ETSI TS 184 010 V3.1.1 (2011-08)

Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN);
ENUM & DNS Principles for an Interoperator IP backbone network

Reference
DTS/TISPAN-04015-NGN-R3

Keywords
DNS, ENUM

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document captures a set of assumptions that would help to define a set of ETSI requirements and a possible architecture for an IPX and in particular the ENUM & DNS aspects. It explains why an IPX may prove useful and provides guidelines which would apply to its use as a private, inter-operator IP backbone for ETSI TISPAN compliant networks. It is important that all potential Carriers' IPX implementations, ongoing in the market, should take account of ETSI NGN standards and specifications in order to ensure different "NGN implementations" may interoperate together.

The present document analyses a particular case of numbering and naming resolution for use by NGN Communications Providers when providing indirect interconnection as specified in ES 282 001 [18] and covers the need for a standard solution to address numbering and naming resolution implemented through an ENUM/DNS solution for this particular case.

A TISPAN IPX does not currently exist. It should not be assumed from the present document that ETSI would look to set in place an ETSI specific IPX, but the detailed requirements and approach set out within this document will ensure that ETSI is able to assess the options in moving forward. No decision on the way forward has yet been taken. However within ETSI there is strong recognition of the benefits that can be gained from adopting a combined approach with other parties providing the requirements specified by ETSI TISPAN can be accommodated.

The present document would also allow an assessment to be made against the approach that is currently planned to introduce an IPX by the GSMA.

Whilst the document details possible sub-domains that an operator may use they should only be viewed as possible examples.

The present document does not put constraints on commercial models.

The present document describes an Infrastructure ENUM that need not to be based on an Interoperator IP backbone, but it is managed by a confederation of operators also on the basis of a distributed architecture. As a consequence the applicability of the references to the Interoperator IP backbone network should be evaluated based on the operator's ENUM implementation.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] IETF RFC 1035: "Domain Names - Implementation and Specification".

[2] IETF RFC 6116: "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[3] IETF RFC 3403: "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database".

[4] IETF RFC 3404: "Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI)".

[5] IETF RFC 3263: "Session Initiation Protocol (SIP): Locating SIP Servers".

[6] IETF RFC 2782: "A DNS RR for specifying the location of services (DNS SRV)".

[7] ETSI TS 129 421: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; TISPAN; NGN Release 1; Endorsement of 3GPP TS 29.162 Interworking between IM CN Sub-system and IP networks (3GPP TS 29.421)".

[8] ETSI TS 184 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements and usage of E.164 numbers in NGN and NGCN".

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

[10] IETF RFC 3966: "'The Tel URI for Telephone Numbers".

[11] IETF RFC 4355: "IANA Registration for Enumservices email, fax, mms, ems, and sms".

[12] IETF RFC 3764: "enumservice registration for Session Initiation Protocol (SIP) Addresses-of-Record".

[13] IETF RFC 4769: "IANA registration for an ENUM service containing Public Switched Telephone Network (PSTN) Signalling Information".

[14] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[15] IETF RFC 2671: "Extension Mechanisms for DNS (EDNS0)".

[16] IETF RFC 5358: "Preventing Use of Recursive Nameservers in Reflector Attacks".

[17] IETF RFC 5452: "Measures for Making DNS More Resilient against Forged Answers".

[18] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] IETF RFC 4282: "The Network Access Identifier".

[i.2] GSMA IR67 version 3.1 (Jan 2009).

[i.3] ETSI TR 184 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Portability of telephone numbers between operators for Next Generation Networks (NGNs)".

[i.4] IETF RFC 3824: "Using E.164 numbers with the Session Initiation Protocol (SIP)".

[i.5] ETSI TR 184 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Types of numbers used in an NGN environment".

[i.6] ETSI TR 184 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Infrastructure ENUM Options for a TISPAN IPX".

[i.7] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN-SEC); Threat, Vulnerability and Risk Analysis".

[i.8] ETSI TR 187 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity imanagement and their resolution in the NGN".

[i.9] ETSI TS 184 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Interconnection and Routeing requirements related to Numbering and Naming for NGNs; NAR Interconnect".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

carrier of record: Service Provider to which the E.164 number was allocated for end user assignment, by the National Regulatory Authority (NRA) or the International Telecommunication Union (ITU), for instance, a code under "International Networks" (+882) or "Universal Personal Telecommunications (UPT)" (+878)

NOTE: In the case that the number is ported the carrier of record maybe changed due the national number portability (NP) policies. It is understood that the definition of carrier-of-record within a given jurisdiction is subject to modification by national authorities.

Communications Provider (CP): any entity providing communications services to 'End Users' and using a network to provide routeing capabilities

delegation: when a part of a zone is maintained separately, it is delegated to a new nameserver that will have authority of that part of the domain namespace

NOTE: The original zone will have the nameserver (NS) record for the delegated domain and the new sub-zone will have a new Start Of Authority (SOA) record.

DNS Client: See "DNS Resolver".

DNS Resolver: also known as a "DNS Client", this is an entity that is attempting to resolve a given domain name to an address or vice versa

NOTE: Usually the DNS Resolver is connected to a local DNS caching server that performs the DNS look-ups on behalf of the DNS Resolver. Application programs use function calls, such as 'gethostbyname', to find the IP address representing a domain name. The name may be specified either as a Fully Qualified Domain Name (FQDN) or only partially. In the latter case, the DNS Resolver appends (a) configured local domain name(s) at the end of the name.

DNS Server: can be a Nameserver, a Local Caching DNS Server or both

domain name: consists of two or more labels separated with a dot ('.') character

NOTE: It starts from the least significant domain on the left, and ends with the most significant domain (or top-level domain) on the right. This naming convention naturally defines a hierarchy.

interoperator IP backbone provider: provider of a transit network or transit services that does not offer "services" to end users, but offers pure IP connectivity or session-based service interconnection to Communications Providers

nameserver: takes care of DNS Queries sent by DNS Resolvers

NOTE: The query is answered by using locally stored information (either configured locally or cached from a previous query result), by requesting the information from another DNS Server, or by providing the DNS Resolver with the details of another DNS Server to query. One Nameserver can serve (i.e. be authoritative for) several domains. There may also be several Nameservers serving one domain (Usually one Nameserver is the Primary and the other/rest are Secondaries. The Seconedary Namersever request authoritative DNS data from the Primary Nameserver due to a configured DNS data update process.).

Shared ENUM Infrastructure: Inter-operator infrastructure according to ENUM technology as defined in RFC 6116 [2], used by the originating or an intermediate network to map a specific E.164 number into a URI that identifies a specific entry point into the network actually serving that specific E.164 number

NOTE: Carrier ENUM infrastructure is different from user ENUM infrastructure where the end-user may register his E.164 number to be associated with a URI of his desire.

zone: DNS is a distributed database that contains information of each domain name

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

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
ATM	Asynchronous Transfer Mode
BGCF	Border Gateway Control Function
BGF	Border Gateway Function
BGP	Border Gateway Protocol
CC	Country Code
CP	Communications Provider
CSCF	Call Session Control Function
DNS	Domain Name System
ENUM	Telephone Number Mapping
FQDN	Fully Qualified Domain Name
GSMA	Global System for Mobile Communications (GSM) Association
GTP	GPRS Tunnel Protocol
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
I-CSCF	Interrogating - Call Server Control Function
IDNA	Internationalized Domain Names for Applications
IMS	IP Multimedia sub-system
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPX	IP Packet eXchange
MGCF	Media Gateway Control Function
MMS	Multimedia Messaging Service
NAI	Network Access Identifiers
NAPTR	Naming Authority PoinTeR
NGN	Next Generation Network
NP	Number Portability
NS	Name Server
P-CSCF	Proxy - Call Service Control Function
PLMN	Public Land Mobile Network
QoS	Quality of Service
RTP	Real-Time Transport Protocol
S-CSCF	Server - Call Session Control Function
SEG	Security gateway
SIP	Session Initiation Protocol
SIP(S)	Session Initiation Protocol (Secure)
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SOA	Start Of Authority
TCP	Transport Control Protocol
UDP	User Datagram Protocol
UPSF	User Profile Server Function

URI	Uniform Resource Identifier
VPN	Virtual Private Network

4 Description and Assumptions

4.1 Introduction

DNS/ENUM can be used in an ETSI TISPAN compliant environment to support E.164 number resolution and number portability.

