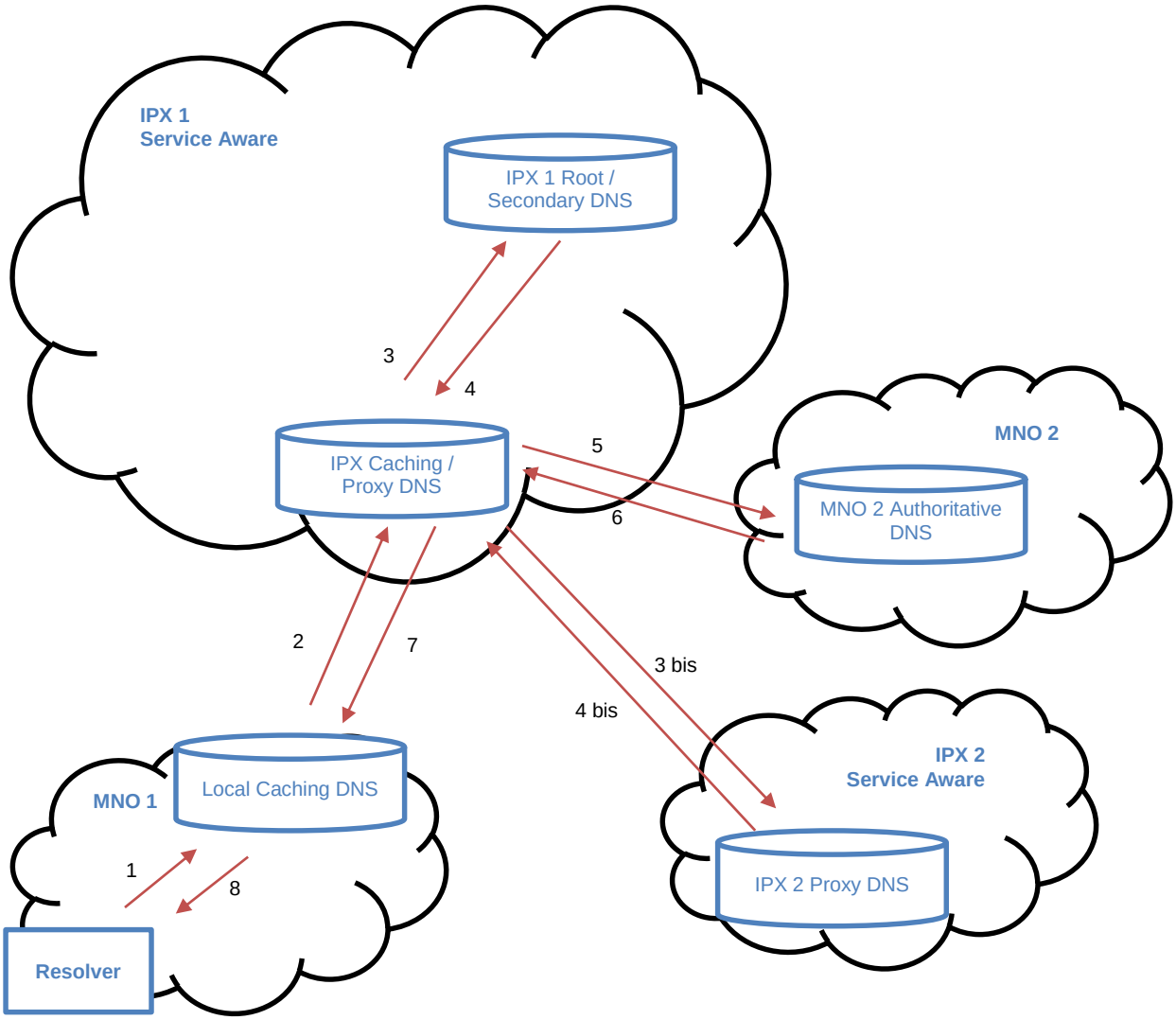

Figure 5 Service aware network resolver architecture

1. The Resolver sends a query, to its local caching DNS server for the hostname for which it wants the IP address.

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 8). Otherwise, it forwards the query on to the IPX proxy/DNS
3. Based on the requested domain, the IPX DNS/Cache, either sends the query to the root DNS (in case MNO2 is on-net) or to the next IPX provider proxy (if MNO2 is off-net) to resolve the query.

4. The secondary root DNS returns the authoritative DNS for the requested domain in MNO 2 or (message 4-bis) the IPX 2 proxy returns the query response.

5. (Case of on-net only:) The IPX proxy/cache sends the query to the authoritative DNS in MNO 2 network.
6. (Case of on-net only:) The authoritative DNS in MNO 2 returns the response to the query.
7. The IPX proxy/cache returns the response to the query to the cache in MNO 1 network.
8. The response is returned from the local cache to the resolver.

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 2.3.3 below. **No other domain name formats are currently supported on the GRX/IPX network!** This effectively means a limitation of domain names 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.

For the ".gprs" domain name, so called "human friendly" sub-domains are also allowed, as specified in 3GPP TS 23.003 [8], section 9. This consists of simply an FQDN reserved in the Internet domain name space e.g. serviceprovider.fi, serviceprovider.co.uk. However, such sub-domains of ".gprs" are not generally used in the GRX/IPX network and it is recommended not to use these as they can negatively affect GPRS/3G PS roaming. See section 2.3.3 below for more details.

More information on processes and procedures relating to domain names can be found in section 5.

2.3.3 Domain names used on the GRX/IPX DNS

The following provides a summary of the domain names that are used by Service Providers on private IP inter-connects and on the GRX/IPX network. These domain names are only resolvable by network equipment and not by end users. That is, they are exclusively used on the Network-Network Interface (NNI) and not on the User-Network Interface (UNI).

Additional domain names that are resolvable on the GRX/IPX network's DNS may be added in the future. See section 5 for more details.

For more details 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	Service Provider domains of the form: <Network_Label>.mnc<MNC>.mcc<MCC>.gprs Where <Network Label> is the Network Label part of the Access Pont 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, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in GPRS for the Operator ID in APNs. See section 4.2 and also 3GPP TS 23.003 [8], section 9, for more information. For Support of 2G/3G and EPC coexistence, see also section 4.17	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. Service Providers should avoid using Network Labels consisting of any of the below defined sub-domains, in order to avoid clashes.	Domain needs to be resolvable by at least all GPRS/PS roaming partners.
	rac<RAC>.lac<LAC>.mnc<MNC>.mcc<MCC>.gprs 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, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	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 and also 3GPP TS 23.003 [8], Annex C.1, 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.	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).

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
	nri<NRI>.rac<RAC>.lac<LAC>.mnc<MNC>.mcc<MCC>.gprs 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, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	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 and also 3GPP TS 23.003 [8], Annex C.1, for more information.		
	rnc<RNC>.mnc<MNC>.mcc<MCC>.gprs 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, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in SRNS relocation to route to the target RNC in the new SGSN (possibly in a new PLMN). See section 4.2 and also 3GPP TS 23.003 [8], Annex C.3, for more information.		
	mms.mnc<MNC>.mcc<MCC>.gprs Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits	Used in MMS for the domain name part of the FQDN for MMSCs. See section 4.3 and also 3GPP TS 23.140		Domain needs to be resolvable by at least all directly connected MMS interworking partners/Service Providers and directly

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
	by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	[15], section 8.4.5.1, for more information.		connected MMS Hub Providers.
	<Internet_assigned_domain_name>.gprs Where <Internet_assigned_domain_name> is a domain name reserved by the Service Provider on the Internet. An example is "example.com.gprs"	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.	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.	Domain needs to be resolvable by at least all GPRS/PS roaming partners.
.3gppnetwork.org	ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in IMS in SIP addressing; specifically, in the Private and Public Identities used in SIP registration. See section 4.5 and 3GPP TS 23.003 [8], section 13, 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. Sub domains within the Service Provider's domain (i.e. mnc<MNC>.mcc<MCC>) are documented in	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.
	rcs.mnc<MNC>.mcc<MCC>.3gppnetwork.org As above. The differentiator “rcs” is used to enable differentiation between IMS cores providing MMTEL and RCS services in the dual registration case (see	Used in SIP addressing to a MNO-provided IMS core providing only RCS services.		As above

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
	GSMA PRD NG.102 [578]). In this case, the IMS core providing RCS services is hosted by the MNO.		3GPP TS 23.003 [8]. It is recommended that 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.	
	`<provider>.rcs.mnc<MNC>.mcc<MCC>.3gppnetwork.org` The <provider> identifies a non-MNO 3rd party entity providing RCS services on behalf of a single MNO identified by MCC/MNC. Used to identify the IMS core providing RCS services in the dual registration case (see GSMA PRD NG.102 [578]) where the hosted IMS solution is provided with MNO consent (i.e. using the 3rd party's terms and conditions, but using standard MCC/MNC based domain for provisioning).	Used in SIP addressing to a hosted IMS core providing only RCS services.		As above
	`<provider>.rcs.3gppnetwork.org` In this case, the <provider> is a domain name reserved by a 3rd party RCS provider on the Internet. It identifies Used to identify the IMS core providing RCS services in the dual registration case (see GSMA PRD NG.102 [587]) where the hosted IMS solution is provided without MNO consent (i.e. using the 3rd party's terms and conditions and a proprietary domain for provisioning).	Used in SIP addressing to a hosted IMS core providing only RCS services.		As above
	`wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org` Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in WLAN inter-working for NAI realms. See section 4.4 and 3GPP TS 23.003 [8], section 14, for more information.		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

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
				Diameter is used and the next hop is determined by DNS rather than a look up table.
	gan.mnc<MNC>.mcc<MCC>.3gppnetwork.org Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in the Generic Access Network for Full Authentication NAI realms and Fast Re-authentication NAI realms. See section 4.7 and 3GPP TS 23.003 [8], section 17.2, for more information.		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.
	epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in the Enhanced Packet Core (EPC) architecture (previously known as Service Architecture Evolution – SAE) for NAIs and FQDNs of EPC related nodes. See section 4.9 and 3GPP TS 23.003 [8], section 19, for more information. For support of EPC and 2G/3G		Domain and sub-domains need to be resolvable by EPC/SAE roaming partners.

