INTERNATIONAL INTERCONNECTION FORUM
FOR SERVICES OVER IP

(i3 FORUM)

(www.i3forum.org)

Workstream "Technical Aspects"

White Paper

Techniques for Carriers' Advanced Routing and Addressing Schemes

(Release 2.0) May 2011

Table of Contents

Executive Summary

As carrier voice interconnection evolves to an IP based architecture, carriers need to route the voice traffic based on the IP routable addresses rather than the direct E.164 format address (telephone number) for routing in the traditional PSTN network. Therefore, a solution is required to map the E.164 format address to an IP routable address that can be used for routing the call to its destination network in an IP environment. The destination network can be either the far-end user's service provider network or an intermediate network (carrier network) to transit the call.

An added complexity is introduced with number portability. Number portability allows a user to change its service provider while retaining the telephone number. A carrier prefers the number portability corrected data to make routing decision to effectively minimize the traffic transiting cost and increase the end-to-end quality level where possible.

The initial i3 Forum Technical Interconnection Requirements for International Voice Services document assumed route selection based on Country Code (and perhaps number block assignment within the CC) rather than the full E.164 number. It did not support definitive identification of the terminating service provider in the face of number portability, nor did it support routing decisions based on other individual number characteristics, e.g., supported services.

This document discusses what is required to enable carrier routing decisions to take into account number portability and other service/capability aspects of destination numbers.
The previous edition of this white paper provided an overview of the carrier interconnection techniques for advanced routing and addressing schemes. It specified some technical requirements for the provisioning and query interfaces and a set of the minimum information required in the addressing database that will allow carriers to exchange number portability corrected data. The main purpose was to set a standard for the carriers to develop their own routing and addressing solution and to promote the carriers' exchange of the number portability corrected data in order to identify the terminating network. The interface and database requirements were intended to be relatively independent of the solution architecture.

This release of the Routing & Addressing document offers a strategy for the evolution of routing and addressing taking into account the realities of the current environment. This strategy focuses on leveraging existing and planned service provider efforts to create registries for number portability corrected data and supplementing these to meet the particular needs of international carriers.

At this stage of the i3 Forum routing and addressing discussion, any routing policy, i.e. the least cost routing, is left to each carrier to manage based on the information made available via the mechanisms detailed in this document. Likewise the integration of the information into each carrier's Least Cost Routing (LCR) infrastructure along with the bilateral/multilateral agreement management is an individual carrier's responsibility.

1 Scope of the Document

International carriers traditionally exchange traffic, mainly for voice calls, based on the user dialed numbers. The traffic is routed to the selected carriers by the carrier dial code breakout considering both commercial and technical arrangements. Unlike the service providers who own the end users and the telephone numbers within their networks, international carriers usually do not consider the assignment of a number to a network when making routing decisions. When an end user telephone number is ported from one service provider network to another network, international carriers traditionally do not route the traffic based on the number portability corrected address.

The i3 Forum foresees an increasing demand for the carriers to route traffic intelligently to the other carriers who have the best quality and cost structure for terminating the traffic. This requires the carrier to receive the number portability corrected data in order to make a routing decision based on this information combined with other business considerations, e.g. least cost routing, etc. There are solutions available in the market for service providers routing their interconnect traffic to the terminating service provider network directly. (In the scope of this document, the term "terminating Service Provider" is to be understood as either a service provider network providing the local service to the destination user, or an exclusive carrier network that represents the underlying service provider.) However, the existing solutions may not always work for the international carrier community as the international carriers prefer to manage the routing decision within their own domains, often via the existing Interconnect Business Optimization (IBO) systems to factor the cost, quality, network capacity, service capability, e.g. CLI delivery capability, into the routing decisions.

The previous edition of this white paper provided an overview of the carrier interconnection techniques for advanced routing and addressing schemes. It specified some technical requirements for the provisioning and query interfaces and a set of the minimum information required in the addressing database that will allow carriers to exchange number portability corrected data. The main purpose was to set a standard for the carriers to develop their own routing and addressing solution and to promote the carriers' exchange of the number portability corrected data in order to identify the terminating network. The interface and database requirements were intended to be relatively independent of the solution architecture.

This release of the Routing & Addressing document offers a strategy for the evolution of routing and addressing taking into account the realities of the current environment. This strategy focuses on leveraging existing and planned service provider efforts to create registries for number portability corrected data and supplementing these to meet the particular needs of international carriers.

2 Objective of the Document

The objective of this document is to allow the participating carriers to obtain addressing (and routing) and service attribute information to facilitate effective and flexible bilateral/multilateral traffic exchange.

The solutions to be adopted by carriers should be able to achieve the following goals.

- Be able to obtain number portability corrected data;
- Be able to provide all necessary information for each carrier to decide the routing when such information is not available by other means;
- Be able to provide the information to support service based routing, e.g. far-end user characteristics and/or applications supported, including non-voice service, e.g. SMS, MMS. FAX etc.

- Be able to provide a smooth evolution path for the participating carriers with forward looking considerations;
  - The solution architecture should be flexible, scalable and evolvable;
  - Be able to inter-work or incorporate with other industry carrier federations/consortiums;
  - Start with focus on E.164 addressing, but evolvable to accommodate Non E.164 addressing.