Due to TR 184 003 [i.3] DNS/ENUM can be used to support number portability between operators of NGNs by using a shared infrastructure or operator local infrastructure (non-root approach). The present document describes the usage of DNS/ENUM in a shared infrastructure. Nevertheless some general DNS/ENUM protocol requirements are also applicable in a provider local DNS/ENUM infrastructure.

An inter-operator IP backbone network provides a method of supporting interconnectivity of IP based services and interconnection between different IMS based IP networks. 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 operators have all the necessary information to hand to ease configuration of their DNS servers that are connected to the Interoperator IP backbone network for each IP based service provided.

The present document consists of an overview of DNS in relation to the successful interworking of fixed network services, the configuration of DNS servers, and procedures that would assist in the configuration and usage of domain names and DNS Servers within an inter-operator IP backbone network.

This network is viewed as a key enabler for the support of full interconnectivity between communications providers.

Whilst competing, Communications Providers deploying Next Generation Networks have the common objective of delivering traffic to each other in a profitable and cost effective manner. This will enable their customers to realise the full value of these services and comply with regulatory conditions that are applied to these services/networks. The common protocol for these networks is IP.

Two basic possibilities exist for Interconnection between communication providers on the network layer as specified in ES 282 001 [18]:

- Direct connection between two NGN Communication Providers on a bilateral basis (e.g. often using leased lines and VPN connectivity).
- Indirect Connection via an Interoperator IP backbone network which facilitates interconnectivity for Communication Provider networks. Such indirect interconnection is isolated from the Internet. Security rules are defined to prevent unintended access to it.

These two options are not mutually exclusive and it is a commercial decision which method Communications Providers use. The benefits of connectivity via an IPX include the ability to reach different interworking partners across the globe via one connection.

These two options are not mutually exclusive and it is a commercial decision which method Communications Providers use. The benefits of connectivity or "session-based" services via an Interoperator IP backbone provider include the ability to reach different communication providers using a single network connectivity agreement.

To ensure interoperability of all Communications Providers connected to the Interoperator IP backbone network will need to adhere to a set of common rules. These include rules regarding architecture functionalities, protocols, numbering and IP addressing resolution mechanisms, routeing, security, QoS, etc.

The Interoperator IP backbone provider does not offer "services" to end users, but offers pure IP connectivity or session-based service interconnection to Communications Providers, and may provide transport functions required to enhance that interconnection, for example ENUM & DNS functionalities, numbering resolution mechanism, routeing capabilities and, if required, Triggering functionalities (see TS 184 006 [i.9]).

Direct Connectivity between Communications Providers is a viable alternative defined in ETSI TISPAN NGN standards and specifications, but it is outside of the scope of the present document.

The IPX is isolated from the Internet and security rules are defined to prevent unitended access from it.

An interoperator IP Backbone network could be operated by any qualified party. The IP backbone network is expected to support Quality of Service features end to end, which requires parties involved in the transport of a service up to the terminating user equipment, to be bound by service level agreements.

4.2 DNS as used on an Interoperator IP backbone network

The proposed approach requires a specific a DNS architecture.

The Master Root DNS node(s) that Interoperator IP backbone providers see are known as "Slave Roots". DNS Servers and are commonly provisioned by Communication provider. However, these Slave Root DNS Servers can be provisioned by operators themselves if they so wish. Each Slave Root DNS Server is synchronised with a "back-end" Root DNS Server known as the "Master Root". This is known as a "Zone Transfer" and ensures that the data is the same in all interconnected Communication Providers. Figure 1 depicts this.

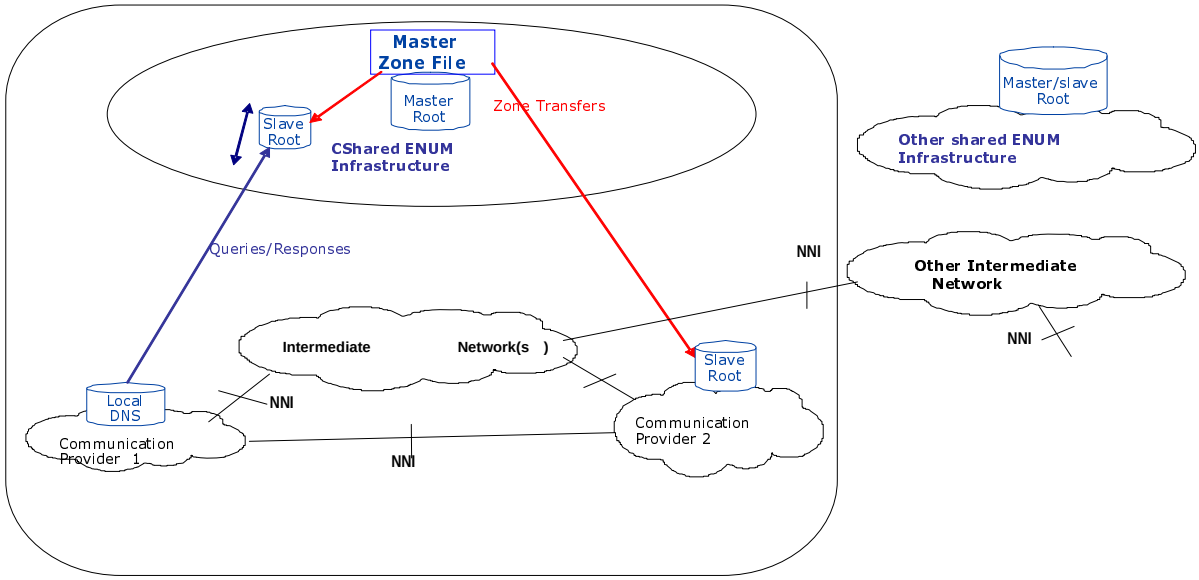

Figure 1: Backbone Architecture

The ENUM&DNS is completely separate and autonomous from the DNS infrastructure of public Internet to be managed for QoS, availability, security, as required.

Communication Providers will define a bilateral agreement with the Interoperator IP backbone network provider to manage access procedures to the ENUM&DNS servers for the numbering, naming and addressing resolution.

The access to the Inter-operator IP Backbone network infrastructure and functionalities (for instance to ENUM/DNS, etc.) and related data population is limited to Communication Provider interconnected with specific Inter-operator IP backbone network eventually also in charge for NAR resolution and routeing determination.