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
		coexistence see also section 4.17		
	5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2-digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in the 5G Core (5GC) architecture for NAIs and FQDNs of 5GC related nodes. See section 4.19 and 3GPP TS 23.003 [8], section 28, for more information.		Domain and sub-domains need to be resolvable by 5GC roaming partners.
	ics.mnc<MNC>.mcc<MCC>.3gppnetwork.org Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in the IMS Centralised Services feature in SIP addressing. See section 4.10 and 3GPP TS 23.003 [8], section 20, for more information.		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.
	node.mnc<MNC>.mcc<MCC>.3gppnetwork.org Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	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.
	oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org	Used by eNBs and possibly other network entities in network	Each Service Provider is allowed to use only sub-domains	Domain should only be resolvable by entities within an

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
	Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	element self-configuration to discover an Operations and Maintenance (OAM) system. See section 4.16 and also 3GPP TS 23.003 [8] section 23, for more information.	consisting of MNC(s) and MCC(s) that are allocated to them by ITU-T and their local national numbering authority.	operator's network, or in the case of network sharing, within the shared operator's network.
	5gc.nid<NID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org Where <NID>, <MNC> and <MCC> are the NID, MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2-digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used to identify Home Network Domain for a Stand-alone Non-Public Network (SNPN). See section 4.20 and 3GPP TS 23.003 [8], section 12.7 (NID) and section 28, for more information.	For interworking with an SNPN (e.g. discovery of AMFs from an SNPN by a shared NG RAN), this sub-domain can be used when the MCC, MNC and NID uniquely identifies the SNPN. For signalling within an SNPN, this sub-domain can be used regardless of whether the MCC, MNC and NID uniquely identifies the SNPN or not.	Domain needs to be resolvable by at least all roaming/interworking partners for the services used by this domain name.
	mc1-encrypted.3gppnetwork.org	Used by the MCPTT service in an XML text where confidentiality protection of a URI as specified in TS 24.379 [55] is required. See	Each Service Provider is allowed to include this domain name when confidentiality protection of a URI as specified in TS 24.379	Intentionally not resolvable by any entity.

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
		Rel-13 version of 3GPP TS 23.003 [8], section 26.2, for more information.	[55] is required and the URI is not used for routing.	
	unreachable.3gppnetwork.org	Used in WLAN inter-working, specifically as a realm in the Alternative NAI. Its purpose is to enable the UE to retrieve a list of PLMNs behind a WLAN Access Point. See 3GPP TS 23.003 [8], 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.
.ipxsp.org	spn<SPN>.ipxsp.org Where <SPN> is the Service Provider Number of the Service Provider. An example is: "spn001.ipxsp.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 domain "mnc<MNC>.mcc<MCC>.3gppnetwork.org".	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.	Each Service Provider is allowed to use only SPNs that are allocated to them by ITU-T.	Domain needs to be resolvable by at least all roaming/interworking partners for the services used by this domain name.

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		

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
		available tools using this hierarchy for reverse look-ups, it would not be feasible to use any different TLD.		
ipxnetwork.org	<IPXN>.ipxnetwork.org Where IPXN is the IPX provider company name or acronym. It is agreed amongst IPX/GRX providers and assigned on a first come – first served basis (see section 5.2). Further subdomains under this are the responsibility of the owning IPX provider.	Not used in any particular service, however, can be used by any IPX Provider for any service they see fit. The main intention is to provide a domain name that IPX provider can use for IPX proxies or other equipment.	One subdomain per IPX provider. An IPX provider shall not use two subdomains.	Domain needs to be resolvable by at least all roaming/ interworking partners for the services used by this domain name.

Table 1: Definitive list of domain names owned by GSMA that are used on the GRX/IPX DNS

2.3.4 Domain names used on the Internet DNS (and owned by GSMA)

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	gan.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in the Generic Access Network for home network domain names in node identifiers. See section 4.7 and 3GPP TS 23.003 [8], section 17.3, 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. 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	Domains need to be resolvable on the Internet.
	w-apn.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in WLAN inter-working for PDG addressing. See section 4.4 and 3GPP TS 23.003 [8], section 14, 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. The same rules apply for APN constructs, as defined in GSMA PRD IR.34 [12].	
	h-slp.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in	Used in the Secure User Plane Location feature for Home SUPL Location Platform addressing. See	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	

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
	decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	section 4.8 and OMA-AD-SUPL-V1_0-20070615-A [27] section 7.2.2, for more information.	national numbering authority.	
	`bsf.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org` Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in the Generic Authentication Architecture for BSF addressing when USIM is used in bootstrapping. See section 4.6 and 3GPP TS 23.003 [8], section 16, for more information.		
	`andsf.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org` Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in EPC and WLAN inter working (3GPP Rel 8) home agent addressing. See 3GPP TS 23.003 [8], section 21, for more information.		
	`ha-apn.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org` Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC		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,	

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
	padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.		as defined in GSMA PRD IR.34 [12].	
	`bcast.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org` Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in the OMA Mobile Broadcast Services (BCAST) enabler, version 1.1, for Service Guide discovery by a client with access to an IMSI. See section 4.12 and OMA-TS-BCAST_Service_Guide-V1_1-20100111-D [40] 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.	
	`rcs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org` Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any two (2) digit MNC padded out to three (3) digits by inserting a zero ("0") on the beginning for example 15 becomes 015.	Used for the RCS/RCS-e service. RCS/RCS-e service may use further subdomain names depending on the RCS/RCS-e service evaluation and developments (for example config.rcs.mnc	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 name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
		<MNC>.mcc<MCC>.pub.3gppnetwork.org). The description and the use of the subdomain names will be referenced in the RCS/RCS-e specifications where this domain can be used by all RCS/RCS-e versions.		
	bsf.ims.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in the Generic Authentication Architecture for BSF addressing when ISIM is used in bootstrapping. See section 4.6 and 3GPP TS 23.003 [8], section 16, 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.	
	xcap.ims.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC	Used in supplementary service configuration using XCAP as specified in IR.92 [46]. Also see section 4.13	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	

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
	padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	and 3GPP TS 23.003 [8], section 13.9, for more information.	national numbering authority.	
	epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used in inter-working untrusted non-3GPP access network to EPC. See section 4.15 and 3GPP TS 23.003 [8], section 19.4.2.9, 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	
	mbmsbs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org Where <MNC> and <MCC> are the MNC and MCC of the Service Provider represented in decimal (base 10) form, with any 2 digit MNC padded out to 3 digits by inserting a zero ("0") on the beginning e.g. 15 becomes 015.	Used by a UE for MBMS Service Announcement Bootstrap. See section 4.18 and 3GPP TS 23.003 [8], section 15.5, 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	
	epdg.epc.mcc<MCC>.visited-country.pub.3gppnetwork.org Where <MCC> is the MCC of the country in which the UE is located represented in decimal (base 10) form.	Used by a roaming UE to determine whether visited country mandates the selection of an ePDG in this country.	Details of usage is defined in Release 13 version of 3GPP TS 23.402 [29], section 4.5.4.5.	

Domain name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
		See 3GPP TS 23.003 [8], section 19.4.2.9.3 for more information.		

Table 2: Definitive list of domain names owned by GSMA that are used on the Internet DNS

2.3.5 Domain names used on the GRX/IPX DNS for UNI

Only the domain name "ipxuni.3gppnetwork.org" is defined for domain names of this type (see 3GPP TS 23.003 [8]). However, there are currently no sub-domains reserved under this domain name.

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 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.spn< SPN>.ipxsp.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.spn001.ipxsp.org

Note that usage of the hostnames and sub-domains specified within this section under "mnc<MNC>.mcc<MCC>.gprs" is now deprecated, and Service Providers are recommended to use either of "mnc<MNC>.mcc<MCC>.3ppgnetwork.org" or "spn<SPN>.ipxsp.org" domains at their earliest convenience. Of course, usage of "mnc<MNC>.mcc<MCC>.gprs" for the uses as stated in section 2.3.3, is *not* deprecated and should continue as per normal.

