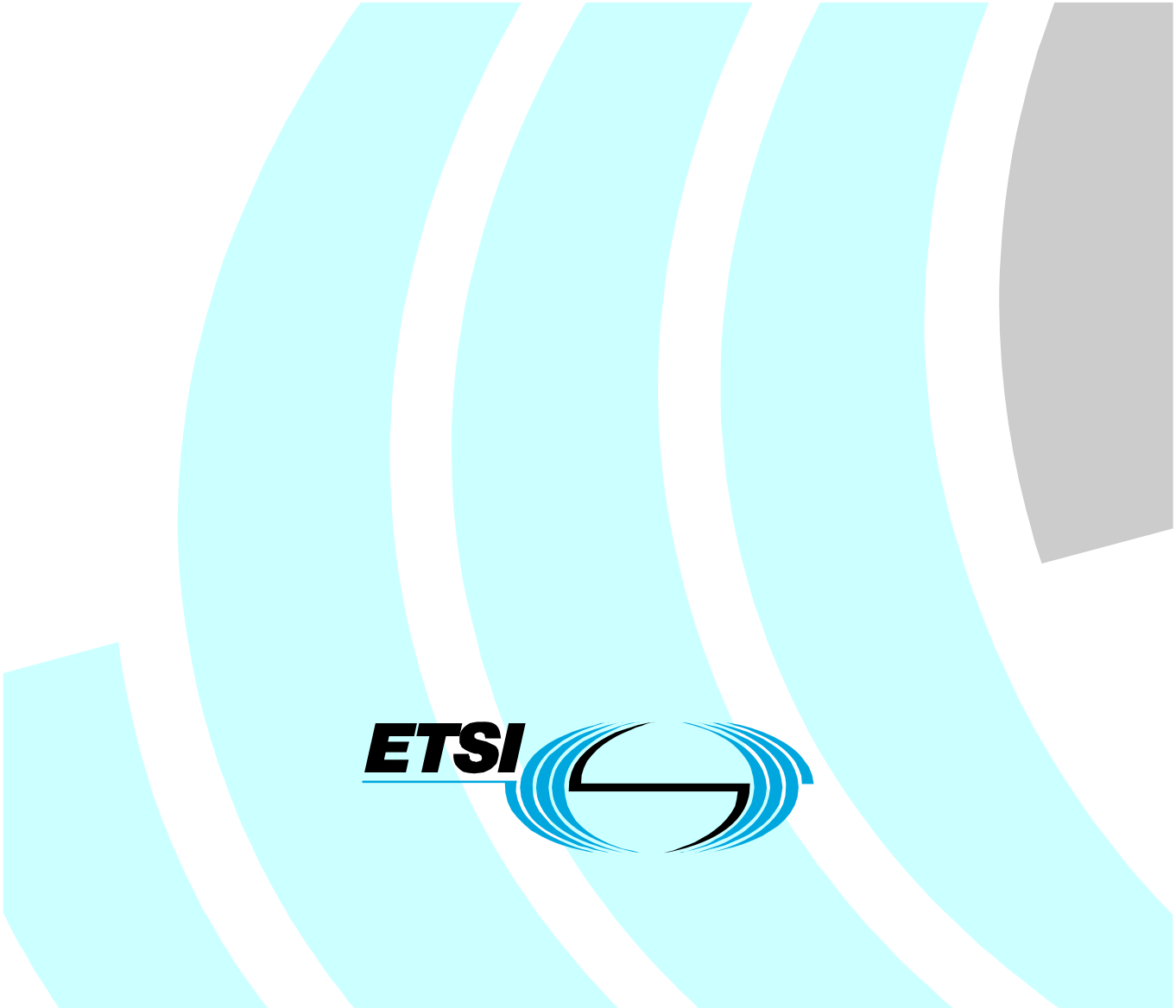
ETSI TR 184 008 V2.1.1 (2009-02)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Infrastructure ENUM Options for a TISPAN IPX



Reference
DTR/TISPAN-04012-NGN-R2

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

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://webapp.etsi.org/IPR/home.asp).

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

1 Scope

The present document provides an overview of some of the relevant options that can be used to implement Infrastructure ENUM (I-ENUM), which in the present document is defined as the use of the technology specified in RFC 3761 [i.1] by the carrier of record to map a telephone number into a URI. That URI then identifies a specific point of interconnection to that communication provider's network that could enable the originating party to establish communication over an IPX to the associated terminating party.

An assessment of the options is given and recommendations made in order to provide a secure and reliable implementation of I-ENUM for TISPAN networks to facilitate routeing and interconnection within NGNs.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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 indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] IETF RFC 3761: "The E.164 to Uniform Resource Identifiers (URI); Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[i.2] IETF RFC 1034: "Domain Names - Concepts and Facilities".