The data in the Master Root DNS Server is known as the Master Zone File. Access to the master Zone file will only be available to parties authorised to perform that role by the Interoperator IP backbone providers/Communications Providers. The population of the data that goes into the Master Zone File has a number of sources, mainly from Communications Providers, and Interoperator IP backbone providers acting on their behalf. It also needs to be policed and validated to ensure integrity of the sub-domain allocation and usage. Communications Providers can also query the root directly.

Figure 2 showing the overall process architecture depicts the administration of the name server information that is required to populate the master root and slave servers.

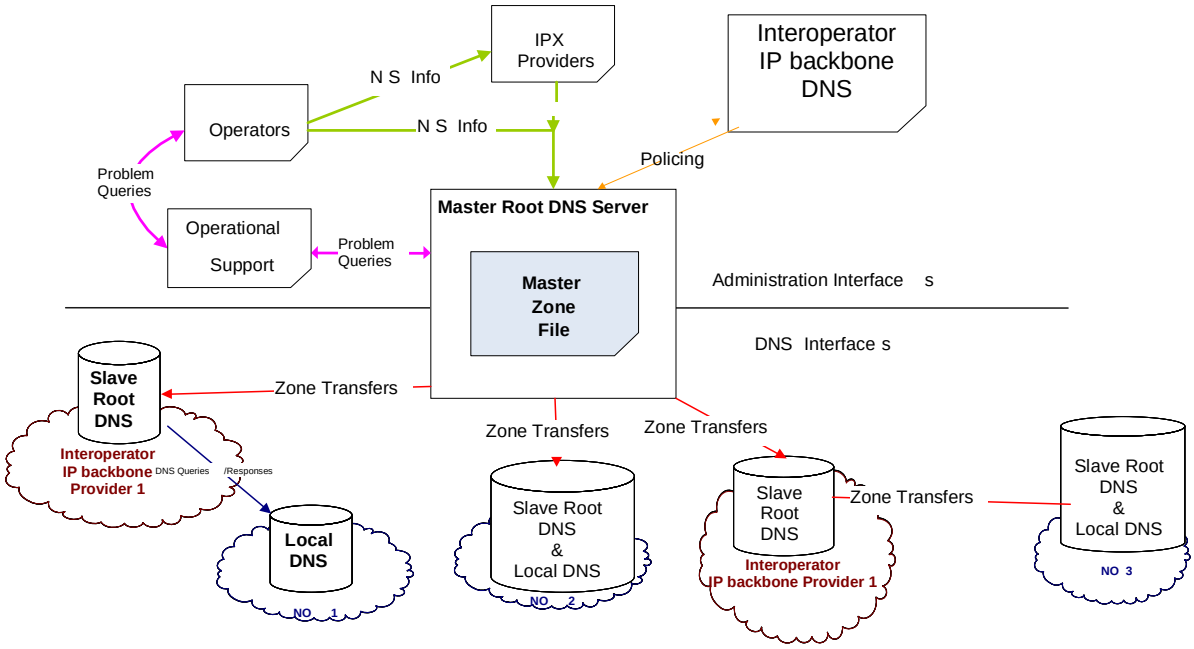

Figure 2: Overall Process Architecture

4.3 IP Connectivity and Service-oriented interconnection services

The Interoperator IP backbone network may permit three connectivity options:

- Transport-Only Connectivity
- Bilateral Service Transit Connectivity
- Multilateral Service Transit for pure IP connectivity or "session-based" services

Transport only connectivity

Communication Providers interconnected indirectly using the Inter-operator IP backbone network with guaranteed QoS. This model is not service aware and it can be used to transport general IP traffic between two Communications Providers (provided compliance with security requirements is maintained).

Bilateral Service Transit connectivity for pure IP connectivity or "session-based" services

A bilateral agreement between Communications Providers interconnected indirectly for specific 'session based' services using as a transit operator the Interoperator IP backbone provider with guaranteed QoS. This model provides the opportunity to include service based interconnect charging in addition to the transport charging of the transport only model.

Multilateral service transit for pure IP connectivity or "session-based" services

Communications Providers interconnected indirectly for specific "session-based" services using as a transit operator the Inter-operator IP backbone network with guaranteed QoS. In this case the transit service is a multilateral one among Communication Providers.

In order to support interworking of IP services, cascade interconnect billing and multilateral interconnect service hub (e.g. IP service Proxy) working would be required.

Considered purely from a connectivity point of view the required IP network between different operators might take different forms via the public Internet (with VPN) or direct leased line such as Frame relay or ATM. However Inter-operator IP backbone network shall be compliant with ETSI TISPAN standards for NGN architectures, protocols, interconnection, numbering, naming, addressing resolution and routing, etc., utilizing, to enable QoS, availability, reliability, security, etc., a dedicated inter-operator NGN "IP-based" network, that is totally separate from the public Internet.

Communication providers should evaluate the alternatives for direct interconnection or indirect interconnection and choose the most appropriate. Issues such as QoS, security, control of interworking networks, overall reliability and issuing of new network features such as support for ENUM/DNS are easier handled within direct or indirect interconnections, being an operators' managed interconnection architecture. The benefits of this approach are more clearly assessed in TR 184 008 [i.6].

4.4 Requirements for the Interoperator IP Backbone network

4.4.1 General Issues

Considered purely from a connectivity point of view the required IP network between different operators might take different forms via the public Internet (with VPN) or direct leased line such as Frame relay or ATM. However the preferred ETSI approach is similar to the model used by 3GPP networks, utilizing a dedicated inter-operator IP network, that is totally separate from the public Internet.

Using an inter-operator IP backbone network to carry IMS traffic would be less onerous than building direct connections between each and every IMS network in the world. As the number of operators increases, such an approach clearly does not scale without the introduction of 'transit IPX carriers' that would result in some form of carrier based IP backbone network.

Communications Providers should evaluate the alternatives for IMS interworking and choose the most appropriate. One approach would be to use the inter-operator IP backbone network as the default routing choice but where traffic is high (typically between national carriers) a leased line or IP-VPN may be more cost effective. As the IP routing is separate from the physical topology, multiple physical connections may co-exist. In practice operators may have several physical interconnection links: leased line for national traffic, IP-VPN for medium volume and an inter-operator IP backbone network for all others. The DNS system will resolve the destination domain to an IP address that will be routed over the appropriate link.

Issues such as QoS, security, control of interworking networks, overall reliability and issuing of new network features such as support for ENUM are easier handled inside an inter-operator IP backbone network than when using public internet to relay IMS traffic between operators. This is due to the fact that the inter-operator IP backbone network can be considered to be a closed operator controlled network unlike public Internet, which is totally open for everyone. The benefits of this approach are more clearly assessed in TR 184 008 [i.6].

4.4.2 Top level requirements

NGNs will not emerge at the same rate in all countries due to market differences, economic drivers and technological differences. It's therefore essential that any proposal to establish an Interoperator IP backbone network takes full account of the variable timeframe for evolution from country to country. Whilst connectivity at the IPX level can be facilitated in a number of ways, different countries are likely to require different connectivity implementations within their national environment, particularly as national databases will already be implemented or planned, closely coupled with different national number portability implementations. The rapid introduction of NGNs must not be hampered by the need to change such arrangements in order to facilitate connectivity at the Interoperator IP backbone level.

There will also be an overriding need to ensure compliance with applicable national regulatory requirements and agreed processes, procedures and operating practices which are adopted at the national level in order to facilitate national number portability.