2.5 Host names for the evolved packet Core (EPC)

The naming of Nodes for the Evolved Packet Core is specified in clause 19 of 3GPP TS 23.003 [8]

2.6 Host names for the IP Multimedia Subsystem (IMS)

Within the IP Multimedia Subsystem (IMS) the following Naming Convention for IMS Nodes shall be used <Node name>. <SP Domain Name>, where

- <Node name> may consist of one or more labels that uniquely identifies the IMS node within the Service Provider network.

  To avoid conflicts with future other subdomains to the <SP Domain Name> it can be considered good practice to include ".node" as the right-most label of the <Node Name>

- <SP Domain Name> is a Domain Name that is owned by the Service provider.

  "ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org" is the recommended <SP Domain Name> for all IMS Nodes.

"ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org" must be used as <SP Domain Name> for IMS Nodes that are individually addressable over the IPX network by SIP or any other protocol, and where those Node Names need to be resolved over the IPX DNS system.

Examples of IMS nodes that may need to be individually addressable, are all nodes that are addressed using a SIP Route Header, such as the nodes hosting the functionalities of a P-CSCF, S-CSCF, TRF, ATCF, and eMSC-S for I2.

3 General DNS Configuration 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).

Such commercial DNS Namesserver 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 PTR (Pointer) records for all IP addresses that FQDNs refer to, for example for APNs, MMSC addresses and so on. This is not needed for inter-working to be successful, but rather, is recommended as it aids in trouble shooting/debugging activities such as performing a "traceroute".

Reverse mapping for IPv4 addressing uses the "in-addr.arpa" domain, and reverse mapping for IPv6 addressing uses "ip6.arpa". See section 2.3.3 for more information.

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 6 below depicts both iterative and recursive queries:

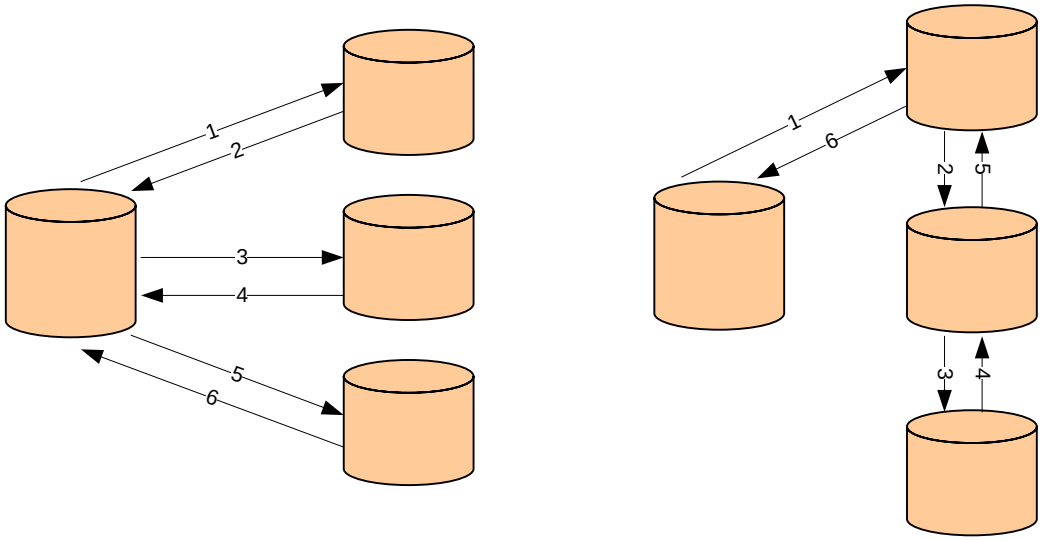

Figure 6: Iterative (left) and Recursive (Right) modes of DNS querying

In non-service aware IPX (Example: GRX), 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 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, this could be 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, that is 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 for example their GRX/IPX Provider.

Service providers may have all appropriate data available in a single level of authoritative DNS servers, where each authoritative DNS server holds all the appropriate data for the Service Provider.

Alternatively, Service Providers may choose to divide the appropriate data between a First Level Authoritative DNS Servers and 2nd Level Authoritative DNS Servers whereby each 2nd-level Authoritative DNS server only holds a subset of the appropriate data for the Service provider.

When information about DNS servers are exchanged with the GRX/IPX Root DNS and other Service Providers for example via PRD IR.21, and when 2nd-Level Authoritative DNS server are used, it is essential to make a clear distinction between the First Level Authoritative DNS servers and 2nd-Level Authoritative DNS servers. This is to ensure that only First Level Authoritative DNS server are published in the GRX/IPX Root DNS such that the first query to an Operators DNS always goes the First Level Authoritative DNS and that the second level DNS servers are reached only by means of referrals from the First Level Authoritative DNS server.

3.10 Resource Records

Service Providers and IPX Providers should take care to provision only the DNS Resource Records (RRs) that are necessary for service interworking, trouble shooting and O&M (Operations & Maintenance).

3.11 Support for IPv4 and IPv6

Support for IPv4 and IPv6 on Service Provider DNS Nameservers is twofold: the ability to serve data relating to IPv4 and IPv6 addresses, and connectivity to/from the nameserver.

For configuration information in a Nameserver, both IPv4 and IPv6 information can coexist together. Service Providers just need to ensure that the Nameserver software used is

capable of supporting the relevant Resource Records (RR) required. The "A" RR is used to hold IPv4 address information and the "AAAA" RR for IPv6 address information. Details on reverse mapping (IPv4/IPv6 address to domain name) are specified in section 3.6.

For connectivity to a Nameserver, it is highly recommended that all Service Provider Nameservers be reachable using IPv4. Any Nameservers serving IPv6 information should also be reachable using IPv6.

See GSMA PRD IR.34 [12] and GSMA PRD IR.40 [42] for more information on recommendations relating to IPv4 and IPv6 routing and addressing.

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 [26].

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 [23], and 3GPP TS 29.060 [26].

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 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).

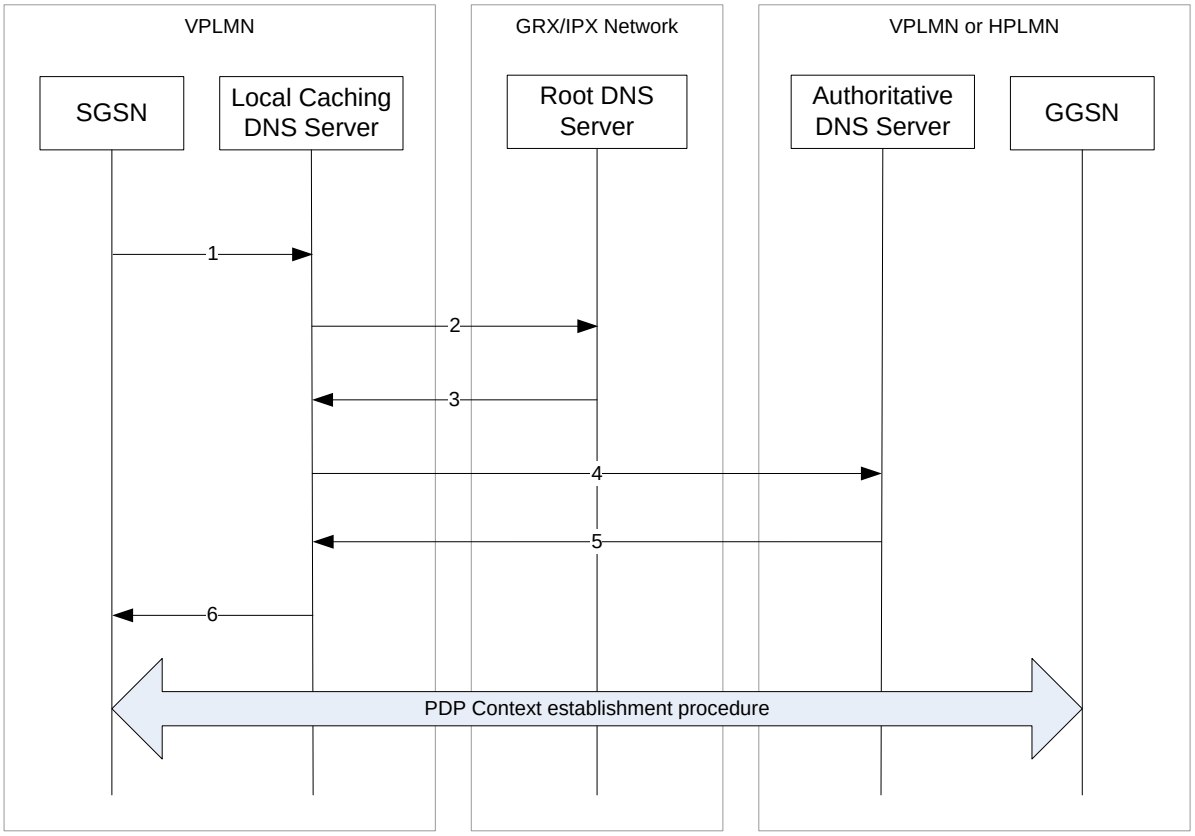

Figure 7: DNS message flow for PDP Context activations

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).