[i.3] IETF RFC 1035: "Domain Names - Implementation and Specification".

[i.4] ITU-T Recommendation E.164: "The International Public Telecommunication Numbering Plan".

[i.5] ETSI ES 282 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture".

[i.6] IETF RFC 5067: "Infrastructure ENUM Requirements".

[i.7] IETF RFC 3263: "Session Initiation Protocol (SIP)".

[i.8] IAB instructions to RIPE NCC.

NOTE: Available at: http://www.ripe.net/enum/instructions.html.

[i.9] ETSI TS 102 051: "ENUM Administration in Europe".

[i.10] ETSI TR 184 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Naming/Numbering Address Resolution (NAR)".

3 Definitions and abbreviations

3.1 Definitions

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

Carrier of Record:

- the communication provider to which the E.164 number was allocated for end user assignment, whether 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); or
- if the number is ported, the communication provider to which the number was ported; or
- where numbers are assigned directly to end users, the communication provider that the end user number assignee has chosen to provide a Public Switched Telephone Network/Public Land Mobile Network (PSTN/PLMN) point-of-interconnect for the number.

It is understood that the definition of carrier-of-record within a given jurisdiction is subject to modification by NRAs (National Regulatory Authorities).

E.164 number: string of decimal digits that, for a geographic country code, uniquely identifies a subscriber or a point where a service is provided

For the case of a global service code, it identifies the subscriber of the service. For Networks, it identifies a subscriber of the Network.

An international E.164 number can act in the "role" of both a name and an address. Portability is reducing a number's role as an address. Numbers are increasingly acting in the role of a name only.

The number, which includes the country code and subsequent digits, but not the international prefix, contains the information necessary to route the call to this termination point on a public network (it may also contain the supplementary information necessary to forward it on a private network).

NOTE: It is sometimes referred to as an "international number", "international public telecommunication number" or "E.164 number".

Name Number Address Resolution (NAR):

The terms "address resolution" and "name resolution" are synonymous and are used in the IP world in different manners:

In IP network, there are two types of Address Resolutions defined:

- The first is the conversion from a domain name into an IP address (see DNS).
- The second is from the IP address to the Ethernet Address Resolution – this is not in the scope of the present document.

Private: any arrangement between parties (specific to a communication provider or shared between consenting groups of communication providers e.g. federation) that is outside of the public Internet

TISPAN IPX:ETSI TISPAN defined inter-operator IP backbone network that is compliant with TISPAN standards and is transparent to subscribers

NOTE: This is able to support connectivity between any type of Service Provider, for interworking, a range of IP services on a bilateral basis with end-to-end QoS and interconnection charging.

3.2 Abbreviations

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

CP	Communications Provider
DDOS	Distributed Denial Of Service attack
DNS	Domain Name System
I-ENUM	Infrastructure ENUM
IPX	IP Packet eXchange
ITU	International Telecommunications Union
NAPTR	Number Authority Pointer
NAR	Naming/Numbering Addressing Resolution
NGN	Next Generation Network
PoI	Point of Interconnection
PSTN	Public Switched Telephone Network
RRs	Resource Records
SIP	Session Initiation Protocol
URI	Uniform Resource Identifier
PLMN	Public Land Mobile Network
NRA	National Regulatory Authoritie
CC	Country Code

4 Introduction

Within ETSI TISPAN work is progressing on Next Generation Networks (NGNs). A Next Generation Network (NGN) is a packet-based network able to provide services including Telecommunication Services and is able to make use of multiple broadband, QoS-enabled transport technologies in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different communication providers. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

The realization of those capabilities requires a numbering and routeing capability and the use of DNS protocols and functionality. The present document focuses on the use of Infrastructure ENUM to map a telephone number into a URI that could identify a specific point of interconnection (PoI) to that communication provider's network that could enable the originating party to establish communication with the associated terminating part through an IPX.

5 Types of ENUM

ENUM (RFC 3761 [i.1]) is a capability that transforms E.164 numbers into domain names and then uses the DNS (Domain Name System) to discover NAPTR records that specify the services available for a specific domain name. There are basically two broad variants of ENUM, User ENUM and Infrastructure ENUM.

5.1 User ENUM

User ENUM as originally defined was based on the end-user opt-in principle, where the explicit consent of the user who has the rights to use a specific telephone number is required in order to insert that number into the ENUM system. The user also has the right to specify the ENUM capabilities that are provided against that number e.g. what is inserted in the associated NAPTRs that facilitate the ENUM services delivered. The standardized implementation of User ENUM

utilizes the public Internet and the .e164.arpa domain name as specified within RFC 3761 [i.1]. Procedures about administration of User ENUM have been specified by ETSI [i.9].