Interoperator IP backbone network operators should:

- Comply with any IP addressing guidelines set within ETSI, comply with DNS guidelines as specified in the present document
- Have IPv4/IPv6 routing capability

- Distribute all valid known routes to Communications Providers
- Control which routes a Communications Provider can advertise to the network
- Offer interconnectivity to other inter-operator IP backbone networks (IPX peering)
- Comply with agreed Service Level Agreements
- Conform with security requirements laid out in TS 187 001 [14], TR 187 002 [i.7] and TR 187 010 [i.8]
- Support end-to-end QoS requirements, described in any agreed SLA
- Create the agreements required with other IPX Providers to fulfil the end to end SLA
- Maintain required traffic separation e.g. invoke mechanisms to ensure the underlying IPX network is not reachable by end users

4.4.3 IP Version Issues

IMS core systems & terminals can be either IPv6, IPv4 based or dual stack. General usage of IPv4 and IPv6 regarding IMS detailed in TS 129 421 [7].

4.4.4 IP Addressing

Internet routers should not be able to route to the IP addresses advertised to the Inter-ServiceProvider IP Backbone. The IP Backbone Providers and Service Provider networks shall be totally separated from public Internet, from an IP routing and connectivity perspective.

Currently, Inter-Service Provider IP Backbone networks use IPv4 addressing but it is assumed that plans to introduce native IPv6 addressing will emerge in the foreseeable future. Support of IPv6 by native transport or tunnelling the IPv6 traffic over IPv4 between Communications Providers where required are options that could be considered.

Both IP Backbone Providers and Service Providers who employ IPv6 in their network should assume full responsibility for Communication Providers that deploy IPv4.

An IP Backbone Provider is responsible for the denial of IP spoofing attacks originated by its Service Provider customers, i.e. only traffic from valid IP address ranges is allowed to flow to other customers or other IP Backbone Providers.

4.4.5 DNS data transport

Providers shall:

- support the transport of DNS queries and responses require to facilitate routeing
- provide transport of ENUM queries and responses to support any identified services [2]
- support the transport of DNS and ENUM queries and responses via IPv4 and IPv6, UDP and TCP
- support the differentiation between different DNS domains and ENUM domains regarding the IPv4/IPv6 addresses of the DNS caching servers to provide advanced security as well as scalability measures

4.4.6 DNS/ENUM client

An DNS/ENUM client which sends DNS/ENUM queries and receives DNS/ENUM answers (e.g. S-CSCF, BGF, DNS) resolver should be supported by the following requirements:

- must support the DNS/ENUM basic functional standards RFC 1035 [1], RFC 6116 [2], RFC 3403 [3], RFC 2782 [6];
- in the case of using UDP as transport protocol the DNS/ENUM client must support RFC 2671 [15] to extend DNS the limitation of 512 octets in size when DNS protocol messages are sent over UDP;

- to ensure a basic level of security the DNS/ENUM client must support RFC 5358 [16] and RFC 5452 [17].

4.4.7 Security Issues

In order to maintain proper level of security within the Interoperator IP backbone network certain requirements for operators and backbone providers should be taken into account.

It is strongly recommended that operators should implement firewalls adjacent to Border Gateways. Generally operators should allow only routing information (BGP), GTP traffic, signalling, DNS, SMTP and SIP(S) traffic. However, also traffic related to IMS user plane (such as RTP and HTTP) should be allowed due to IMS interworking. Therefore, due to potentially numerous new protocols introduced by IMS interworking, there should not be any kind of restrictions on the used protocols or port numbers with in the inter-operator IP backbone network.

It is important to note that also firewalls must support IPv6 when IPv6 is used.

Security gateways (SEGs) should be used at the border of an operator network.

IPSec tunnels between CSCFs are not needed, if the Interoperator IP backbone network itself provides comparable level of security such as IPSec tunnel.

SEG should be responsible for enforcing security policies for the inter-network traffic; all incoming & outgoing IP traffic would then need to pass through it.

Usage of IPSec is mandatory if connectivity with the public Internet occurs, i.e. IMS connection must always be secured at some level. If IPSec is used in inter-PLMN IMS connections, it is recommend using the common IPSec parameter set in order to reduce the number of options.

Above all, operators should realize that the actual security level of the whole IMS system depends on much more than just securing the transportation between CSCFs. This is done on an operational service level, where it is decided how these services are deployed and used. ETSI TISPAN IPX itself is nothing else than just IP bearer network, which does not provide any kind of actual security features besides the fact that no outsider should be able to access the a Interoperator IP backbone network.

Consideration with TS 187 001 [14], TR 187 002 [i.7] and TR 187 010 [i.8].

Security issues related to IMS services, such as Peer-to-Peer traffic, are for further study.

4.4.8 Quality of Service

An SLA will define a service specification between a communications Provider and an IP backbone provider. The involved parties may agree an IP QoS profile that should be supported over the connection and this extends to whole Inter-Service Provider IP backbone network comprising IP backbone Providers maintained networks and routers.

Service guarantees should be defined and the backbone provider should take responsibility for providing measurements and also permit the Communications Provider to analyse the results.

4.4.9 Service Related Issues

Different end-user services used in IMS have different requirements. The actual IMS based services and their requirements are not within the scope of the present document.

5 DNS and ENUM for the Interoperator IP backbone network

5.1 Naming and Addressing within IP Multi-media core network Sub-system (IMS)

IMS subscribers are addressed by SIP URIs and/or E.164 numbers represented as Tel URIs. For E.164 numbers, ENUM can be used in IMS as the means to convert an E.164 number into a SIP URI.

TS 184 011 [8] provides requirements and describes the manner the E.164 numbers shall be used within NGN and NGCN environments.

For resolving SIP URIs to SIP Servers (see RFC 3263 [5]), support of the SRV Resource Record functionality (as defined in RFC 2782 [6]) is needed in operator's DNS servers.

5.2 E.164 Number Translation (ENUM)

E.164 numbers cannot be used on their own for addressing in IP based networks. The Internet Engineering Task Force has defined a mechanism for converting E.164 numbers to addresses relevant to services which the user wishes to use and which are accessible through means using IP. RFC 6116 [2] defines storing E.164 numbers and services related to a particular number using DNS. This mechanism is known as ENUM.

5.3 Shared ENUM Infrastructure for Inter-operator IP backbone Networks

NGN architecture requires a name, number, addressing and routeing capability to be in place to facilitate the resolution of numbers, names and addresses to facilitate connectivity both within, and between networks. The ENUM protocol as defined within RFC 6116 [2] provides a method of achieving that.

There is a need to process dialled digits that have been entered by the originating party in order to identify a called party or service, these digits are transmitted as a dial string to the NGN. To facilitate the routeing of calls the dial string is analysed and inserted in the ENUM application in the international format (an E.164 number) e.g. +44nnnnnnnnnn for processing within Shared ENUM Infrastructure. The output from the ENUM resolution process would be an address in the form of a SIP URI or tel URI, depending on whether then called part number can be reached on an IP based network or the PSTN.

Within ETSI TISPAN Shared ENUM Infrastructure will be provided using a private DNS as set out in TR 184 008 [i.6] i.e. no direct connection to the public Internet. It will be transparent to users and not reachable by users of the Internet. Data can only be read by those that share that specific DNS architecture and related servers. The routeing data is populated by the communications service providers who are responsible for the numbers inserted. Amendments to the ENUM database can only be performed by the operators responsible for that specific set of number(s) e.g. numbers for which they are the carrier of record.