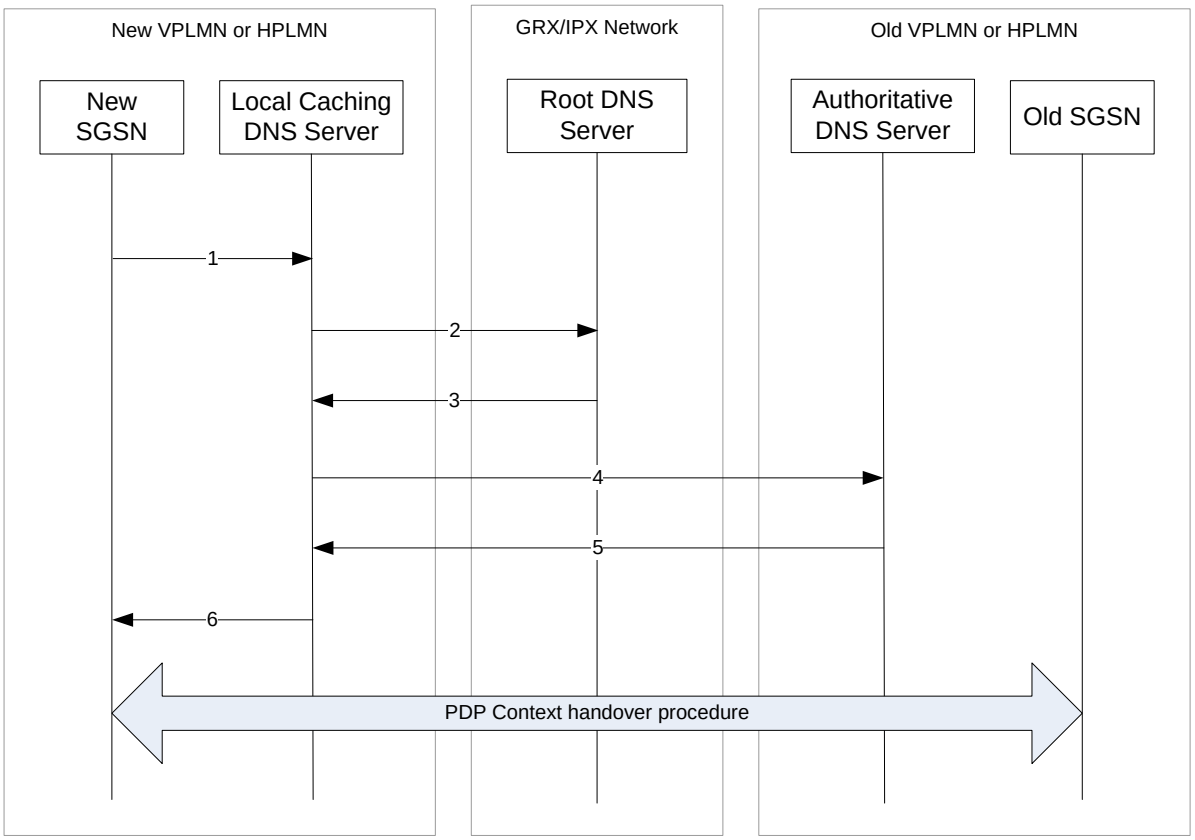

Figure 8: DNS message flow for PDP Context handovers between SGSNs

7. 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).
8. 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.
9. 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)).
10. 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).
11. The Authoritative DNS Server replies to DNS Query received from the Local Caching DNS Server with the IP address of the old SGSN.
12. 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 routeing 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 section 2.3 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:

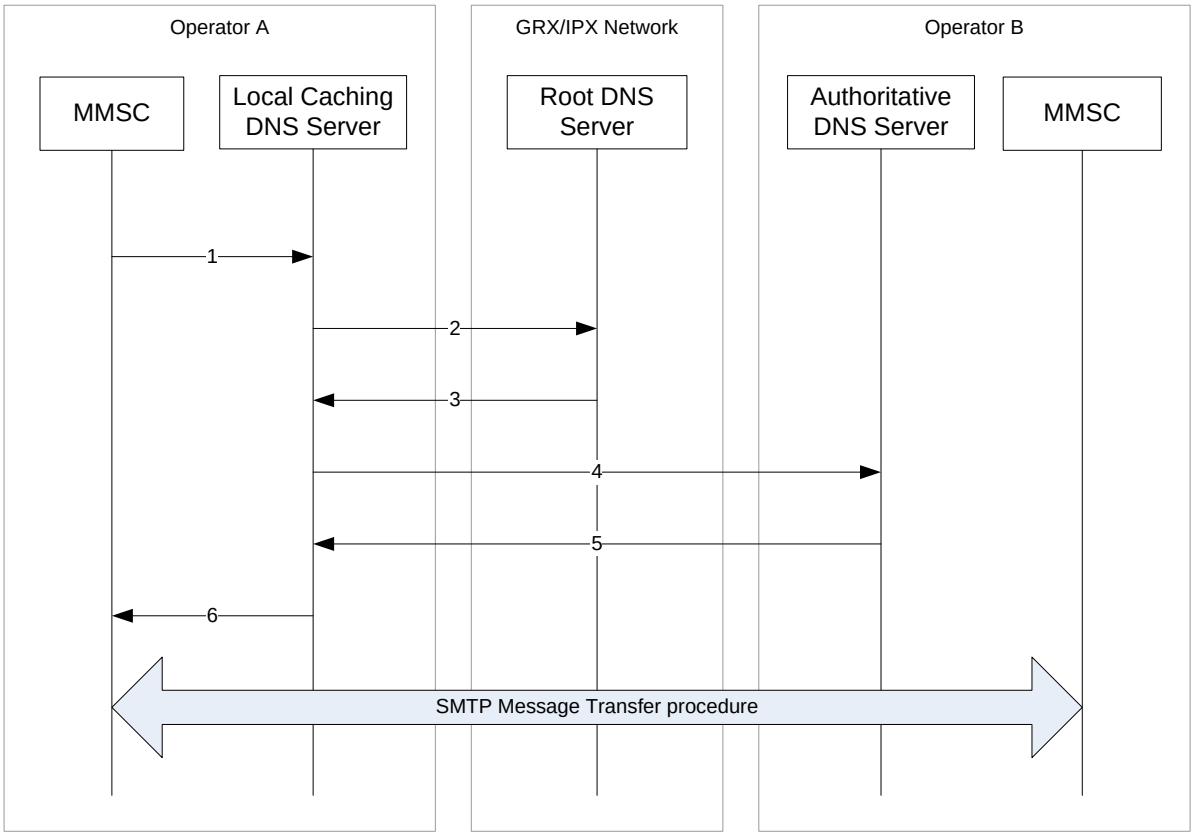

Figure 9: MMS Direct Inter-network Delivery

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.

   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:

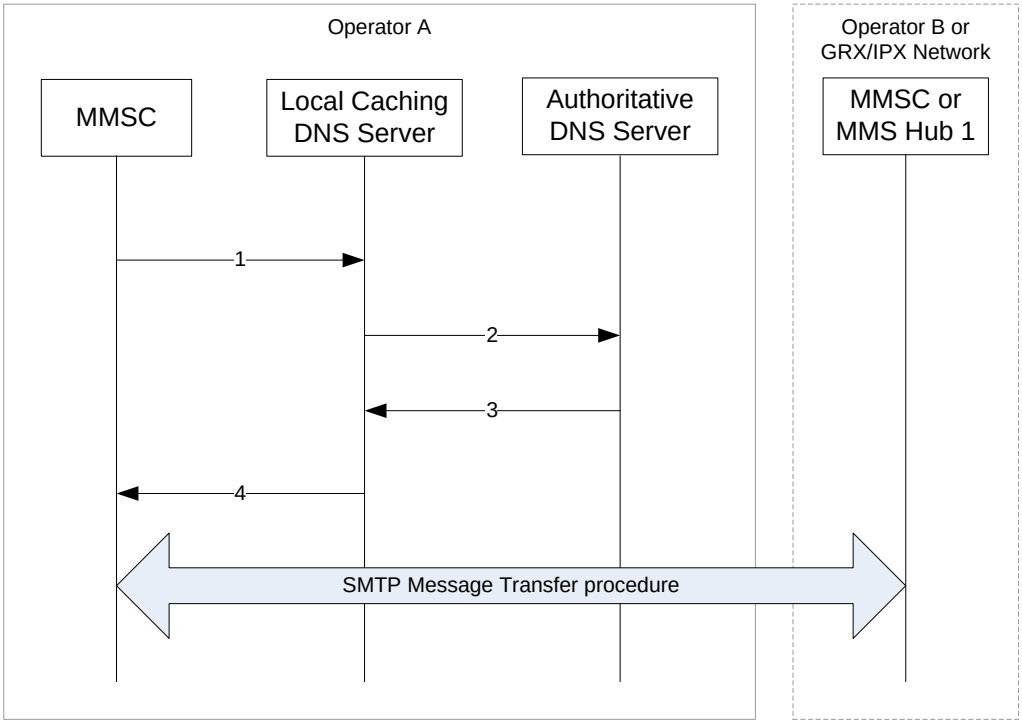

Figure 10: MMS Inter-operator Delivery

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.