3 Acronyms

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
CC	Country Code
CIC	Carrier Identification Code
CLI	Calling Line Identification
CPU	Central Processing Unit
DNS	Domain Name System
ENUM	E.164 Number Mapping
EPP	Extensible Provisioning Protocol
ESPP	ENUM Server Provisioning Protocol
FTPS	File Transfer Protocol over SSL
HTTP	Hyper Text Transfer Protocol
IBO	Interconnect Business Optimization
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISP	Internet Service Provider
ITU	International Telecommunications Union
LCR	Least Cost Routing
MMS	Multimedia Messaging Service
NAPTR	Naming Authority Pointer
NDC	National Destination Code
NNI	Network to Network Interface
NP	Number Portability
NPDB	Number Portability Database
NPDI	Number Portability Dip Indicator
P-FTP	Passive File Transfer Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RN	Routing Number
SCP	Secure Copy Protocol
S-CSCF	Serving Call Session Control Function
SFTP	SSH File Transfer Protocol
SMS	Short Message Service
SPID	Service Provider Identification
SPN	Service Provider Number
SS7	Signalling System 7
TLS	Transport Layer Security
TN	Telephone Number
URI	Uniform Resource Identifiers
VPN	Virtual Private Network
XMPP	Extensible Messaging and Presence Protocol

4 References

[1] I3 Services Work Stream – Routing and Addressing Services for International Interconnections over IP (v 1.0) June 2010

[2] GSMA PRD IR.67 - DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers – August 2010

[3] IIETF RFC 6116 The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM) – March 2011.

[4] IETF RFC 4769 IANA Registration for an Enumservice Containing Public Switched Telephone Network (PSTN) Signaling Information – November 2006

[5] IETF RFC 3261 SIP: Session Initiation Protocol – June 2002

[6] IETF RFC 4694 Number Portability Parameters for the "tel" URI – Oct 2006

[7] IETF RFC 3588 Diameter Base Protocol - September 2003

[8] IETF RFC 4740 Diameter Session Initiation Protocol (SIP) Application - November 2006

[9] IETF RFC 5730-3735 Extensible Provisioning Protocol (EPP) -August 2009

[10] IETF RFC 5731 Extensible Provisioning Protocol (EPP) Domain Name Mapping –August 2009

[11] IETF RFC 5732 Extensible Provisioning Protocol (EPP) Host Mapping – August 2009

[12] IETF RFC 5733 Extensible Provisioning Protocol (EPP) Contact Mapping – August 2009

[13] IETF RFC 5734 Extensible Provisioning Protocol (EPP) Transport over TCP – August 2009

[14] IETF RFC 3735 Guidelines for Extending the Extensible Provisioning Protocol (EPP) – March 2004

[15] IETF RFC 4114 E.164 Number Mapping for Extensible Provisioning Protocol (EPP) - June 2005

[16] PacketCable ENUM Server Provisioning Protocols (ESPP) CableLabs PKT-SP-ENUM-PROV-I03-090630

[17] IETF RFC 1034 Domain names - concepts and facilities –November 1987

[18] IETF RFC 1035 Domain names – Implementation and specification –November 1987

[19] IETF RFC 1995 Incremental Zone Transfer in DNS–August 1996

[20] IETF RFC 1996 A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)–August 1996

[21] I3 Technical Work Stream – Security for IP Interconnections over IP (v 1.0) May 2011

[22] IETF RFC 5067 Infrastructure ENUM Requirements – November 2007.

[23] IETF RFC 6117 IANA Registration of Enumservices: Guide, Template, and IANA Considerations – March 2011.

[24] IETF RFC 6118 Update of Legacy IANA Registrations of Enumservices: – March 2011

[25] IETF RFC 5526 The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application for Infrastructure ENUM - April 2009

5 Supported Services

The purpose of this document is to define needs for the query, provisioning, and replication interfaces as well as the general solution requirements for carriers to obtain the addressing and the service attribute information to support the following two service categories:

- International carrier traffic routing

The received addressing information from service providers supplemented by that exchanged with other carriers will allow a carrier to route the traffic to its international bilateral/multilateral carrier of choice and avoid expensive charges and quality degradation from the extra transiting hops. Many Mobile Network Operators and Cable Network Operators have already established the peering relationships within the network operator community. However, there are some additional requirements from the carrier perspective to support the carrier bilateral/multilateral traffic exchange and essentially move from country-to-country to carrier-to-carrier routing. One of the requirements is for carriers to manage the final routing decision based on other business considerations, i.e. least cost routing, bilateral overage traffic cost etc. Other requirements involve quality considerations driven by the far-end user service attributes and the underlying carrier capability.

- Service based routing

Specific service based routing will allow a carrier to make the routing decision based on the services supported by the far-end user and the underlying carrier service supporting capability. For instance, a carrier could choose another carrier A as its default interconnect provider but carrier B for some specific service types, e.g. FAX/IFAX.

At the initial stage of the i3 Forum routing and addressing discussion, the focus is for the carrier to obtain the number portability corrected data based on E.164 address to support routing in the IP environment. The actual routing policy, e.g. the least cost routing, the specific service based routing, is left to each carrier to manage. This offers a simple solution for participating carriers to benefit before a full set of the services, e.g. the routing policy management, is supported.