5.4 Non-root DNS/ENUM architecture

In some circumstances, where the DNS or ENUM database or parts of them are under a single administrative control there is no need for operating dedicated root, Top Level Domain, Second Level Domain, Third Level Domain etc. DNS server respectively Tier-0, Tier-1 and Tier-2 ENUM server. In such a case the whole DNS and/or ENUM data can be stored on one single device. This approach is called a Non-Root DNS architecture. Because there is no Name Server hierarchy a DNS/ENUM client can send DNS/ENUM queries direct to such an non-root DNS/ENUM server. The need for a caching NS is not applicable. The message flow is optimized, there is just one DNS query and response message needed for DNS resolution.

6 Addressing and Routeing

6.1 User Addressing

Every IMS user has at least one private user identity. Private user identity is assigned by the home operator, and used, for example, for Registration, Authorisation, Administration, and Accounting purposes. Private user identity is in the form of a Network Access Identifier (NAI) RFC 4282 [i.1], for example joe.doe@carrier.com.

Private user identity is not used for actual routing of SIP messages, but it is contained in all registration requests when S-CSCF stores the private user identity. Private user identity is permanently allocated to a user in order to identify the subscription and it is stored in home operator UPSF.

In addition to private used identity, every IMS user has one or more public user identities. The public user identity is used in e.g. user-to-user communication. For example, it might be included on a business card. Public user identity is not authenticated by the network during registration, but it must be registered before the identity can be used in IMS activities. Public user identities can be used to identify the user's information within the UPSF. Format of public user identity is either SIP URI (RFC 3261 [9] or the "tel:"-URI format (RFC 3966 [10]), for example sip: tispan.support@etsi.org or tel: +33492944200.

Routing of SIP signalling within the IMS uses SIP URIs. E.164 format public user identities are not used for direct routing within the IMS and session requests based upon E.164 format public user identities will require conversion into SIP URI format for internal IMS usage. This conversion is done using ENUM. In all roaming cases, visited network just forwards all requests to home network S-CSCF, which is then responsible for making ENUM query, if necessary. In case of interworking it is up to originating operator's S-CSCF to support this conversion mechanism. Details of conversion mechanisms other than ENUM are for further study.

CSCF, BGCF and MGCF nodes are identifiable using a valid SIP URI (Host Domain Name or Network Address) on those interfaces supporting the SIP protocol. SIP URIs are used when identifying these nodes in header fields of SIP messages.

6.2 Naming of home network

An operator can use any domain name that he has publicly registered as the name for his home network.(thereby providing uniqueness). The present document describe only the usage of RFC 1035 [1]. Therefore it is highlighted here that a TISPAN IPX supports only domain labels which consists of 7-bit ASCII characters as letters, digits, and hyphen. Mechanism and procedures to support Internationalized Domain Names for Applications (IDNA) are not part of the present document.

DNS has an important role in IMS. During the session establishment an originating S-CSCF obtains the address of the I-CSCF for the network operator serving the destination user. Similarly during a registration a visited P-CSCF needs to resolve a home domain name to an address of I-CSCF in order to route SIP messages. DNS infrastructure is used for resolving an address of IMS contact point I-CSCF located in the home network.

IMS typically uses multiple DNS queries, for example registration procedure requires at least 6 DNS queries, mobile originated call with E.164 numbers requires at least 3 DNS queries, and receiving a notification (SIP NOTIFY) from the AS requires approximately 4 DNS queries. Usage of cache, however, means that majority of these queries are transmitted only between resolver and the first configured/found DNS server.

There are basically two major alternatives for IMS DNS deployment:

1) IMS domains are resolved using Internet DNS infrastructure (e.g. .com)

2) IMS domains are resolved using Interoperator DNS infrastructure, with three possible implementation models:

   - IMS Public User Identity (SIP URI) ends with (e.g. .3gppnetwork.org)

   - Subset of operator's global DNS infrastructure is duplicated in the Interoperator IP backbone network. Thus DNS server related to e.g. ims.operator.net can be found using the DNS service offered by the Interoperator IP backbone network

   - A mixture of Interoperator IP backbone DNS and operator internal mapping schemes is used

7 ENUM and DNS Structure and Delegation Model

7.1 Introduction

There are three top level principles which the ENUM model should support. First, there should be a competitive environment. Second, equal accessibility is required, such that the ENUM data fill is available to all entities who need it. Third, accuracy is critical, which means that there exist authoritative databases with the required information.

7.2 Model for the Interoperator IP backbone network

7.2.1 Introduction

A strict hierarchy is followed as DNS is designed to have a hierarchical structure allowing different organisations to have control of different parts of the overall structure. E.164 numbers also have a hierarchical structure and this can be mapped onto the DNS structure on the Interoperator IP backbone network. When one country or a group of operators has solved the provisioning of their ENUM Tier-1 server provider and in certain cases operators have established their tier 2 information, all operators connected to the Interoperator IP backbone network are able to use data for interworking scenarios.

7.2.2 ENUM & DNS Architecture

The DNS architecture for this model is depicted in figure 3.

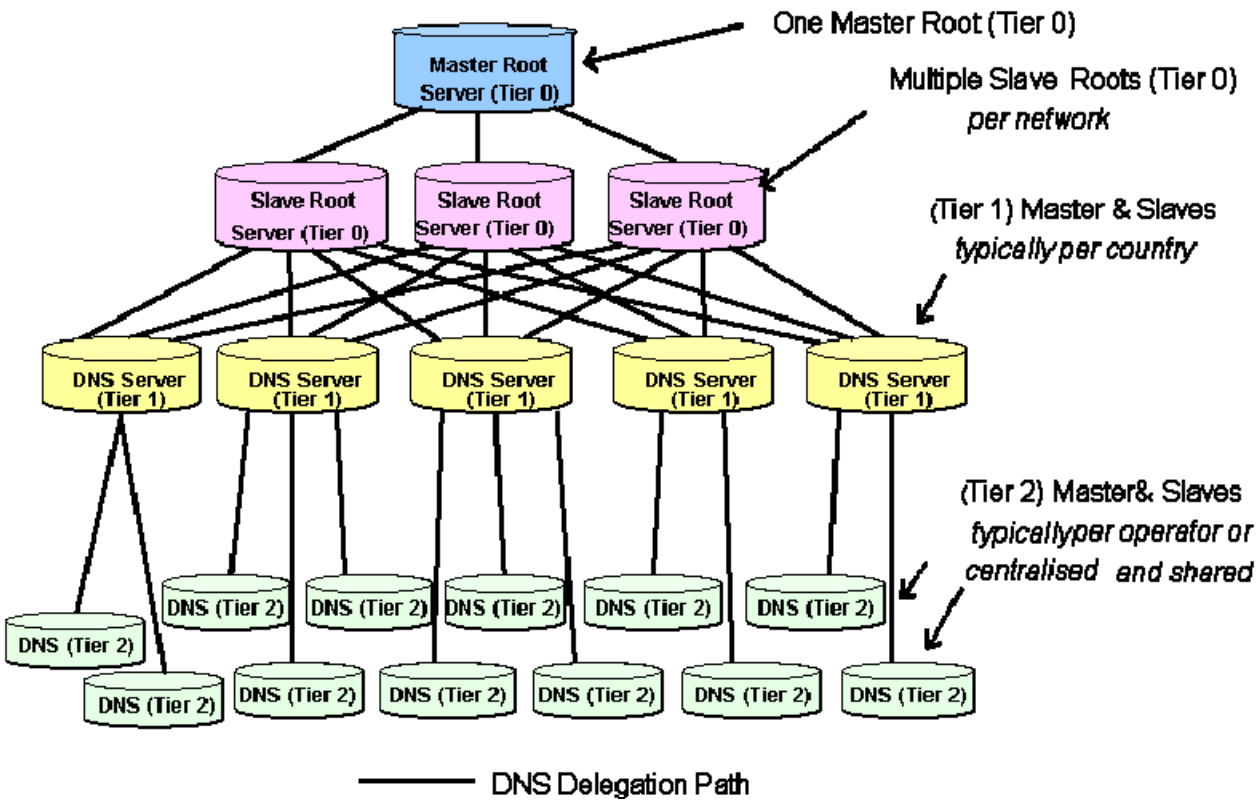

Figure 3: ENUM DNS hierarchy

It should be noted that what is represented in figure 3 are logical entities and thus one or more of those logical entities can be offered by one physical server. The physical realisation of this arrangement is not depicted in figure 3.