5.2 Infrastructure ENUM

Infrastructure ENUM is defined in the present document as the use of the technology specified in RFC 3761 [i.1] by the carrier of record to map a telephone number into a URI that identifies a specific point of interconnection to that communication provider's network that could enable the originating party to establish communication with the associated terminating party. Other concepts may also apply for I-ENUM in the NGN.

The present document, also embraces the ENUM concept and protocol when it is implemented within a private DNS environment e.g. when it does not use the global public DNS.

In either case no user data is inserted in the database. Only information required to identify the carrier responsible for the called number, or in some cases additional information to route the call is inserted within the database and remains under the control of the relevant carrier.

Figure 1 depicts the main differences between user and infrastructure ENUM and variants within those categories.

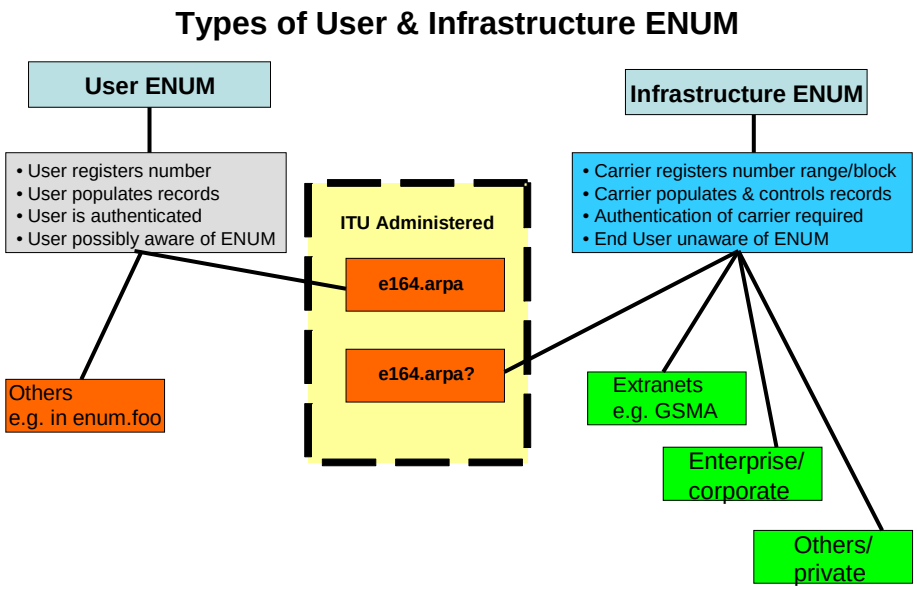


Figure 1: Types of User and Infrastructure ENUM

It shows that both User and Infrastructure ENUM can be provided in a number of forms.

For User ENUM implementations could occur within a national environment using e164.arpa once the appropriate National Regulatory Authority has signalled their approval of this delegation to the ITU-TSB in accordance with the instructions issued by the Internet Architecture Board (IAB) to RIPE-NCC regarding how to proceed with any requests received by RIPE-NCC. Those instructions can be found at http://www.ripe.net/enum/instructions.html [i.8] and at the ITU web site at http://www.itu.int/ITU-T/inr/enum/procedures.html.

A number of different but complimentary implementations of ENUM will exist using both public (e.g. Internet) and private DNS infrastructure. It is for communications providers to decide which of these best meets their needs.

5.2.1 Infrastructure ENUM within the public DNS

This option is where the resolution of the initial ENUM look-up to identify interconnection points within or between networks is resolved within servers that form part of the public Internet. In some cases the information required may be cached within local network servers.

Within the public Internet, theoretically it is possible to utilize different parts of the name space for infrastructure ENUM, however the adoption of a common approach would radically reduce interworking difficulties.

It should be noted that it is possible for a group of communication providers to share a common part of the public segment that can be made more secure, even though the existing infrastructure is used, however this still raises some issues over the degree of security that can be maintained as no part of the public Internet is totally immune from DDOS attacks.

5.2.2 Infrastructure ENUM within private DNS

A private DNS implementation is where the DNS servers can only be accessed by a communication provider (or group or federation of communication providers) within their own environment. The supporting infrastructure also remains private and cannot be accessed via the public Internet, therefore this implementation can be viewed as an extranet. The choice of domain name is under the control of the communication provider(s) concerned.

Enterprise and corporate networking requirements can also be realized as both extranets and intranets, dependent upon their needs However access to and from networks outside of those arrangements will remain a key requirement.

Other arrangements will also emerge where third party ENUM providers will facilitate detailed routeing information that will support peer to peer networking, including IP PBX capabilities.