5.1 Information Elements Required

The document [1] by i3 Forum Service Work Stream covers the routing and addressing market requirements from the carrier community's perspective.

Based on the requirements identified by the i3 Service Work stream, two types of information about E.164 numbers are desired to enhance carriers' routing decisions are:

- Terminating service provider identity. The information to identify the terminating service providers network, e.g., a unique service provider ID (SPID) or a domain name in the SIP URI that contains the network identity[1]
- Services and capabilities associated with a number.

The information obtained is the input to carriers' routing decisions; routing decisions remain with each carrier. Thus, what is desired are information elements to be input to carriers Least Cost Routing mechanism rather than URIs to be directly utilized by carrier's call control elements to initiate a SIP INVITE. Each carrier's least cost routing mechanism provides the mapping from a terminating service provider identity to a carrier or a group of carriers for routing.

[1] While an SPID is preferable, a SIP URI might be used for compatibility with certain registries, such as the GSMA's PathFinder.

5.2 Information Sources

5.2.1 Terminating Service Provider Identity

There are four sources that can potentially provide the terminating service provider identity to a given E.164 number.

- Carriers who have the knowledge of their represented service provider E.164 number database; These carriers may benefit the most from this solution and are more likely to provide this address data than other potential sources;
- Service providers who own the end user and their E.164 numbers; It might be a challenge finding incentives for these service providers to supply their E.164 numbers as they may not directly benefit from the carrier solution;
- National or regional number registries and Number Portability Databases (NPDB);
- Other existing industry carrier federations/consortiums address databases.

Authoritative SPID information is in some, but not all cases available from national number registries and number portability databases where they exist, e.g., in the USA and Canada. These sources may not provide information about the entity maintaining the retail relationship with the end users.

Carrier or service provider sourced SPID information cannot be regarded as authoritative unless verified again authoritative sources. Without the authoritative verification, the SPID can still be used, at the carrier's discretion, for the carriers who have the bilateral/multilateral routing relationship.

As of today, there is no global standard for SPID. Therefore, Number portability databases cannot provide a standard SPID. They may provide a national SPID or a routing number (rn) and may continue to do so even after a world-wide SPID is standardized. Deriving a global SPID, may require a mapping table in a registry and, in the routing number case requires a further translation. Mapping could also be done by the querying carrier, although that would require each carrier to develop mappings for each country. There are, however, efforts underway that could lead to a standard global SPID as discussed in section 9 below and these represent the best path forward.

In nations that allow number portability but do not implement a central number portability database there may be no direct authoritative source for SPID. Existing number plan information may identify the provider that originally served a ported number but only that entity may be able to identify the current service provider.

Efforts by service providers to build registries for their own purposes represent the most likely path to authoritative data. It should be recognized that service providers are the ultimate source of the terminating service provider identity and capability information that international carriers desire. SPs have their own incentives for making this information available in registries and i3 members will be better served by leveraging that activity as opposed to developing a separate infrastructure

5.2.2 Services & Capabilities

Service and capability information, on the other hand, is generally not available in national number portability databases but is only known to the serving providers.

When the terminating service providers are represented by an exclusive carrier, the carrier may provide the service and capability information.

Again, efforts by service providers to build registries for their own purposes represent the most likely path to authoritative data.

6 Routing and Addressing Data Exchange Architectures

6.1 Call Model

Before considering candidate architectures for the exchange of routing and addressing data, it is useful to consider how such data will be employed in the route selection process during session setup. A call control element (such as an S-CSCF) presumably queries some server to determine a route. The routable URI returned reflects the outcome of an LCR decision. The data discussed in this document (SPID, Services/Capabilities) are inputs to the LCR decision. Carriers (or their LCR vendors) need to carefully consider how to most efficiently structure information flow. For example, should the registries (or local copies or data stores) envisioned in this document be queried by the call control element or by the routing server? In the former case, the call control element will have to pass the info to the routing server for processing. Alternatively, the routing server could perform the query in response to the request from the call control element. This would also allow the query to be bypassed in cases where the server does not need additional information to make a decision (e.g., the carrier has only one route to a particular country or NDC.)

Figure 1 below illustrates the call model. Carrier 1 seeks to terminate a call to the telephone number associated with the phone at the right, which has ported from Service Provider 1 to Service Provider 2. Routes from several carriers (A,B,C) are available but the IBO/LCR system makes use of additional information from the Addressing Registry to select Carrier B.