Tier-0: Delegates E.164 numbers for a specific country code to a country-defined Tier-1 server. "Where can I get information about E.164 numbers for a given country code?". All slave root servers contain the same information; an exact copy of the master.

Tier-1: Delegates a particular E.164 number or a block of numbers to a network operator-defined Tier-2 server.

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

The ENUM Tier-1 server provider can be one operator in a country, or a designated third party, who has access to the Interoperator IP backbone network. The ENUM Tier-1 server could be shared between multiple network operators. In some instances the ENUM Tier-1 server provider can even be the same provider who provides the ENUM Tier-0 server.

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

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

It is also possible to run mixed mode, i.e. where part of the delegations are done in Tier-1 and rest is done in Tier-2.

In practice there are many considerations relating to DNS delegation. Who has control of particular servers and number ranges is a matter of concern to telecomm carriers, especially in countries where numbers are portable between mobile and fixed carriers and there are potentially a large number of organisations involved. In the "real world" the delegation structure may not follow the model shown above and different Tiers may share the same server and delegation model.

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

7.2.3 Example resolution

Figure 4 depicts an example of ENUM resolution.

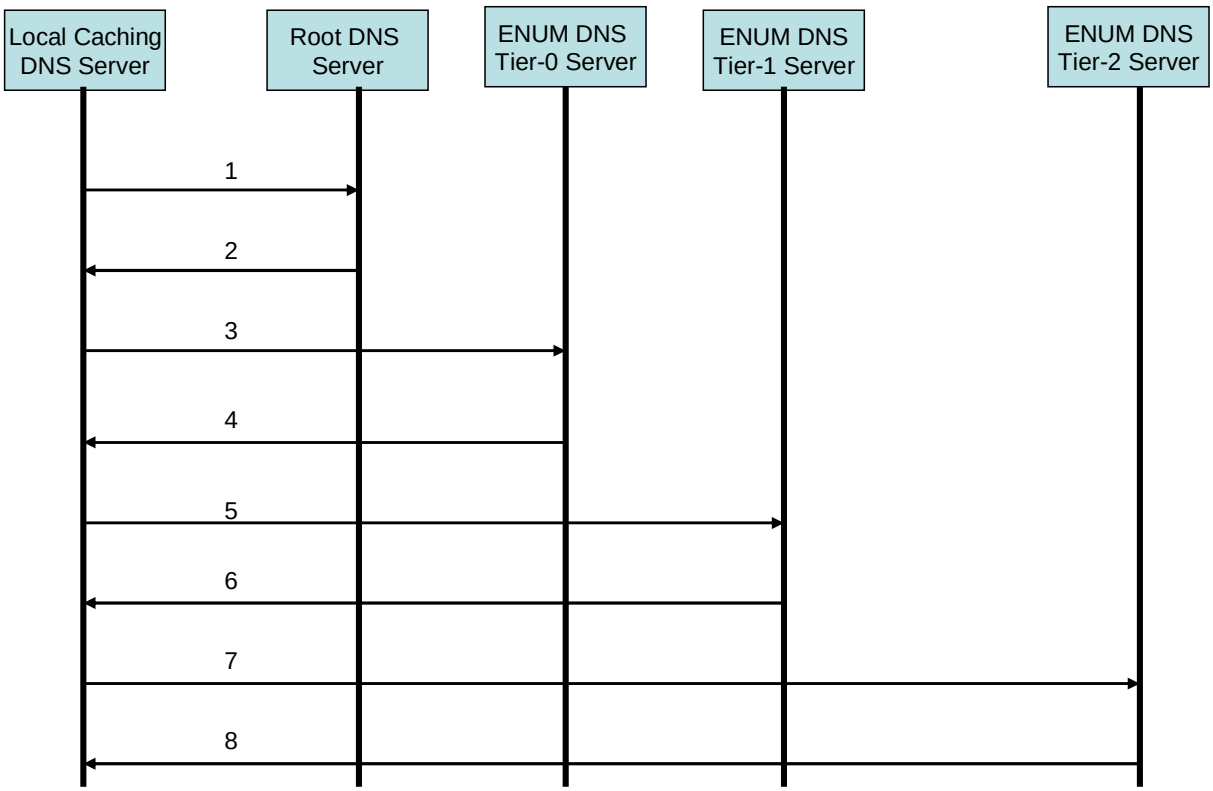

Figure 4: Example of ENUM resolution for an IMS session establishment

The numbers in the messages in figure 4, refer to the below:

1 Service Provider's Local Caching DNS Server sends the DNS query to the Root DNS Server (which is essentially a DNS server that is authoritative for that delegation).

2 Root DNS Server replies with the NS record for the ENUM DNS Tier-0 Server.

3 Service Provider re-sends the DNS query, but to the ENUM DNS Tier-0 Server.

4 ENUM DNS Tier-0 Server replies with the NS record for the ENUM DNS Tier-1 Server.

5 Service Provider re-sends the DNS query, but to the ENUM DNS Tier-1 Server.

6 ENUM DNS Tier-1 Server replies with the NS record for the ENUM DNS Tier-2 Server.

7 Service Provider re-sends the DNS query, but to the ENUM DNS Tier-2 Server.

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

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

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

NOTE 3: The Originating Communications Provider apply an optional policy check upon receiving any response.

NOTE 4: A NS record contains normally FQDN. To reach the NS the FQDN has to be solved as an IPv4 or IPv6 address. In some cases the IP address is delivered in the answer packet of the NS record (glue record).

7.2.4 Access to ENUM servers

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

IP address Public addressing shall be applied in all Communications Provider IP Backbone network elements, which are advertised or visible to other Service Providers. Using public addressing means that each Communications Provider has a unique address space that is officially reserved from the Internet addressing authority. However, public addressing does not mean that these addresses should be visible to Internet. For security reasons, Communications Provider and inter-Service Provider backbone networks shall remain invisible and inaccessible to the public Internet.

Internet routers should not be able to route to the IP addresses advertised to the Inter-Service Provider IP Backbone. In other words the IP Backbone Providers' and Communications Providers' networks shall be totally separated from public Internet, from an IP routing perspective.

8 Delegation and use of domains

The exact choice of domain names to be used for the inter-operator IP backbone network is for further study however some high level principles and guidelines on their control, administration and structure follow. At this stage all detailed references and use of domain names within the present document should be treated as examples used merely to demonstrate the required structures.