6 Infrastructure ENUM requirements in TISPAN NGN

As detailed in clause 4 Infrastructure ENUM is distinguished from user ENUM as defined in RFC 3761 [i.1] in which the entity or person having the right-to-use a number has the sole discretion about the content of the associated domain and thus the zone content. From a domain registration perspective, the end user number assignee is thus the registrant. As VoIP evolves and becomes pervasive, E.164-addressed telephone calls need not necessarily traverse the Public Switched Telephone Network (PSTN). Therefore, VoIP service providers have an interest in using I-ENUM to facilitate both intra and inter-carrier routeing capabilities, thus keeping VoIP traffic on IP networks on an end-to-end basis. Different implementations of Infrastructure ENUM can facilitate this requirement. For NGN the usage of TISPAN IPX can be seen as one option.

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 3761 [i.1] 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 ENUM as tel URI in the international format (an E.164 number) e.g. +44nnnnnnnnnn for processing within Infrastructure ENUM (I-ENUM). The output from the I-ENUM resolution process would be an URI that could identify a specific point of interconnection to the communication provider's network that could enable the originating party to establish communication with the associated terminating part through an IPX.

It should be appreciated that at this stage specific route determination may require more information.

6.1 Top level requirements

The top level requirements for I-ENUM and the interworking capabilities it provides as specified within ETSI TISPAN are listed below:

- Adherence to relevant standards:

  All implementations are expected to comply with the same basic elements defined with relevant standards documents and IETF RFCs. In particular adherence to RFC 3761 [i.1] for detailed ENUM protocol requirements is mandatory except for the choice of the top level domain name, if an approach is adopted that uses private rather than public DNS e.g. an approach that does not use the basic internet for ENUM look ups.

- single global approach worldwide across all participating communications providers fixed and mobile (aim):

  Ideally a single global approach is required. However the disparate growth of different types of ENUM implementation across the world, coupled with the urgent drive by communications providers to meet near term commercial goals has resulted in a recognition that the world will not wait for a single global approach to be standardized. It is hoped that gradually more communications providers will merge their initial solutions and a de facto large scale approach will emerge. Realistically that solution will not embrace all communications communication providers and it will remain imperative that differing types of ENUM facilitate global connectivity, even if all numbers are not within a single ENUM tree (domain name space). This is recognized as a likely requirement that would be imposed by National Regulatory Authorities (NRAs) as well as an industry needs to facilitate global connectivity.

- Secure environment:

  A secure environment is essential to all communication providers to facilitate I-ENUM. As network operations are totally dependent upon the reliability and security of routeing information. The exposure of that information, or of interconnection points potentially poses a threat to the security and stability of any network.

- Shared control of infrastructure amongst all communications providers (technically and administrative):

  Shared control of infrastructure in a standardized and acceptable form is seen as key requirement because it has the potential to drive down overheads and enhance competition, whilst facilitating full connectivity in an efficient manner.

- End to end service delivery (controlled):

  All communications providers require guaranteed end to end service delivery with other providers/networks which meets predetermined parameters. Best effort results will not be acceptable for all types of traffic/interconnection.

- Service operability:

  Service operability across multiple networks is a prerequisite. The imposition of resource intensive intelligent networking capabilities/additional look-ups and interworking requirements across networks to facilitate operability between networks will inhibit service creation and market growth.

- Efficient interconnect and peering arrangements between communications providers (both bilateral and hierarchical dependent on levels of trust):

  It is recognized that different levels of interconnect and trust will exist between communications providers, dependent upon specific relationships e.g. communications providers peering arrangements, whether communications providers are part of the same I-ENUM tree, etc.

- Efficient service creation/amendment:

  Service creation and amendment within the I-ENUM environment are expected to be flexible and efficient, and fit within minimum agreed parameters.

- Equitable playing field for all participating communications providers:

  Whilst a fair playing field for all communications providers participating in each I-ENUM realization is inherently desirable, this is also likely become a regulatory issue if implementations are view as closed environments and full interconnect and connectivity is not achievable, or is implemented in a manner that results in unfair competitive practice.

- Global approach:

  Whether public or private DNS approach is utilized for I-ENUM, ideally a global approach is required, however it is recognized that single global implementation is unlikely to prove achievable and the more likely scenario is the emergence of a number of federations. That being the case interworking between federations will become a key requirement.