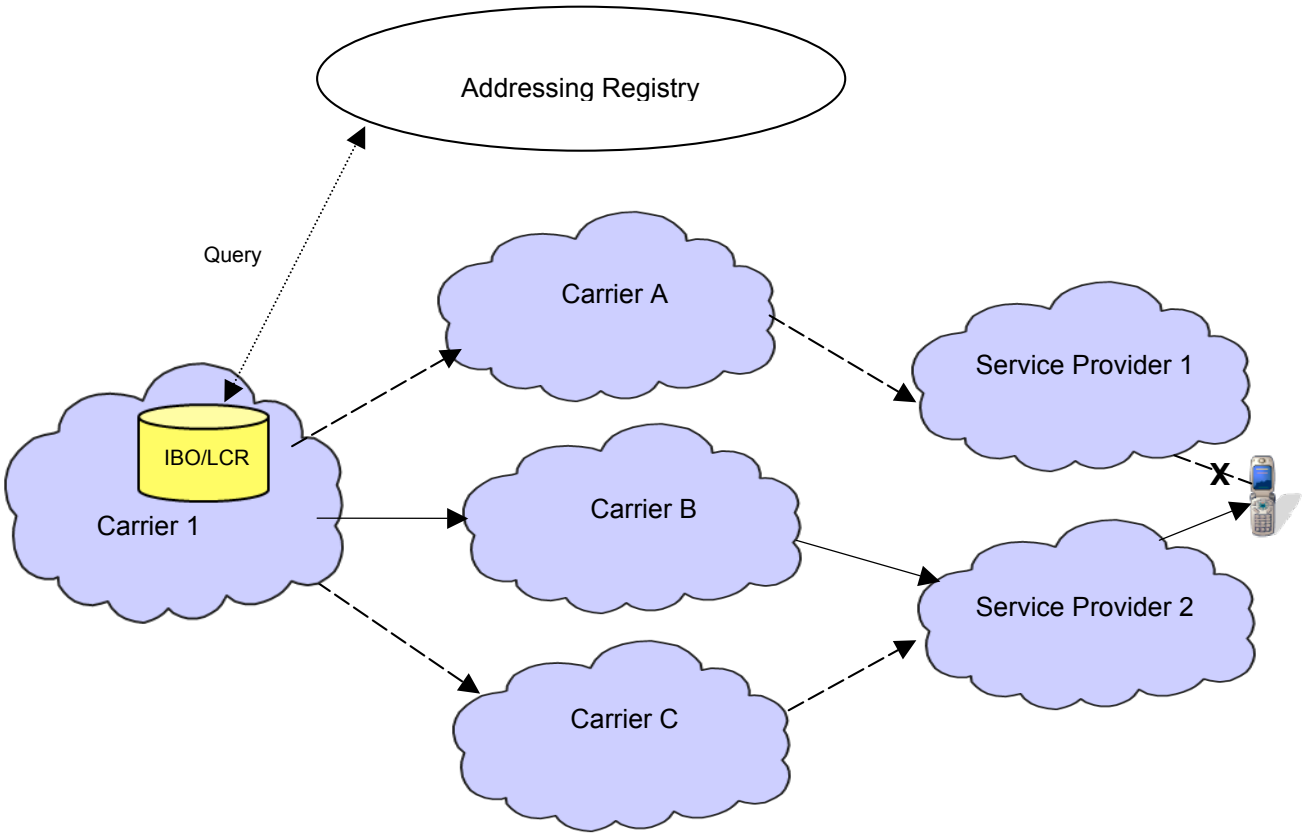

Figure 1 - Call Model for International Carrier Route Selection

6.2 Architecture

Exchange of routing and addressing data may take place bilaterally between carriers or mediated by a shared registry. While certain exchanges might take place bilaterally, they can become complex as the number of carriers involved increases. Thus at the international level, carriers do and will continue to make use of shared addressing registries.
These registries can be the result of cooperative industry initiatives, with or without regulatory involvement, or commercial vendor proprietary offerings. In either case they will be mostly supported by third party registry service providers.

Annex 1 discusses some of the architectural forms that registries may take. Since, as discussed above, international carriers are not the sources of the number portability and service capability information they need for routing decisions, except in so far as they also happen to be end user service providers, international carriers are unlikely to control the architecture of such registries, which are more likely to be instantiated driven by the needs of service providers moving to IP interconnection for domestic traffic exchange. The previous release of this document does, however, outline the characteristics international carriers would desire in an architecture:

- Data sharing based on bilateral/multilateral agreement and defined authorization policy;
- Automatic data replication among authorized carriers with bilateral/multilateral agreement;
- Near-real time data update for data to be number portability corrected;
    - Each Carrier is responsible for providing and updating the addressing data that the carrier represents;
    - Data is directly or indirectly synchronized with each country's national, regional or carrier based Number Portability Database (NPDB) to prevent false ownership declaration.
- Interoperability with other industrial carrier federations/consortiums.

6.3 Industry Existing Architectures

Some service provider sponsored registries are already under development. Two instances are discussed below. These are in addition to vendor proprietary registry offerings.

6.3.1 - GSMA

There are vendor specific routing and addressing solutions available in the market as well as some solutions proposed by the industry service operator associations. One of the existing architectures proposed by GSMA is an implementation of Carrier ENUM as detailed in GSMA document IR.67. [2]

The GSMA defines one tree, where the root is identified by the domain e164enum.net with a flexible tiered structure below it. Below the root (tier 0) is a tier 1 level, which is at a country level. As an example, a UK tier-1 would be responsible for the sub-domain 4.4.e164enum.net (UK = +44 country code). Number portability is also managed at the tier 1 level. Below the tier 1 level is the retail operator level at tier-2 level. Tier-2s are responsible for providing the NAPTR records.