The choice of domain name to be used must:

- to ensure there is no conflict with Public user ENUM
- be registered on the Internet to ETSI TISPAN
- have an appropriate suffix e.g. .net

- the chosen domain name must be available to be registered on the public internet for use by the inter-operator IP backbone network
- neutral between mobile/fixed standards groups
- has an indication of its purpose i.e. E164 and ENUM
- can support future connection of both fixed & mobile services to an IPX common to ETSI TISPAN (and possibly GSMA)

If a decision was taken to implement an ETSI TISPAN specific inter-operator IP backbone network appropriate control and oversight procedures would need to be determined but that study must remain dependent upon that event.

Annex A (informative): Configuration Information for Services that Utilise DNS

A.1 Introduction

This clause describes the technical characteristics of each service that utilises DNS. Further detail can be found in the referenced specifications. If there are discrepancies between the description of the services in these clauses and the referenced specifications, what is stated in the referenced specifications prevail.

A.2 ENUM FQDN Format

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

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

EXAMPLE 1: +44-7700-900123.

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

EXAMPLE 2: +447700900123.

- Remove all characters with the exception of the digits.

EXAMPLE 3: 447700900123.

- Put dots (".") between each digit.

EXAMPLE 4: 4.4.7.7.0.0.9.0.0.1.2.3.

- Reverse the order of the digits.

EXAMPLE 5: 3.2.1.0.0.9.0.0.7.7.4.4.

- Append a top level domain name to the end (example: ".e164.arpa" for Public ENUM, or "e164enum.net" for Carrier ENUM on the GRX/IPX). For the inter-operator IP backbone network a top level domain name of the form .e164.tispan.foo is assumed.

EXAMPLE 6: 3.2.1.0.0.9.0.0.7.7.4.4.e164.tispan.foo.

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

A.3 ENUM Tiers

To ensure proper distribution and scalability of the DNS structures, ENUM uses a tier system. This is typically used in user ENUM as follows:

Tier 0 - Global level

- Under this domain are pointers to the Tier 1 authoritative servers.

Tier 1 - Country level (CC)

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

Tier 2 - User level

- Authoritative for E.164 number ("6.5.4.3.2.1.0.0.7.7.4.4.e164.arpa").

  Under this domain are the individual Subscriber Numbers each with one or more NAPTR records.

In the case of shared ENUM infrastructure, the role of the user is taken by the operator (Carrier of Record).

ENUM Tiers can be combined or even expanded. Further Tiers may be relevant in some networks and/or countries.

ENUM is only for E.164 numbers. If the E.164 number is in a national format, as first step a conversion to an international format is needed. ENUM does not support non E.164 numbers (e.g. short codes). For further information see TR 184 005 [i.5]. Services that are related to particular E.164 numbers are stored and described in NAPTR records. NAPTR records are defined in RFC 3403 [3] and can be used for mechanisms other than ENUM.

A.4 Technical Requirements for Interconnexion

A.4.1 NAPTR formats

The NAPTRs used in ENUM are defined in RFC 3404 [4]. An example of ENUM datafill in a DNS is as follows. This shows a part of an E.164 number which supports both IMS and MMS. Note that the $ORIGIN statement is used here to ensure correct syntax and would have limited use in a live DNS.

$ORIGIN 3.2.1.0.0.9.0.0.7.7.4.4.e164enum.net.

NAPTR 100 10 "u" "E2U+SIP".

"!^.*$!sip:+447700900123@provider.net!".

NAPTR 100 20 "u" "E2U+MMS:mailto".

"!^.*$!mailto:+447700900123@provider.net!".

A NAPTR contains the following fields:

ORDER	It is recommended to set the ORDER field in ENUM applications to 100.
PREFERENCE	The PREFERENCE field gives the preference by which the destination network wants the NAPTRs to be processed.
FLAG	The FLAG field may be "u" or blank "". In the inter-operator IP backbone network it is always "u", indicating that the regexp filed contains an URI. The "" is not used in inter-operator IP backbone network.
ENUMservice	The ENUMservice field contains E2U, indicating an ENUM application, plus one or more enumservices such as "sip", "mms:mailto" or "pstn:tel". The enumservices are defined in RFCs and registered via IANA.
Regexp	This field contains the URI in a regular expression.
Replacement	The replacement field is not used currently in the inter-operator IP backbone network.

A.4.2 ENUMservice field

The ENUMservice field appears in the NAPTR records for a particular E.164 number. It describes the services supported by that number. The following are recommended values to be used for different services defined by 3GPP.

The ENUMservice to be used for IP-based services in IMS is "E2U+SIP" as defined in RFC 3764 [12].

The ENUMservice for services still on the PSTN/ISDN/PLMN on circuit-switched networks is "E2U+pstn:tel" as defined in RFC 4769 [13].

The ENUMservice to be used for MMS is "E2U+MMS:mailto" as defined in RFC 4355 [11].

A.4.3 URI Formats

The information between the right side pair of "!" is known as an URI. For the inter-operator IP backbone network the user part contains the E.164 number in the international format, the domain name contains a unique indication to the destination network.

EXAMPLE: sip:<+E.164 number>@provider.net

add other examples:

sip:<user>@example.com

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

tel:<+E.164 number>

The MMS ENUM URI domain format is not yet finalised (see GSMA PRD IR.67 [i.2]).

A.4.4 SIP server configuration

There are several IETF RFCs covering use of SIP in the DNS. These include RFC 3824 [i.4].

The reason this configuration is needed is as follows:

When a SIP call is made by a user, he addresses the call to either a SIP URI (e.g. kim@provider.net) or an E.164 number. In both cases the IMS system needs to know the IP address of the SIP server to which it can route the call. The SIP server information contains the detail needed to provide the called network's SIP server IP address to the calling network based on the information in the SIP URI. If the call is to an E.164 number the ENUM system first translates that number to a SIP URI e.g. to:

`+447700900123@provider.net`

The approach described in this clause is compliant with these RFCs and consists of 4 separate steps.

Step 1

This is the ENUM related step and is only performed for cases where the service has been addressed to an E.164 number. An IMS call to a user using the format bob@provider.net would not require this step. Example of DNS data for a particular SIP URI and its servers

$ORIGIN 3.2.1.0.0.9.0.0.7.7.4.4.e164.foo.

NAPTR 100 10 "u" "E2U+SIP"

"!^.*$!sip:+447802345678@provider.net!" .

NAPTR 100 10 "u" "E2U+MMS:mailto"

"!^.*$!mailto:+447802345678@provider.net!" .

The calling application asks the DNS for all the NAPTR records for the given E.164 number. There may be multiple NAPTR records returned as in this example. The calling application then selects the NAPTR record which contains the desired services which in this case are "E2U" and "SIP". "SIP" is called an enumservice.

The "u" flag indicates the result of this lookup is a URI. The rest of the NAPTR is a Regular Expression. The calling application substitutes the relevant fields into the regular expression to get the result which is a SIP URI.

The calling application then extracts the domain name from the URI. This is the domain name of the destination network to which the SIP call should be routed.

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:

- provider.net. IN NAPTR 50 100 "s" "SIP+D2U" "" _sip._udp.provider.net.
- provider.net. IN NAPTR 90 100 "s" "SIP+D2T" "" _sip._tcp. provider.net.
- provider.net. IN NAPTR 90 100 "s" "SIPS+D2T" "" _sips._tcp. provider.net.