6.2 Detailed Requirements

- I-ENUM is expected to provide a means for a provider to populate DNS resource records (RRs) for the E.164 numbering resources for which it is the carrier-of-record, either in a private DNS arrangement or a single common publicly accessible namespace.
- Queries of I-ENUM fully qualified domain names are expected to return a result, even if the result is NXDOMAIN. Queries are expected to not be rejected, e.g. based on access control lists.
- I-ENUM is expected to support RRs providing a URI that can identify a point of interconnection for delivery to the carrier-of-record of communications addressed to the E.164 number.
- I-ENUM is expected to support the capability that allows qualified parties to obtain information regarding the E.164 numbering resources and the corresponding carrier-of-record. Determination of what information, if any, is expected to be available to which parties is a national matter.
- I-ENUM is expected to be implemented under a top level public or private domain that can support reliability and performance suitable for PSTN PLMN applications.
- I-ENUM is expected to meet all reasonable privacy concerns about visibility of information an end user has no control over. It should, for example, support mechanisms to prevent discovery of unlisted numbers by comparison of ENUM registrations against directory listings, or inadvertent disclosure of user identity.
- The selected method of providing I-ENUM is expected to be implementable within the required timescale.
- The selected method of providing I-ENUM is expected to enable early implementations to transition to a global implementation.
- Proposed implementations of I-ENUM should:
  - Minimize changes required to existing requirements that are part of RFC 3761 [i.1].
  - Work with fixed and variable number lengths.
  - Minimize the number of lookups required to obtain as many NAPTR records (end-user and infrastructure) as possible.
  - Minimize the client knowledge of the numbering plan required.
  - ENUM provided within the public DNS is expected to support interworking with private ENUM trees.

7 Architectural considerations

Within TISPAN, numbering and addressing functionality forms a key requirement.

In ES 282 002 [i.5] the need to find the URI to which SIP messages should be sent to effect a connection with the customer at a dialled number is recognized as a requirement.

Figure 2 shows examples of the numbering and routeing functionality, involved identifiers, components and functions and shows where I-ENUM fits within the process.

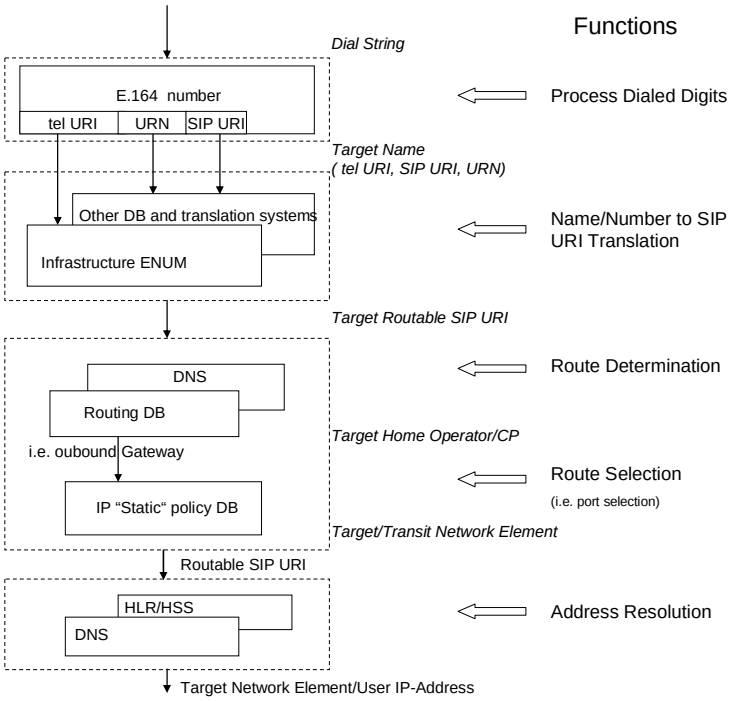


Figure 2

At each level of the ENUM routeing hierarchy different considerations will impact the preferred implementation.

7.1 ENUM Architecture within TISPAN

One of the first decisions that needs to be taken is whether to utilize the public DNS (public internet) or private DNS. Once that decision has been taken within each carrier grouping, further consideration can be given to the routeing hierarchy and how individual networks can access ENUM data.

7.2 Implementing ENUM using public or private Infrastructure

When ENUM is implemented within public infrastructure, RFC 3761 [i.1] specifies the use of the *e164.arpa* domain for ENUM within the public Internet for that purpose. With the original focus being on User ENUM the administration of that domain was developed within ITU with a set of Interim Procedures being agreed.

Whilst it is possible to provide I-ENUM within any part of the domain name space, in general the main focus for communications providers until now has been the use of the e164.arpa domain. There is general recognition that the use of multiple top level domains, particularly if applied to large communications providers, is likely to result in large scale interworking requirements that will be difficult to address. If all major communications providers participate in a single tree, those situations are avoided.

7.2.1 Using Public DNS (Public internet)

The recognition that large scale interworking is essential has been the main driver for discussions within the IETF on the possible use of part of the e164.arpa name space. Another perceived benefit of this approach is that the temporary assignment guidelines to facilitate delegation of each National Regulatory Authorities (NRAs) part of the name space is already existing for User ENUM, with many delegations having been made e.g. *44.e164.arpa* for the UK, *49.e164.arpa* for Germany. Extending them to cover I-ENUM should be quite easy. Each appropriate NRA will need to agree and accept this.