Tier 0 – Global level (e.g. Root DNS server)
- Authoritative for the top level domain ("e164enum.net").
- Under this domain are pointers to the Tier 1 authoritative servers.

Tier 1 – Country level (CC)
- Authoritative for country code (e.g. "4.4.e164enum.net" for country code +44)

- Under this domain are pointers to the Tier 2 authoritative servers (portability corrected).

Tier 2 – Operator level (NDC)

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

The GSMA proposal recognizes that the tier structure will vary on a national basis. For example, where number portability has been implemented carriers may no longer be authoritative for an NDC and the Tier 1 may contain delegations for individual subscriber numbers. Alternatively, some providers may wish to provision their NAPTR records onto a common server, resulting in a combined Tier 1 and 2.

6.3.2 Country Code 1 ENUM LLC

Another example of a service provider driven architecture is presented by the ENUM registry being developed by the Country Code 1 ENUM LLC.[2] Consistent with the GMSA effort, it adopts ENUM as the query protocol and makes use of a tiered structure. The common registry provides a combined Tier 0/1 (until interworking with a global Tier 0 can be developed) which contains NS records that point to service provider maintained Tier 2 name servers that provide the actual NAPTR records. This allows service providers to control routing and supports partitioning (see Section 12 below) without requiring SP-specific service logic in the Tier 1 shared industry registry . In the case of the USA, which is the initial focus of the CC1 ENUM LLC effort, the availability of a national number portability data base allows for a registry that is authoritative.

7 Query Interface

The query interface is for carriers to obtain Service Providers' identities and service capabilities information. Such information can be acquired from a shared registry or via a carrier-to-carrier bilateral relationship. The previous release of this document outlined a number of possibilities for a query interface including:

- ENUM/DNS (RFC 6116 [3] & 4769 [4])
- SIP Redirect (RFC 3261 [5] & 4694 [6])
- SS7 MAP/TCAP
- DIAMETER RFC 3588 [7] & RFC 4740 [8]

After consideration of their relative merits the i3 Forum to focused on the use of ENUM and SIP redirect as resolution mechanisms.[3] While a variety of approaches may be used in the interim, the i3 recognizes the emerging consensus with respect to ENUM, particularly since SIP redirect cannot address provision of service and capability information whereas ENUM can already address most needs and can easily be extended to address the others.

Carriers with local address resolvers can define their own query interface. This option requires carriers replicate the registry data in a local store that can be accessed by their chosen query protocol.(Replication in a local store requires ongoing synchronization with the Registry.) Carriers who do not have local address resolvers query an external addressing registry database; countries that disallow local replication of the number portability data require the carrier to query the national registry.

[2] http://www.enumllc.com/
[3] It is recognized that SIP is not a query protocol, although in this document it is used as a query resolution mechanism.

7.1.1 ENUM Query Protocol

An ENUM query returns portability corrected information (potentially including PSTN number portability parameters) and can convey service information via the *enumservice* field as detailed below and in the section 10 of this document.

ENUM Query and Response

The ENUM query interface supports a standard DNS query as defined in RFC 6116 [3]. An ENUM query returns a NAPTR (Naming Authority Pointer) record. ENUM is inherently number portability corrected, meaning that the records returned reflect the current service provider of record.

Information on the current service provider for a PSTN number may be reflected in at least three ways:

- A NAPTR record may resolve to a SIP URI that identifies the service provider's ingress point, e.g., in the hostname, for example

```
$ORIGIN 3.2.1.0.5.5.5.5.1.2.1.e164.arpa. NAPTR 10 100 "u" "E2U+pstn:sip"
        "!^.*$!sip:+12155550123@gw.serviceprovider1.com;user=phone!".
```

- A NAPTR record may resolve to a tel URI that includes number portability information per RFC 4769

```
$ORIGIN 3.2.1.0.5.5.5.5.1.2.1.e164.arpa. NAPTR 10 100 "u" "E2U+pstn:tel"
        "!^.*$!tel:+12155550123;npdi;rn=2155550199!"
```

- As discussed below, ENUM queries may eventually return an SPID that directly identifies the terminating service provider without providing any routing information.

ENUM is focused on returning URIs via NAPTR records. This may complicate the task of the carrier's LCR platform in extracting the service provider and service/capability information it needs for routing. On the other hand, nothing prevents an ENUM query from returning TXT records that could contain arbitrary information to be defined by the i3 to support its needs, for example the SPID discussed in Section 9 or agreed-to capability information that is not suited to the URI format.

Presentation of Number Portability

An ENUM query response that returns the number portability (NP) information does so by populating multiple parameters as detailed in RFC 4769 [4]. The carrier that receives the query response can route the call based on the NP information. The NP parameters are Routing Number (rn), rn-context, Number Portability Dip Indicator (npdi), cic, cic-context and Service Provider Identifier (SPID). Another option is to use SIP URI to capture the routing information in the domain name.