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

Step 3

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

- _sip._tcp.provider.net. SRV 0 1 5060 sipserv1.provider.net.
- _sip._tcp.provider.net. SRV 0 2 5060 sipserv2.provider.net.
- _sip._udp.provider.net. SRV 0 1 5060 sipserv1.provider.net.
- _sip._udp.provider.net. SRV 0 2 5060 sipserv2.provider.net.
- _sips._tcp.provider.net. SRV 0 1 5060 sipserv3.provider.net.
- _sips._tcp.provider.net. SRV 0 2 5060 sipserv4.provider.net.

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

- name of the server
- which port number SIP uses
- 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 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.

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 for an IPv4 address or an "AAAA" (quad A) record lookup for an IPv6 address.

- sipserv1.provider.net. IN A 10.1.2.3
- sipserv1.provider.net. IN AAAA 2001:db80:1234:5678:90ab:cdef:1234:5678

- sipserv2.provider.net. IN A 10.1.2.4
- sipserv2.provider.net. IN AAAA 2001:db80:1234:5679:90ab:cdef:1234:5679

Annex B (informative): General Configuration Information for Providers' DNS Servers

B.1 Introduction

This clause gives some general information on DNS server configuration for operators.

B.2 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.

B.3 Software

Most commonly ISC BIND (usually version 4 or 9) is the chosen functional test reference software by operators and equipment vendors. This works for services which do not necessarily have a large data-fill but for services such as ENUM where the data-fill can run into millions of resource records, a commercial DNS server product may be used.

Such commercial DNS server solutions can also support legacy DNS data-fill, thereby consolidating all operator DNS needs.

B.4 Caching

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

When setting the TTL value for a zone, careful consideration is needed to ensure that the right trade-off is made between performance, consistency as well as operational, regulatory and process requirements. 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, 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. The TTL value for ENUM domains impact the time related requirements for number portability, in the case that ENUM is used to support number portability.

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.

B.5 Reverse Mapping

Each operator is strongly recommended to provide reverse mapping of all FQDNs that they use (e.g. A or AAAA resource record resolution). This is not mandatory for interworking to be successful, but rather, it aids in trouble shooting/debugging activities such as performing a "traceroute".

B.6 Use of DNS Interrogation Modes

Two interrogation modes are defined in the DNS specifications: iterative and recursive.

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. On the inter-operator IP backbone network DNS, this would look like the following.

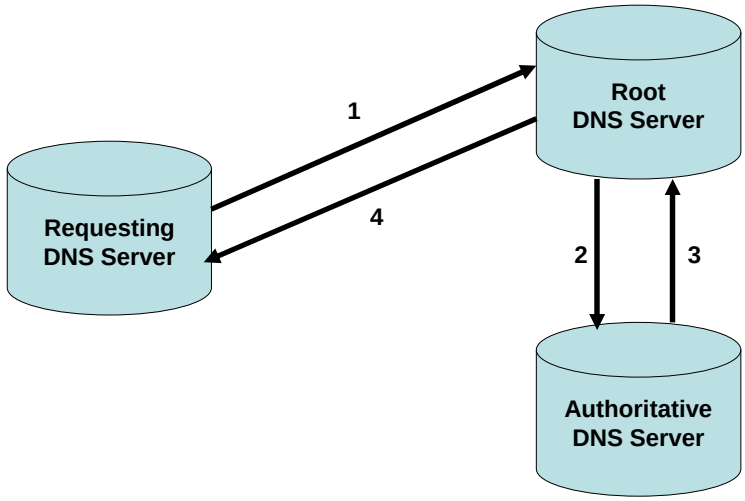

Figure B.1: Recursive interrogation mode as seen by the owner of the authoritative DNS Server

As can be seen above, the owner of the authoritative DNS server has no visibility of the source of the original request (i.e. the VPLMN address is not included in the request).

In Iterative mode, a DNS server interrogates each DNS server in the hierarchy itself, in order to resolve the requested domain name. On the inter-operator IP backbone network DNS, this would look like the following.

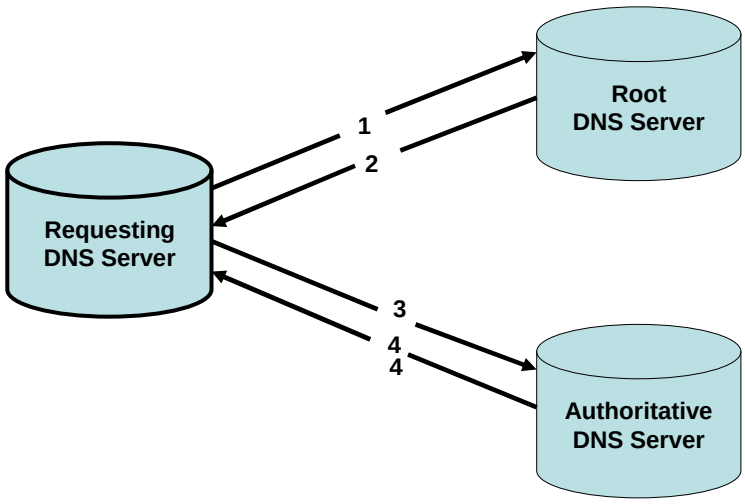

Figure B.2: Iterative interrogation mode as would be seen on the DNS of the inter-operator IP backbone network

As can be seen above, the owner of the authoritative DNS server has full visibility of the source of the original request.

As a security measure it is recommended that on the inter-operator IP backbone network, Root DNS Servers deliberately do not service DNS requests sent in Recursive mode: only those issued in Iterative mode. This would enable owners of Authoritative DNS Servers to determine the true source of DNS requests and thus provide adequate security measures, such as access lists, at the edge of their networks.

B.7 Use of the inter-operator IP backbone network Root DNS Server

There are two possibilities to arrange DNS hierarchy. The first is for each Communications Provider to configure their Nameserver of each domain name individually for all inter-working and partner operators. The drawback of this approach is that it is not scalable as every time a new inter-working and/or partner operator agreement is made or any existing inter-working and/or partner Communications Provider Nameserver data changes, an data update of all DNS Server is needed. This potentially forms a likely source of operational inter-working and roaming problems. Another alternative is to use the common the inter-operator IP backbone network Root DNS Server, as provided for by the inter-operator IP backbone network provider Using the inter-operator IP backbone network Root DNS Server enables changed Nameserver data for an operator to be immediately active (subject to caching).

B.8 Provisioning of Communications Providers DNS servers

Inter-operator IP backbone network Service Providers may take the responsibility for the management of DNS on behalf of the operator subscribing to the IPX. Services require DNS information to be exchanged between all operators and the inter-operator IP backbone network providers (where those inter-operator IP backbone network providers are managing an operator's DNS service on their behalf). Communications Providers and the inter-operator IP backbone network providers should distribute all required DNS information between inter-working/roaming operators, or make available access to their authoritative DNS server(s) to service DNS requests.

Annex C (informative): Bibliography

- IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".
- IETF RFC 3401: "Dynamic Delegation Discovery System (DDDS) Part One:The Comprehensive DDDS".
- IETF RFC 3402: "Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm".
- ETSI TS 123 003: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Numbering, addressing and identification (3GPP TS 23.003 version 6.10.0 Release 6)".
- GSMA PRD IR.65: "IMS Roaming and Interworking Guidelines".
- IETF RFC 1032: "Domain administrators guide".

History

Document history		
V3.1.1	August 2011	Publication