    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 [14]), the message flow is the same as in Figure 7 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 9 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 9 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 9 shows also in principle the difference between the following two authentication methods:

- Web Based Authentication
- 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.

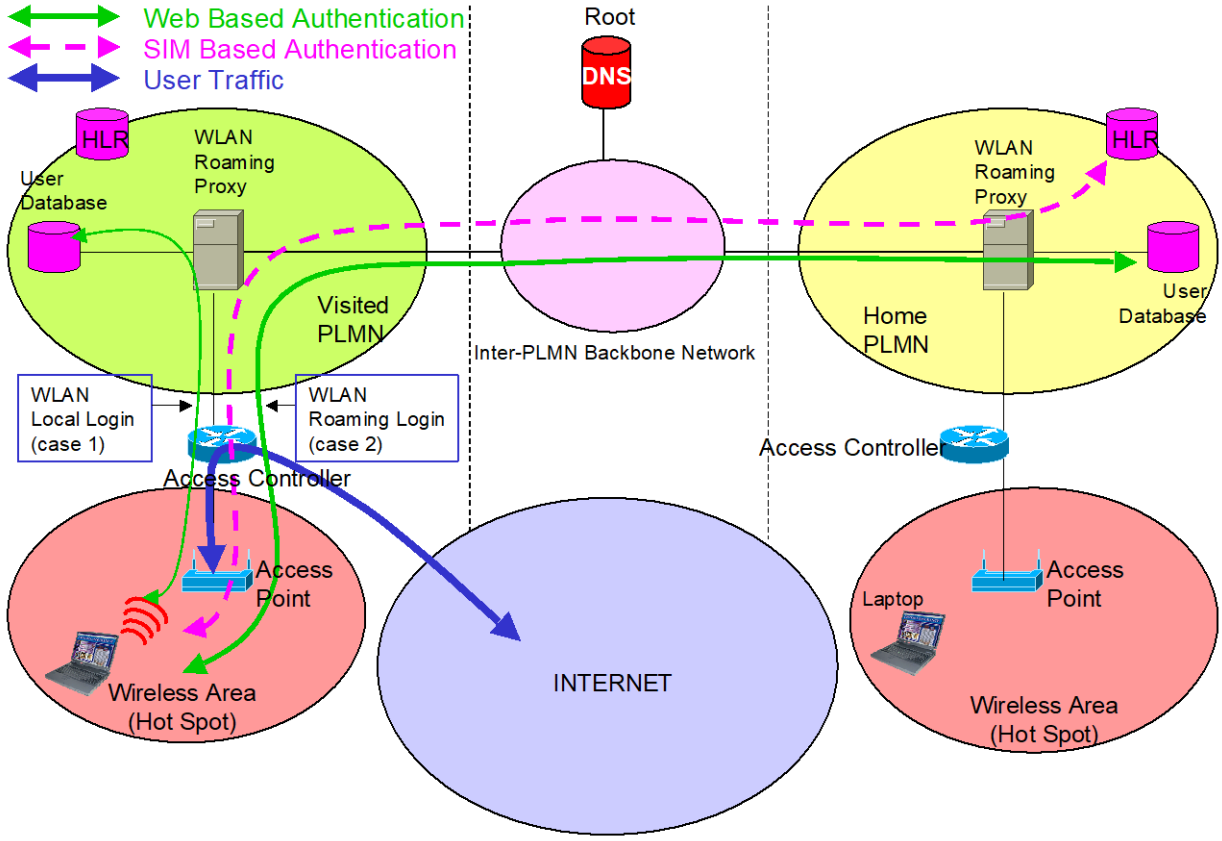

Figure 11: WLAN user authentication mechanism

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 Sub-system (IMS)

4.5.1 Introduction

The IP Multi-media Sub-system (IMS) provides a standardised architecture for providing feature rich multimedia services/applications, such as speech communication, messaging, 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) to be used by Service Providers.

Diameter is also used on some interfaces in the IMS architecture, however, these are intra-Service Provider interfaces and so are outside the scope of this PRD.

Figure 10 shows an end-to-end IMS session. Only the basic architecture of involved IMS network elements is shown. Please note that signalling and user data of an IMS session are separated. Signalling and user data make use of different PDN connections, but use the same (originating) IP address.

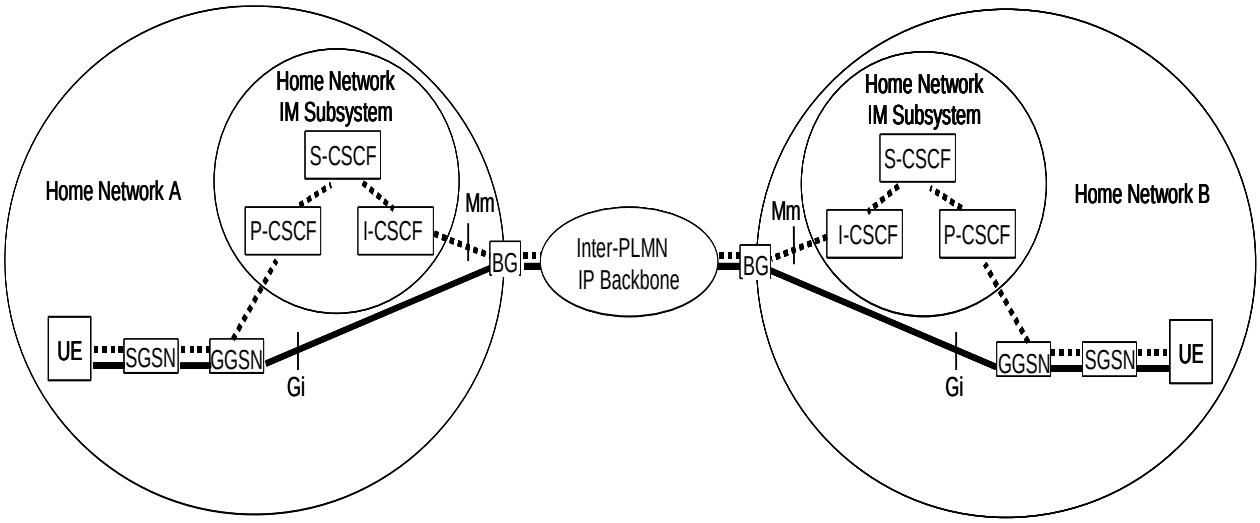

Figure 12: IMS Session Inter-working

IMS subscribers are addressed by SIP URIs or E.164 numbers represented as Tel URIs or SIP URIs with the "user=phone" option. ENUM is specified in IMS as the means to convert an E.164 number into one or more SIP URI as indicated in section 2.3.3. See GSMA PRD NG.105 [56] for more information on ENUM Guidelines for Service Providers and IPX Providers.

For resolving SIP URIs to SIP Servers (see IETF RFC 3263 [17]), the support of the NAPTR Resource Record functionality (as defined in IETF RFC 3404 [7]) and the SRV Resource Record functionality (as defined in IETF RFC 2782 [18]) is needed in the Service Provider's DNS servers.

More information on IMS roaming and interworking can be found in GSMA PRD IR.65 [11].

4.5.2 SIP server configuration

There are several RFCs covering use of SIP in the DNS. These include IETF RFC 3824 [24], IETF RFC 3263 [17], and IETF RFC 3403 [6].

The reason this configuration is needed is as follows:

When a SIP session is initiated by a user, they address the session to either a SIP URI (e.g. kim@example.com) or an E.164 number. In both cases, the IMS needs to know the IP address of the SIP server to which it can route the session. The SIP server information contains the detail needed to provide the destination network's SIP server IP address to the calling network based on the information in the SIP URI.

The approach described in this section is compliant with these RFCs and consists of 4 separate steps. It is consequently known as the “4-step approach”.

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 section 4.5.2.

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    sipserv1.example.com.
_sip._tcp.example.com.      SRV 0 2 5060    sipserv2.example.com.
_sip._udp.example.com.      SRV 0 1 5060    sipserv1.example.com.
_sip._udp.example.com.      SRV 0 2 5060    sipserv2.example.com.
_sips._tcp.example.com.     SRV 0 1 5060    sipserv3.example.com.
_sips._tcp.example.com.     SRV 0 2 5060    sipserv4.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 finds 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.

NOTE: The address of the Bootstrapping Server Function (BSF) used by the UE is dependent on whether USIM or ISIM is used in bootstrapping. See 3GPP TS 23.003 [8], section 16.

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 SPL. 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.