Considering the i3 Forum's position to promote the inter-carrier bilateral/multilateral traffic exchange, the SPID is recommended to present the number portability corrected address data. Unlike a service provider peering agreement where the parties simply exchange each other's organic traffic, the carrier bilateral/multilateral agreement has other factors to consider:

1. A carrier bilateral/multilateral agreement assumes a commercial value, often rate per minute or rate per message to the traffic being exchanged. The imbalance traffic is usually given a higher overage rate that could result in the carrier choosing to route the imbalance traffic through other hubbing agreements.
2. A carrier can claim its representation of any service providers based on the cost structure, i.e. via a service provider peering agreement. In such situations, the traffic originating carrier requires the flexibility to route the traffic outside of the bilateral/multilateral agreement as needed.

At the current stage of the analysis, the carrier will manage the routing within its own network based on the addressing information received from the query response. The service provider information for any given E.164 address is sufficient for the carrier to make the routing decision based on various bilateral/multilateral and hubbing agreements, which often is managed via the carrier owned Interconnect Business Optimization (IBO) system. The IBO system usually factors the vendor dial code breakouts, underlying carrier cost, quality and service capability as well as network capacity into the routing decisions. The carriers would encourage the IBO system vendors or the carrier's own developers to enhance the IBO solutions to accommodate the advanced routing and addressing requirements outlined in this document towards a fully integrated solution for the carriers in the near future.

As noted, applicability and use of rn is not standardized across countries and a global standard for SPID is still a work in progress as detailed in Section 9 of this document.

7.2 Transport and IP Security for Query Interface

Interconnection between a carrier and the registry provider for queries may, like interconnection between carriers, be either private or public. A mix of solutions may be employed, even by an individual carrier, depending on the circumstances of their relationships to different registries.

7.2.1 Private Interconnection

Private interconnection might take the form of either a private line or a VPN using a shared facility separate from those carrying Public Internet Traffic.

- Private Line
  A dedicated transport link would be deployed between carrier and the addressing database. The link provides:
  - IP connectivity for Query interface;
  - A dedicated physical link to prevent any potential security risk from other networks;
  - Guaranteed bandwidth to offer good QoS control for Query traffic.

  However this option also has some limitations:
  - Scalability issue for building private line to each individual carrier requiring query access to the addressing registry database;
  - High cost for implementing and maintaining those links.

- VPN over Shared Facility
  This option takes advantage of a Virtual Private Network (VPN) service from third party provider to offer IP connectivity for Query Interface.
  - Traffic in the virtual network is tunneled through the underlying transport network (Layer3, Layer2, IPSec etc.)

- The proposed solution is to transfer query information on a multipoint-to-multipoint environment;
- This makes the addressing database query available for all carriers who join the VPN;
- It reduces the complexity of having dedicated VPN for each carrier.

Although the nature of VPN makes most security threats from public network impossible, some additional security measurements are still required in a multipoint-to-multipoint environment:[4]

- A security device, e.g. stateful firewall etc., should be deployed in front of the addressing database server farm to protect the system from potential security threats from other operators;
- Each individual operator may also want to deploy their own security device based on internal security policies to prevent the VPN gaining access to its entire corporate network.

- End to end QoS policy is available for query traffic;
- VPN service is generally available internationally from various VPN providers;
- Easy to manage and maintain a single network to handle all query traffic.

The limitations of this option are:

- VPN service from one provider might not be available at certain International locations;
- To maintain a consistent end to end QoS policy might prove challenging for the multiple VPN providers required to cover all locations. The multiple VPN providers will have multiple NNIs among them to limit end to end QoS policy.

7.2.2 Public Interconnection

Public interconnection could take the form of direct use of the Public Internet or may involve VPN techniques as discussed under Private Interconnection above.

- Public Internet
  This option utilizes the Public Internet to provide IP connectivity for Query Interface. It has following benefits:
  - Addressing database could be accessible from most of area in the world;
  - Most carriers would have a reliable internet access in place based on the IP peering links with many other carriers from the ISP perspective;
  - The lowest cost solution to offer IP connectivity for Query interface.

  The concerns for this option are:
  - Both carrier and addressing database infrastructure are exposed under all security attacks on the public Internet;
  - QoS is not available on the public Internet;
  - Security mechanisms have to be in place to protect both carrier and addressing database infrastructure and the transactions between them:
    - Stateful Firewall / ACL (Access Control List) to only allow particular hosts and applications to communicate each other;
    - IPS/IDS (Intrusion Prevention System and Intrusion Detection System) to prevent any security threats on Public Internet;
    - Encryption (TLS, IPSec, etc.) to protect the confidentiality of messages.
    - Use of DNSSEC should also be considered

[4] Further discussion of security requirements for the query interface is contained in [21].

8 Provisioning & Replication Interfaces

In addition to a query interface registries also require interfaces to support provisioning of data, and, where registry data is replicated into service provider/carrier local stores that are queried in place of or in addition to the central registry, a corresponding replication interface. Figure 2 below shows the various interfaces associated with the Addressing Registry.

Provisioning and replication interfaces for service provider developed registries will be driven primarily by service providers. The i3 Forum can best address its members' needs by ensuring that those interfaces also meet the needs of international carriers. Some general themes were identified in the first release of this document.

Provisioning/replication interfaces are required for carriers to update the addressing data into the addressing registry database as well as for carriers to download the authorized addressing data to the local resolver, when such registry database exists.