Two major format have been discussed within the IETF where the branch record for I-ENUM would be denoted by the 'i' character, linked with the relevant country code (CC):

(i) cc.i.e164.arpa.

(ii) i.cc.e164.arpa.

The first format required the ITU to oversee the specific ENUM delegation made to each NRA specifically for I-ENUM in a manner similar to User ENUM. The second potentially placed the sub delegation required to facilitate user and I-ENUM clearly under the direct control of the NRA once a delegation of the CC name space had been made to them.

Figure 3 highlights the elements of I-ENUM that apply to implementation using public infrastructure as opposed to the private space which is shown in green.

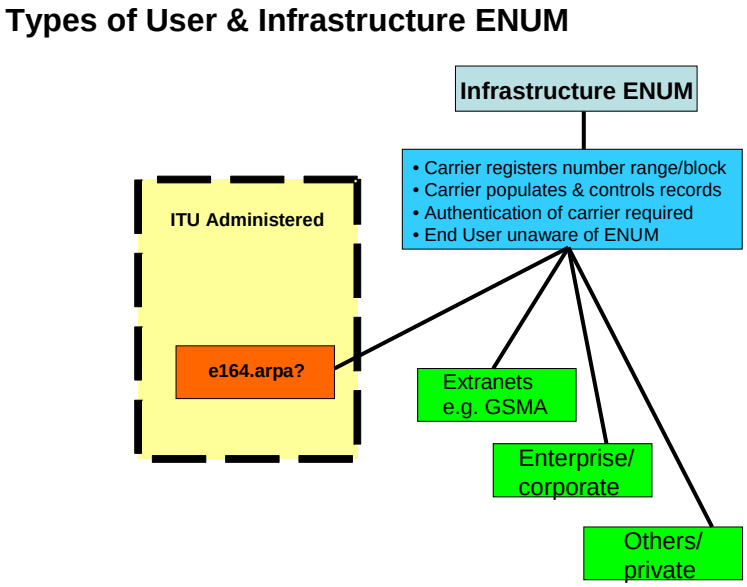


Figure 3: Implementation of Infrastructure ENUM

No decision on the choice of format or its appropriateness has been made.

Whilst this approach (using the public Internet) appears to represents the best opportunity to meet the goal of achieving a single global approach worldwide, some communications providers have also expressed reservations over the use of the public Internet. Their concerns focus on the exposure of points of interconnection to the global DNS could expose their networks to various forms of attack, jeopardizing the security and stability of their services.

7.2.2 Using Private DNS

The approach that uses private DNS will result in a number of different configurations. The predominant approach for large communications will result in a number of shared federation(s) of communications providers.

Figure 4 highlights the elements of I-ENUM that apply to implementation using private DNS as opposed to public infrastructure.

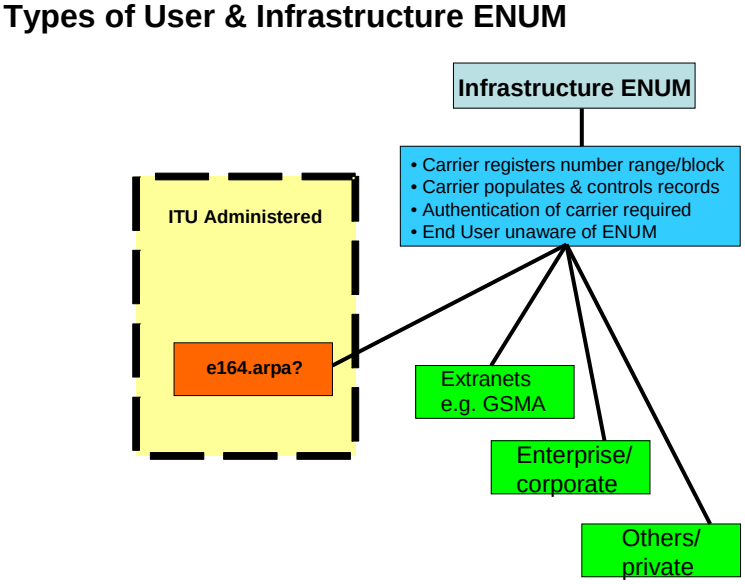


Figure 4: Implementation of Infrastructure ENUM

This functionality provided on private DNS 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 providers who are responsible for the numbers inserted.

Amendments to the ENUM database can only be performed by the communication providers responsible for that specific set of number(s) e.g. numbers for which they are the carrier of record.

New communication provider can only join a federation when certain conditions are met.

Perceived benefits from a private DNS arrangement include the ability of communication providers to support and manage high QoS requirements and the ability to avoid DDOS attacks.