4.12 Mobile Broadcast Services (BCAST)

4.12.1 Introduction

Mobile Broadcast Services is a service enabler defined by the OMA in OMA-TS-BCAST_Service_Guide-V1_1-20100111-D [40]. This enables service/content providers to describe the services and content available (either free, subscription or one-off fee) and how to access them as Mobile Broadcast services either over a Broadcast Channel or over an Interaction Channel. From the user perspective the Service Guide can be seen as an entry point to discover the currently available or scheduled services and content, and to filter those based on their preferences.

Discovery of a Service Guide Function is performed using DNS SRV records, or optionally, using an FQDN derived from the IMSI, as specified in section 6.2.1 of OMA-TS-BCAST_Service_Guide-V1_1-20100111-D [40]. The domain name to use when deriving the FQDN from the IMSI is specified in section 2.3 of the present document.

4.13 The XCAP Root URI on Ut Interface for MMTEL/IMS profile for Voice and SMS (XCAP)

4.13.1 Introduction

XCAP is a protocol defined in IETF RFC 4825 [44], 3GPP TS 24.623 [45], and is part of the IMS profile for Voice and SMS documented in IR.92 [46]. This is used in manipulation of supplementary service configuration.

The XCAP Root URI is defined in IETF RFC 4825 [44], and is used to identify the XCAP Root, which is a context that contains all the documents across all application usages and users that are managed by the XCAP server.

The XCAP Root URI takes the following format: "http://xcap.domain"

The domain part of the XCAP Root URI is derived in accordance with 3GPP TS 23.003 [8], section 13.9.

4.14 RCS - Rich Communication Suite

4.14.1 Introduction

RCS as specified in the RCS specifications [48] is a simple and interoperable evolution to voice and text, which enables customers to send instant messages, video chat and exchange files in real time, that is rich call with content sharing, chat, file sharing etc. All functions are built into the address book of mobile devices. RCS focuses on the communications service aspects building on established interoperability principles within the mobile operator ecosystem providing service definition, functional description and technical realisation to develop new service packages for today's 'always-on' mobile users enabling seamless user experience.

The description and the use of the reserved subdomain names will be referenced in the RCS specifications where this domain can be used by all RCS specification versions.

4.15 Evolved Packet Data Gateway (ePDG)

4.15.1 Introduction

The Evolved Packet Data Gateway is defined in 3GPP TS 23.402 [29]. It provides PDN connectivity to the Evolved Packet Core (EPC) over untrusted non-3GPP IP access networks.

4.16 Network element self-configuration

4.16.1 Introduction

The concept of network element self-configuration is described in 3GPP TS 32.501 [50]. The network elements self-configuration can be applied e.g. for eNBs that is defined in 3GPP TS 36.300 [51].

4.17 EPC and GPRS coexistence

4.17.1 Introduction

When configuring the authoritative DNS server, a mobile operator supporting both GPRS and EPC roaming must consider that different DNS query procedures can be used in GPRS (A/AAAA-record queries) compared with EPC (S-NAPTR queries).

GSMA PRD IR.88 [52] provides further details on the DNS configuration requirements for different GPRS (2G/3G) and EPC coexistence scenarios.

4.18 MBMS Service Announcement Bootstrapping

4.18.1 Introduction

The method for bootstrapping for MBMS service announcement is described in 3GPP TS 26.346 [53]

4.19 5G Core (5GC)

4.19.1 Introduction

The 5G Core is defined in 3GPP TS 23.501 [37]. It provides support for a new and enhanced PS core networks to support NG-RAN (refer also to 3GPP TS 23.501 [37]) and serves as part of the 5G System (5GS).

SEPP IP discovery before N32 Handshake Procedure

The N32 handshake procedure is used between the SEPPs to mutually authenticate each other and negotiate the security mechanism to use over N32-f. More details about N32 handshake procedure in clause 5.2 of 3GPP TS 29.573.

Before the initiating SEPP starts the N32 handshake procedure towards the responding SEPP, the initiating SEPP should dynamically discover the IP address of responding SEPP via DNS. The necessary DNS queries for initiating SEPP to discover the responding SEPP IP and initiate the N32 handshake Procedure are described below.

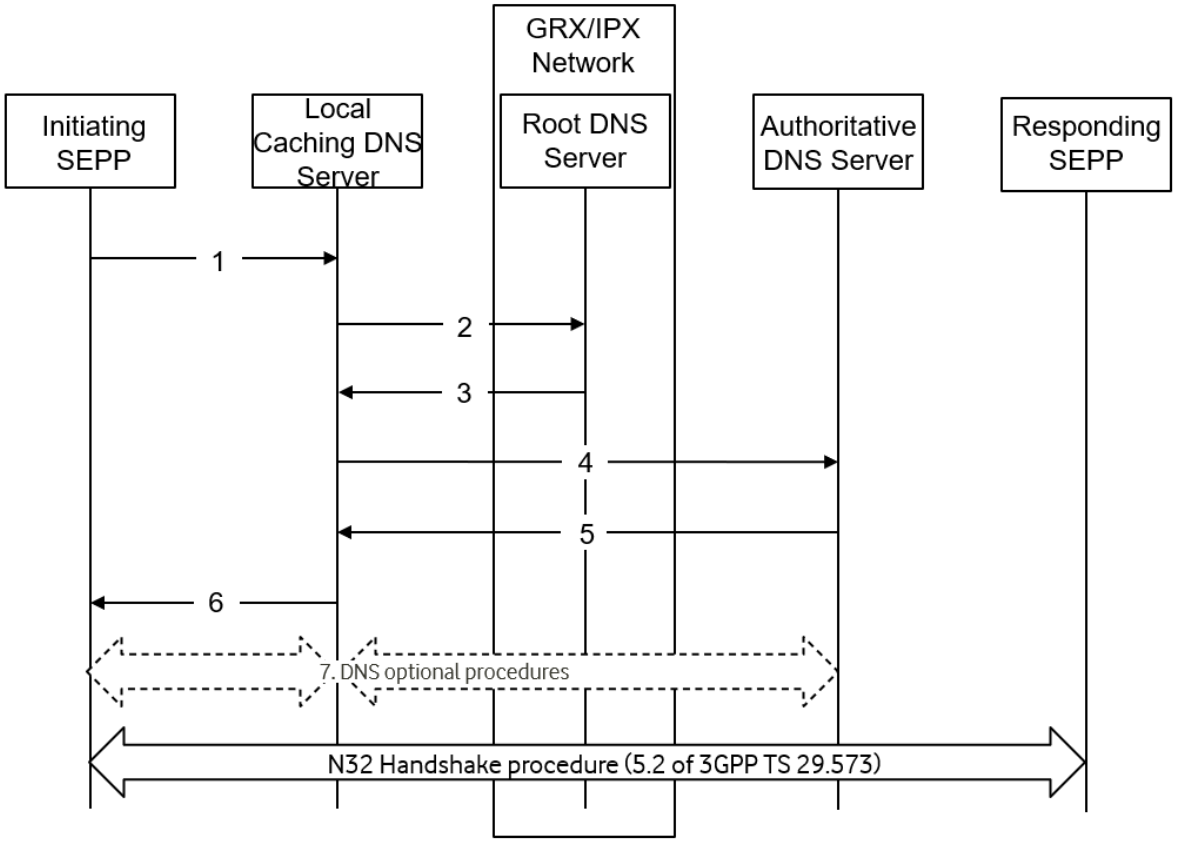

Figure 13: DNS message flow for Initiating SEPP discover responding SEPP IP

1. Before initiating SEPP starts the N32 Handshake Procedure it should query the Local Caching DNS to discover the responding SEPP IP. Initiating SEPP will send a recursive DNS Query 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 with the details of the responding SEPP 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 to resolve the DNS Query received on step 1.
5. The Authoritative DNS Server will resolve the DNS Query received on step 4 and will answer to the Local Caching DNS Server.
6. The Local Caching DNS Server replies to the DNS Query received from the initiating SEPP (in step 1) with the result obtained from the Authoritative DNS Server.
7. Depending on the received answer (step 6), some additional DNS queries could be required to discover the SEPP IP address. When discovered, the N32 handshake procedure could start (as described on section 5.2 of 3GPP TS 29.573).

4.20 Stand-alone NPN (SNPN)

4.20.1 Introduction

The SNPN is defined in 3GPP TS 23.501[37] as a 5GS deployed for non-public use and operated by an NPN operator not relying on network functions provided by a PLMN.

5 Processes and Procedures relating to DNS

5.1 Introduction

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

5.2 Existing domains/sub-domains on the GRX/IPX network and their Allocation

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

- .gprs
- .3gppnetwork.org
- .ipxsp.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 GSMA PRD NG.105 [56] for more information.

The domain names to be used by the 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 (for example routers, MMS Hubs, etc.), it is recommended to use ipxnetwork.org, see section 2.3.3. The ".grx" domain name also is commonly used, but should be reserved for legacy equipment on the GRX network. The sub-domains on “.grx” and “ipxnetwork.org” are agreed amongst other GRX/IPX Providers and assigned on a first come – first served basis in order to guarantee uniqueness (a good place to discuss this with other GRX/IPX Providers is the GRX Working Party).