The defined addressing Data Replication interface/protocol should support both incremental replication and bulk replication.

The defined addressing Data Replication interface/protocol also needs to support the additional reference interfaces to connect other carrier federations/consortium registry service providers and the selected country national or regional based number portability databases, when required. The national or regional based number portability database access offers not only an authoritative source to verify the carrier provided E.164 number owner of record, but also an alternative data source to gain the full E.164 numbers of a nation or region covered by the number portability database.

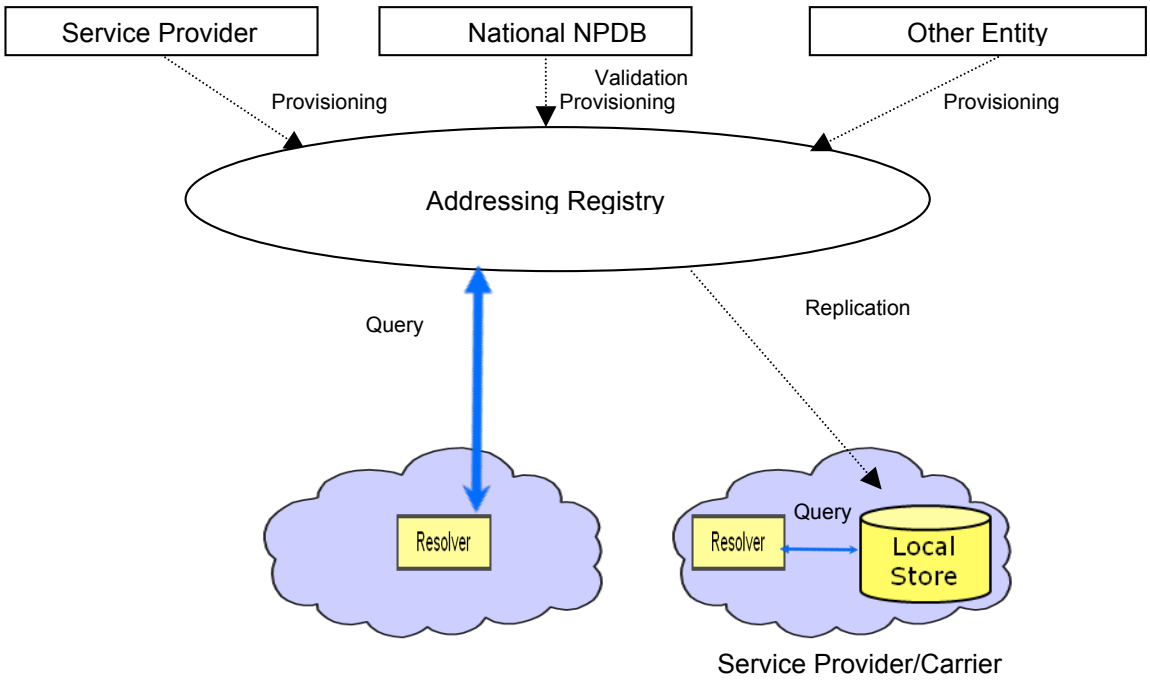

Figure 2 Addressing Data Provisioning, Replication, and Query Interfaces

The query objective is to obtain address data, i.e. SPID and service/capability information. Routing decisions should be managed by the originating carrier based on the address data and on any other available information, e.g. using Least Cost Routing data.
Interface RequirementsProvisioning interface requirements consists of both interface requirements and database requirements.

Interface Requirements

- Support a file-based data transfer mechanism;
- Support both incremental updates (real time, connection oriented) and bulk update (trigger from manual process);
- During bulk updates the server should not accept incremental updates from the same source
- Authentication, integrity and confidentiality;
- Support efficient transportation of a large number of data model objects;
- Ability to add, modify and delete the objects defined in the data model;
- Data storage and transfer optimization, simplify the distribution of redundant information or records, i.e. TN to SPID mapping, support block of TN's transfer;
- Support uploading and downloading policy control to allow or disallow a carrier to download another carrier addressing data and/or to query the data.

Database Requirements

- Support a large addressing space – same magnitude as the PSTN (registry requirement);
- Data uploading and downloading policy control as well as the query authorization information are linked to the source of the address information;
- Alert object data conflicts received from multiple clients;
- Support multiple uploading streams into same server from different sources simultaneously;
- Data storage and transfer optimization, simplify the distribution of redundant information or records, i.e. TN to SPID mapping, support block of TNs storage;
- Manage conflicting uploading streams into the registry from different sources simultaneously.

Potential Provisioning Interfaces

Given that Registries will be built by service providers the i3 Forum may not be able to control the provisioning interface selected.
For servers using the ENUM query interface, there are some candidates available in addition to vendor proprietary interfaces:

- Extensible Provisioning Protocol (EPP) as defined in RFCs 5730-5734 [9]-[13] and RFC 3735, [9], and RFC 4114 [15].
- Enum Server Provisioning Protocol (ESPP) defined by CableLabs PKT-SP-ENUM-PROV-I03-090630 [16].
- The IETF drinks (Data for Reachability of Inter/tra-Network SIP) working group is currently pursuing specification of a protocol for such provisioning.