7.3 Top level architecture

NGNs will not emerge at the same rate in all countries. Their introduction will vary from country to country due to market differences economic drivers and technological differences. On that basis it is envisaged that national databases that support NGNs, based on their national numbering schemes will also emerge. There are also other factors that support the introduction of national routeing databases. Number portability which is generally restricted to the porting of numbers within a national environment also argues for such an approach. Whilst it is accepted that theoretically many of the current constraints on number portability disappear with the introduction of NGNs, currently there are wide differences between national implementations, both at the technical level and with the essential processes that support this functionality. The rapid introduction of NGNs would be hampered if there was a need to change such arrangements in the near term. It also has to be recognized that NRAs across the globe place differing demands on carriers.

Within any scheme that aims to achieve full connectivity there is a need to provide a single top level database that will hold relevant information to enable top level routeing decisions to be made e.g. if the number cannot be resolved within a specific countries/networks database, where does that information reside? There will also be a need to ensure that customers with numbers held within other federations outside of a TISPAN IPX, can be reached.

Local copies of the master database can be held at the national level as well as local copies (or part thereof) at the network level.

Figure 5 shows the top level database architecture for TISPAN NGNs.

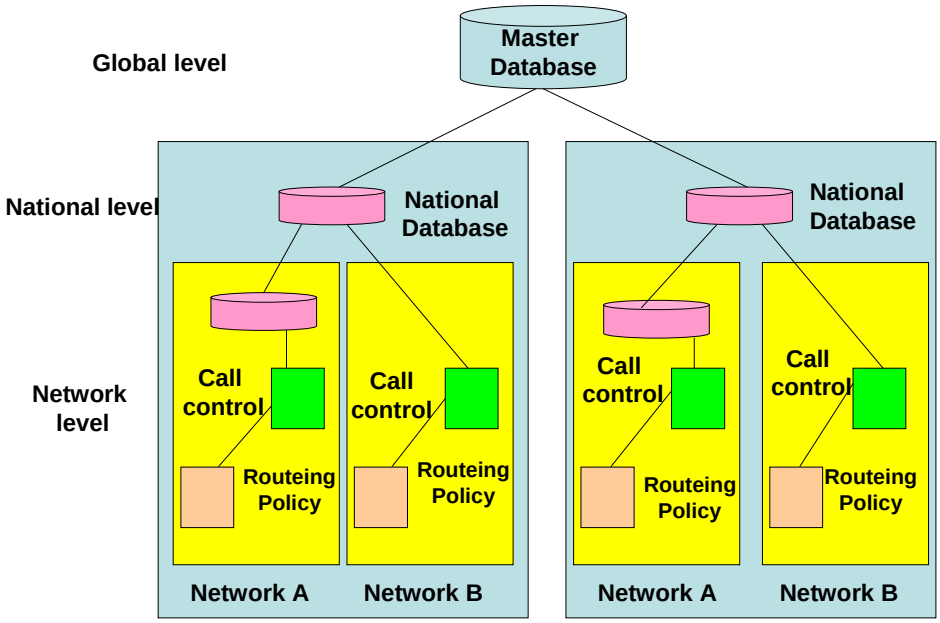


Figure 5: Top level database architecture

Key issues that would require in-depth analysis include:

- Choice of database technology and protocols used at each level of the hierarchy.
- The level of information held within each database (all numbers or partial numbers).
- Whether each communication provider holds a full or partial copy of the database within their own network.
- Caching/data refresh requirements.
- Number portability requirements.
- Detailed processes to support data exchange and possibly number portability.
- Security and stability.

Further detailed discussion on the provision of national common database arrangements falls outside of the scope of the present document. However it is envisaged that initially when most implementations are considered, decisions on the way forward will be taken by the involved parties on a national basis. Whilst within NGNs there exists the potential to provide service capabilities (e.g. roaming, nomadicity) that are not necessarily restricted by the use of nationally assigned numbers, it is recognized that the introduction of these new capabilities will demand careful consideration from both industry and the NRA who remain responsible for the administration of numbering resource at the national level.

The above issues underline the case for the provision of both routeing and number portability functions within a national environment, but in order to achieve full connectivity, interworking between different network federations/national implementations is required.

7.4 Routeing implementation within each carrier network and within national boundaries

The detailed method of implementing the numbering and routeing function within each network will remain a communication provider decision, impacted by the options available, cost, timescales, and to some degree geography as national implementations are likely to emerge in the early years. A number of scenarios and configurations are available whether a carrier opts for public or private DNS. Key questions that need to be considered include:

- Whether to use public or private DNS.
- Whether to become part of a pan industry group e.g. using public infrastructure such as a sub domain of .arpa or any domain specified within an industry group that utilizes private DNS.
- The preferred database technology e.g. DNS/ENUM at all levels of the hierarchy or DNS/ENUM within network or a different technology (e.g. Oracle DBs) at some levels.
- The type and level of information to be held in a top level database/server.