5.3 Procedures relating to new domain names on the GRX/IPX network

New domain names may be added to the GRX/IPX network's DNS by any Service Provider or GRX/IPX Provider, in order to enable further services to be used on the NNI provided by the GRX/IPX network. This could be to allow such things as resolution of domain names used for national interconnect agreements, and so on. However, wherever possible, the existing sub-domains of the domain names specified in section 2.3.3 should be reused.

It is recommended that new domain names to be added to the GRX/IPX network's DNS are:

- a sub-domain of a Country Code Top Level Domain (ccTLD);

- registered/reserved on the Internet, in order to prevent any issues of ownership;
- not provisioned on the Internet (that is. not resolvable, at least no more than is absolutely necessary for example to retain ownership as per the rules of some ccTLD authorities);
- hosted in their own authoritative DNS server(s) on the GRX/IPX network, which is linked from the GRX/IPX Root DNS that is by using NS record entries (this eases administration of the new domain name and also prevents the GRX/IPX Root DNS becoming unmanageable); and
- used by an entity in addition to either their "mnc<MNC>.mcc<MCC>.3gppnetwork.org" domain name or "spn<SPN>.ipxsp.org" domain name, as specified in section 2.3.3 (amongst other things, this enables network node naming as per section 2.4).

The hosting authoritative DNS server(s) need to be reachable and respond to queries from all Service Providers and/or GRX/IPX Providers that need to resolve associated FQDNs. Ideally, access should be allowed to all entities on the GRX/IPX network, but only those who need to should have their queries properly serviced; the rest should be returned a standard DNS or ICMP error.

Care should be taken to not inadvertently force another entity who is denied access/resolvability of the domain name into (automatically or otherwise) trying to resolve it, including (but not necessarily limited to):

- by using only, the new domain name in general network node naming (network node naming should still be done as per section 2.4, using the domain names recommended therein); and
- by returning it in a NAPTR and/or SRV record (for example as used in IMS/SIP, ENUM, EPC).

For domain names that need to be resolvable on the UNI, the Internet DNS should always be used. By design, the GRX/IPX DNS provides resolution only for entities connected to the NNI.

5.4 GSMA Root DNS service and its access

5.4.1 GSMA Root DNS Service

The GSMA Root DNS Service provides authoritative naming management and address resolution mechanisms for the mobile industry that includes GRX Providers, IPX Providers and Mobile Network Operators. This translates into two main functions:

- Assignment and administration of domain names according this IR.67 specification
- Peering connection and DNS zone transfer services

In the SOA record of the root DNS a refresh timer of 900 seconds and a retry timer of 900 seconds is configured for the zones GPRS and 3GPPNETWORK.ORG. The secondary DNS servers will try to update the configuration once every 15 minutes.

he GSMA Root DNS Server is currently available at multiple locations to provide high availability service. GSMA reserves the right to add, relocate or decommission locations in

response with technological advancement, operational requirement and demand from the industry.

5.4.2 Access to GSMA Root DNS Service

For an applicant, who is limited to GRX Provider, IPX Provider which facilitates a connection from a Mobile Network Operator, or Operator requires the access to the service provided by the GSMA.

The application and accreditation process is required prior to its connection and is managed by the Manage Services team at GSMA. Applicant can contact the team by emailing rootdns@gsma.com to request access. An on boarding questionnaire will be provided for the applicant to provide information required for the application and accreditation process, and the service the applicant intend to utilize.

Once the applicant provides the necessary information, an accreditation process is conducted. If the verification is passed, the applicant will enter service agreement with GSMA and other terms as with associated parties, as deem necessary. The applicant also needs to settle any required payment. If any information is missing or incorrect, the applicant will need to resubmit the on boarding questionnaire.

If an application is either controversial or unsuccessful, it is escalated to GSMA staff for their consideration and their final decision. The applicant can appeal against a rejection by contacting the NG Director.

Once the application process completes, an account is created in the system with associated access credentials and security appliance to access the dedicated web portal. The peering and zone transfer between the applicant and the GSMA system can also be established and tested. As final step of the activation process the Participant's name servers are provisioned in the GSMA system.

Applicant can start submitting information to the GSMA DNS Service through the web portal. User can then can create, modify, delete or transfer domain names on behalf of Mobile Network Operators and its other customers according to the operational manual maintained by GSMA and its technology partner.

For any administrative, technical and operation issue regarding the service, including the document required for the accreditation process, please contact rootdns@gsma.com .

5.5 Delegation of sub-domains of "pub.3gppnetwork.org"

GSMA can delegate a sub-domain of pub.3gppnetwork.org to DNS of an MNO. The routine specified by GSMA operations, that the MNO needs follow to do this, consists of the following steps:

9. Identify MCC and MNC values for the MNO.

10. Identify CNAME record for the domain to be transferred.
    The CNAME record shall be in format of:
    <ABC>.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org

    where

acceptable values of <ABC> are defined in 2.3.4 (other values might be added as needed; see also NOTE 2 below)

<MNC> and <MCC> have to be replaced by respective values of the home network in decimal format, with a 2-digit MNC padded out to 3 digits by inserting a 0 at the beginning.

NOTE 1: For RCS configuration server CNAME record should be in format of http://config.rcs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org

NOTE 2: An operator may wish to delegate the entire mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org sub-domain.

11. **Create the Zone File** on the MNO's own NameServer/DNS with the CNAME record specified in step 2.

12. **Complete the Request Form** in Annex B.1 and - if required for your use of the sub-domain - **also the Letter of Authorization** in Annex B.2, and send both to GSMA at 3gppnetwork.org_delegation@gsma.com

NOTE 3: the Letter of Authorization format (Annex B.2) may need to be adapted dependent on your selected Certificate Body's requirements. If in doubt, please contact a Certificate Body of your choice, and obtain a necessary template to be filled in by MNO and signed by GSMA as the registrant of 3gppnetwork.org domain.

13. **GSMA will process the request, delegate the requested subdomain to MNO's DNS, and return a signed copy of the Letter of Authorization to MNO**.

NOTE 4: the typical maximum lead time to process the Request Form and sign the Letter is five (5) working days.

NOTE 5: the requesting MNO is responsible for submitting the Letter to their Certificate Authority.

Annex A Sample BIND DNS Configuration for GPRS

A.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.

A.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.

A.2.1 The "named.conf" file for a PLMN Primary 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 primary;
      notify no;
      file "primary/0.0.127.in-addr.arpa";
};    // only contains information about localhost.
/*
*     PLMN domain information
*/
zone "mnc091.mcc244.gprs" in {
      type primary;
      file "primary/mnc091.mcc244.gprs";
};
zone "sonera.fi.gprs" in {
      type primary;
      file "primary/sonera.fi.gprs";
};    // human readable operator id
zone "168.192.in-addr.arpa" in {
      type primary;
      file "primary/168.192.in-addr.arpa";
};
```

A.2.2 The "named.conf" file for a PLMN Secondary 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 primary;
      notify no;
      file "primary/0.0.127.in-addr.arpa";
};    // only contains information about localhost.
/*
*     PLMN domain information
*/
zone "mnc091.mcc244.gprs" in {
      type primary;
      file "primary/mnc091.mcc244.gprs";
};
zone "sonera.fi.gprs" in {
      type primary;
      file "primary/sonera.fi.gprs";
};    // human readable operator id
zone "168.192.in-addr.arpa" in {
      type primary;
      file "primary/168.192.in-addr.arpa";
};
};
```

A.3 Zone Configuration Files

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

A.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
```

A.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.
```

A.3.3 PLMN zone files

PLMN may configure both mnc.mcc.gprs and operator.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 host configuration.

A.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 primary/hosts
```

A.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 primary/hosts
```

A.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
```

A.3.5 The "168.192.in-addr.arpa" file

There may be several PTR records so that each name associated with and 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.
```

Annex B Forms for transfer of sub-domain of “pub.3gppnetwork.org”

B.1 Request form

Request Form for Transfer of sub-domain of pub.3gppnetworks.org		
IT Contact at MNO	Organisation:	
	Title:	
	Name:	
	Email:	
	Mobile Number:	
MNO Information	MNO Name:	
	MCC Value:	
	MNC Value:	
CNAME record for MNO	*CNAME record for provisioning domain for an MNO shall follow the format: **<ABC>.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org** where <MNC>=mnc value of MNO, <MCC>=mcc value of MNO, both values padded to 3 digits with a leading "0" if it is 2-digit long.	___.mnc___.mcc___.pub.3gppnetwork.org
ZONE file for CNAME	Is Zone File for the identified CNAME record created **on MNO's DNS servers?**	YES / NO
DNS Server Details (IP Address & FQDN)	Please provide MNO's DNS server details, where the ZONE file for CNAME record had been created.	Name / IP Address
Letter of Authorization	Please fill in and email "Letter of Authorization for the transfer of the domain" document to **3gppnetwork.org_delegation@gsma.com**	
Requestee	Organisation:	
	Title:	
	Name:	
	Email Address:	
	Mobile Number:	
	Date:	
	Signature:	

B.2 Letter of Authorization Template

Please fill out all required fields in the template and replace <ABC>, <MNC> and <MCC> as specified in 6.5.