Whether the information is cached within each network and if so the level of data held.

8 Evaluation of options

I-ENUM is distinguished from user ENUM, defined in RFC 3761 [i.1], in which the entity or person having the right-to-use a number has the sole discretion about the content of the associated domain and thus the zone content. From a domain registration perspective, the end user number assignee is thus the registrant.

Within the I-ENUM namespace, we use the term "carrier-of-record" for the entity having discretion over the domain and zone content and acting as the registrant.

From the architectural options listed within clause 7 it can be seen that the main issue facing TISPAN is to decide between the use of the public or private DNS infrastructure. Decisions required at the national level can then be taken.

Using private DNS, each federation will be able to determine, control and administer all aspects of their implementation. The choice of domain name and structure of the name space will remain entirely under their control for the number(s) e.g. numbers for which they are the carrier of record . New Communications providers would be able to only join a federation when specific conditions are met that places them on a par with the other members.

Table 1 provides an indicative assessment of the requirements listed in clause 6 when judged against the ability to comply hen utilizing public or private DNS infrastructure. It should be read in conjunction with any notes listed within the table in order to understand the how each requirement has been assessed.

Table 1: Evaluation of public vs. private DNS options for TISPAN IPX

No	Requirement	Public DNS	Private DNS
	Top level Requirements		
1	Adherence to standards	Y	Y (note 1)
2	Single global approach supporting fixed and mobile communication providers	N (note 2)	Y
3	Secure environment	N (note 3)	Y
4	Shared control of infrastructure	Y	Y
5	End to end service delivery (facilitates more than best effort)	Y	Y
6	Facilitates service operability(not a resource intensive solution)	Y	Y
7	Enables efficient interconnect and peering and levels of trust	Y	Y+ note 4
8	Facilitates efficient and flexible service creation	Y	Y
9	Even playing field for all communication providers	Y	Y
10	Global approach	Y (note 5)	Y (note 5)
	Detailed requirements		
11	Comms providers can populate their DNS records	Y	Y
12	Fully qualified domain names are expected to return a result	Y	Y
13	Can Identify PoI for deliver to carrier of record	Y	Y
14	Choice of Domain enables reqd reliability and performance	Y	Y
15	Meets all privacy concerns	N (note 6)	Y
16	Implementable within required timescale	N	Y
17	Facilitates transition from early implementations	Y	Y
18	Minimize need to change RFC 3761 [i.1]	Y	Y
19	Work with fixed and variable number lengths	Y	Y
20	Minimize number of lookups	Y	Y
21	Minimize knowledge of numbering plan	Y	Y
22	Support interworking with private ENUM implementations	Y (note 7)	Y (note 7)

NOTE 1: Whilst private DNS does not have to use recognized standards , the intent within TISPAN would be to comply.
NOTE 2: Global DNS is not considered a viable option for mobile communication providers as the GSMA have adopted a private DNS solution.
NOTE 3: Whilst steps can be taken to provide enhance levels of security using public DNS, it is considered more insecure than private DNS as it is not possible to provide full protection against DDOS attacks.
NOTE 4: Whilst high levels of trust can be achieved within the public DNS e.g. through the use of DNSSec, etc., even higher levels of trust will exist between CPs if they share infrastructure that cannot be utilized by any entity outside of that federation.
NOTE 5: In principle the goal of achieving a global solution is best met through use of public infrastructure, however the fact that Private DNS implementations of ENUM for routeing already exist, or are planned e.g. GSMA/3GPP, then there is little difference between them as all will need to facilitate full interworking.
NOTE 6: Privacy of information remains a prime concern for communications providers. There is far more likelihood of information leakage or spoofing when using the public Internet, than within a private DNS environment.
NOTE 7: Whilst interworking with private ENUM implementations is possible, no agreed solution on how to achieve that at the global level currently exists.

9 Conclusions and proposed way forward

From the above assessment it can be concluded that whilst the provision of I-ENUM can be facilitated through the use of either public or private DNS, there are additional benefits from a private DNS implementation. It is therefore recommended that TISPAN adopt an approach based on the use of private DNS infrastructure for a TISPAN IPX.

It is also recommended that further work in ETSI TISPAN should concentrate on technical and operational principles required to facilitate the specification of the Master database as shown in figure 5.

In addition, recognizing that the GSMA have already advanced their studies in order to support the 3GPP environment, there appears to be a strong correlation between their approach and the ETSI TISPAN IPX requirements. Further synergies would need to be explored in order to facilitate ease of interworking between the GSMA IPX and ETSI TISPAN IPX environments.

History

Document history		
V2.1.1	February 2009	Publication