This letter can be adapted as per MNO’s selected Certificate Body’s requirement. The letter must be signed by GSMA.

<Certificate Organisation Name>

<Contact Name at Certificate Organisation>

<Certificate Organisation Address>

<Certificate Organisation Fax Number/Email address>

Date: <Please type date>

To whom it may concern,

Dear Sir/Madam,

Re: Domain Authorization Letter

I confirm that:

Organization enrolling for the Digital Certificate set out below is: <Please type your MNO's full company name here> ("Certificate Applicant")

Domain to be included in the certificate is:

<ABC>.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org ("Domain")

Registrant of the Domain is: GSM Association ("Registrant")

Digital Certificate is the certificate relating to the Domain.

I am employed by the Registrant and am duly authorized to sign this Domain Authorization Letter and to deal with all matters related to the registration of the Domain.

Certificate Applicant desires to install the Digital Certificate on its web server(s) for the domain and ultimately to enable secure communications with its users.

Registrant acknowledges that it has granted the Certificate Applicant the right to use the Domain as a common name in the Digital Certificate request referenced above and to otherwise use the Domain in connection with its business.

Regards,

Full Name: Javier Sendin

Job Title: Technical Director

Organization: GSM Association

Signature:_____

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1.0	14 October 2004	First draft – skeleton.	-	Nick Russell, Vodafone
0.2.0	10 May 2005	Second draft, with most sections filled in, or at least with place holders.	-	Nick Russell, Vodafone
0.2.1	11 May 2005	Changed the underlying Word template to the new one.	-	Nick Russell, Vodafone
0.3.0	15 November 2005	Enhancements of ENUM section, including addition of Number Portability in ENUM, plus minor corrections and update of template.	-	Nick Russell, Vodafone
0.9.0	16 December 2005	Final draft for publication; contains only minor corrections to formatting since previous version.	-	Nick Russell, Vodafone
1.0	16 December 2005	Approved for publication.	DAG	Nick Russell, Vodafone
1.1	26 January 2006	Minor formatting corrections.	IREG	Nick Russell, Vodafone
1.2	4 April 2006	Moved in the DNS information from IR.34, ENUM section updated with the agreements made in 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".	IREG Packet	Nick Russell, Vodafone
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.	IREG Packet	Nick Russell, Vodafone
2.0	30 April 2007	Addition of the "No Root" ENUM architecture, plus some other miscellaneous corrections.	DAG	Nick Russell, Vodafone
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".	IREG Packet	Nick Russell, Vodafone

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
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.	IREG Packet	Nick Russell, Vodafone
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.	DAG and IREG Packet	Nick Russell, Vodafone
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.	IREG Packet	Nick Russell, Vodafone
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).	IREG Packet	Nick Russell, Vodafone

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
3.3	21 July 2009	Implementation of the following CRs: 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. 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".	IREG Packet	Nick Russell, Vodafone
4.0	10 December 2009	Implementation of CR #21 (Major): To document the lessons learned after the ENUM trial, and to make the whole specification of the GRX/IPX Carrier ENUM take a more top-down approach. New template also applied.	DAG #64	Nick Russell, Vodafone
4.1	3 March 2010	Implementation of CR #22 (Minor): addition of "bcast" sub-domain to "mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org". Minor editorial corrections also made, including clarification on a zero being inserted on the left side of any 2 digit MNCs used in domain names e.g. 15 becomes 015.	IREG Packet (email approval)	Nick Russell, Vodafone
5.0	21 July 2010	Implementation of CR#23 (Major): Updates to domain names used on the GRX/IPX network and inter-SP links	DAG #71	Nick Russell, Vodafone
5.1	13 August 2010	Implementation of the following CRs: CR #24 (Minor): Support of IP versions in DNS CR #25 (Minor): ENUMservice field value for SIP-I/PVI	IREG Packet (email approval)	Nick Russell, Vodafone

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
6.0	1 December 2011	Implementation of CR#26 (Major): Addition of new '.ipxuni' domain name and sub-domain name used for "well known" XCAP Root URI to "mnc<MNC>.mcc<MCC>.ipxuni.3gppnetwork.org"	DAG#86	Gert Öster, Ericsson
7.0		Implementation of the following CRs - CR #28 (Major): Addition of new subdomain for RCS/RCS-e as “rcs.mnc>mnc>.mcc<mcc>.pub.3gppnetwork.org” CR #29 (Major): Removal of sub domain name for the “XCAP root URI” from the “ipxuni” domain name and adding a new sub domain as xcap.ims.mnc<mnc>.mcc<mcc>.pub.3gppnetwork.org, and adding a new subdomain for bootstrapping when ISIM is used as bsf.ims.mnc<mnc>.mcc<mcc>.pub.3gppnetwork.org,	IREG#62 DAG#92	Gert Öster, Ericsson

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
8.0	23/11/2012	Implemetation of the Following CRs • CR 29 (Major) To briefly describe how GRX/IPX providers can subscribe to the RootDNS and access its services • CR 30(Major) Adding the possibility to provide Non-authoritative final ENUM responses for ported-out users based on Legacy Number Portability Information • CR 31(Major) Adding examples of Number portability solutions allowing the IPX/GRX ENUM to work for countries without a national Tier-1 ENUM DNS server, as requested by IWG IMQ and RCS-e. • CR 32(Major) Removal of text not considering that Local Breakout for it specified method for IMS roaming in relation to VoLTE • CR 33(Major) Adding a further example of ENUM NAPTR records with regular expressions where part of the result shall be substituted by the “original” E.164 number. • CR 34(Major) To show that a Service provider does not need to provide all data for domain names the Service provider is authoritative for one DNS but that they may choose to imply multiple levels of Authoritative DNSs where a First level may refer to the Second level Authoritative DNS severs.	IREG#63 DAG#99	Gert Öster, Ericsson

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
9.0	21/10/2013	Implemtation of the following CRs • CR1001 (Major) To add the “ipxnetwork.org” TLD for IPX providers that need a subdomain to identify their equipment and realms. • CR1002 (Major) To add the subdomain used for interworking untrusted non-3GPP access networks to the EPC using the ePDG. • CR1003 (Major) to clarify that text on provisioning in clause 5.4.3 only relates to ENUM and not HSS. • CR1004 (Major) To describe the routine for delegation of "pub.3gppnetwork.org" sub-domains • CR1005 (Major) To provide information on DNS resolution when IR.21 information is used. • CR 1006 (Major) To correct the e-mail address for Root DNS questions to reflect the new “gsma.com” e-mail address	IREG#65	Gert Öster, Ericsson
10.0	24/04/2014	Implemetation of the following CRs • CR 1007 (Major) To add the subdomain for the “OAM System Realm” that can be used for IP autoconfiguration services e.g. in case Self-Organizing Networks (SON) as defined by 3GPP • CR 1008 (Major) To provide guidance on naming of IMS Nodes, and to inform where guidance on EPC node name can be found	IREG#66	Gert Öster, Ericsson

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
11.0	16/04/2015	Implemetation of the following CRs • CR 1009 (Major) To add pointers to IR.88 for DNS configuration requirements in various 2G/3G and LTE coexistence scenarios. • CR 1010 (Major) To add the subdomain for “Bootstrapping of MBMS service Announcements” • CR 1011 (Major) To correct e-mail address to Delegation of “pub.3gppnetwork.org”	NG#01	Gert Öster, Ericsson
12.0	01/02/2016	IR.67 CR1012 Resolver architecture for service aware IPX	NG	Frederic Paquette Tata Communications
13.0	06/09/2016	CR1013 Sub-domain for ePDG selection with DNS-based Discovery of Regulatory requirements CR1014 SOA Refresh Timer alignment on root DNS	NG	Frederic Paquette Tata Communications
14.0	21/11/2016	IR.67 CR1015IR.67 CR1015 DNS Guidelines for Service Providers and GRX and IPX Providers	NG	Frederic Paquette Tatacommunications
15.0	27/07/2017	IR.67 CR1017 DNS Guidelines for service providers – removal of ENUM content now in NG.105	NG	Frederic Paquette Tatacommunications
16.0	09/06/2020	CR1018 Introducing New Sub-domain for IWK with SNPN CR1019 Clean-up of References	NG	Sajid Soormally (Nokia) Wayne Cutler (GSMA)
17.0	21/10/2020	CR1020 NNI Interworking - singledual registration IMS cores	NG	Wayne Cutler (GSMA)
18.0	06/05/2021	CR1021 DNS Guidelines for Service Providers and GRX and IPX Providers	NG	Chris Li (GSMA)
19.0	23/11/2021	CR1022 SEPP FQDN resolution before N32 Handshake Procedure	NG	Eddy Goffin (Orange)

Other Information

Type	Description
Document Owner	NG Packet
Editor / Company	Eddy Goffin (Orange)

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

Your comments or suggestions & questions are always welcome.