The i3 Forum will need to track ongoing developments.

Potential Replication Interfaces

In addition to proprietary interfaces, DNS bulk zone transfer (RFCs 1035 [17] and 1035 [18]) and incremental zone transfer (RFCs 1995 [19] and 1996 [20]) could be employed. The work of the IETF drinks group may also produce additional alternatives.

8.1 Transport and IP Security for Provisioning & Replication Interfaces

The IP connectivity requirements for Provisioning are similar to the query interface requirements as discussed in Section 7.1. The proposed approach is to share the same IP infrastructure for both Provisioning and Replication and Query interfaces.

In addition, the data replication function of the Provisioning interface requires a mechanism to pass the bulk data in a fast and secure method[5]. The following protocols, as examples, can be implemented for file transfer with the security consideration:

- Secure Copy Protocol (SCP);
- Passive File Transfer Protocol (P-FTP);
- SSH File Transfer Protocol (SFTP);
- File Transfer Protocol over SSL (FTPS).

9 Service Provider Identity

A service provider carrier ID schema needs to be standardized as part of the solution. The Services Workstream has created a draft document proposing use of a globally defined 8-digit numeric SPID with the following characteristics:

- Globally unique.
- Flat in structure.
- Only numeric digits (0-9).
- Fixed length.
- At least 8 digits, giving 100 million possible identifiers.

Administratively

- Global SPID identifiers should be available to all entities that require them and not limited to licensed operators or 'Carriers of Record'.
- Global SPID identifiers should be assigned by an international assignment body.
- Global SPID identifiers should be able to be reassigned and reused by the entity they have been assigned to (though not delegated to outside entities). The assignment body should not reuse them however.
- Entities should be able to apply for multiple Global SPID identifiers as required for their routing purposes.
- There should be a range of Global SPIDs provided for the use within a network for internal purposes. These Global SPIDs should be private to the user's network.
- There should be a range of Global SPIDs in which a specific initial digit sequence indicates that what follows will be a SPID consisting of an E.212 Mobile Country Code and Mobile network code with padding where required for carriers that wish to define a SPID based on their E.212 assignment.

Because the i3 Forum itself or even international carriers themselves will not be developing a registry, it is important to settle on a SPID that is likely to be accepted by the parties (i.e., service providers) that have or will take on that task.

GSMA IR.67 now assumes that the ITU SG 2 will eventually standardize a Service Provider Number that would be used as follows:. For example for IPX use between IMS systems, the identifier would be as described in the table below extracted from IR.67:

Domain Name	Sub-domain(s)	Explanation	Rules of Usage	Resolvability
.ipxsp.org	spn<SPN>.ipxsp.org Where <SPN> is the Service	Not used in any particular service,	Each Service Provider is	Domain needs to be resolvable by

[5] Further discussion of security requirements for the provisioning and replication interfaces is contained in [21].

	Provider Number (as defined in ITU-T E.xxx [41]) of the Service Provider. An example is: "spn001.ipxsp.org". Further sub-domains under this are the responsibility of the owning Service Provider. However, it is recommended to use/reserve the sub-domains defined above for the domain "mnc<MNC>.mcc<MCC>.3gppnetwork.org".	however, can be used by any Service Provider for any service they see fit. The main intention is to provide a domain name that Service Providers without an E.212 number range allocation can use when connecting to the IPX network.	allowed to use only SPNs that are allocated to them by ITU T.	at least all roaming/interworking partners for the services used by this domain name.

10 Information to be stored in IP routing directory

The data model objects should include:

- Public Identity: TN or TN range
- Service Provider Identity
  - SPID is suggested
  - Alternatively, service provider identity might be derived from the domain in the host portion of a SIP URI encapsulated in a NAPTR record or the number portability parameter rn (routing number), from RFC 4769 where an appropriate national standard has been defined [4].
- For shared databases, Source Identity: Carrier or federation ID to show the data source, this could be a carrier identification or a carrier federation/consortium ID. This source identity information is required to trace any data in the registry to its original source. When a data conflict occurs, e.g. two sources provide different SPIDs on a same E.164 number, the source of data can be identified to manage the conflict. Source information may also be needed for route selection purposes. First, while some registry implementations restrict provisioning to the carrier of record for a number, others allow any participating entity that can provide termination to the E.164 number in question to provision routing information[6]. In this case it is necessary to identify the entity associated with particular routing information and also important to distinguish which entity, if any, is the carrier of record. Second, some registries may, as some number portability databases, distinguish between the network service provider for a number (akin to the carrier of record) and a reseller entity that provides retail service to the end user associated with the number. In such cases, an "alt SPID" is sometimes provisioned to identify the retail account holding entity.
- End user service objects: far-end user characteristics and/or applications supported. For ENUM a set of the *enumservice* registrations triggering different URI schemes has been defined (http://www.iana.org/assignments/enum-services) as per the table below (see

[6] RFC 5067 [22] provides the following definition of carrier of record:
o The Service 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,
o if the number is ported, the service provider to which the number was ported, or
o where numbers are assigned directly to end users, the service 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 national authorities.

RFCs 6117 [23] and 6118 [24]). The service types can be identified and returned to the originating carrier upon ENUM query. Such information is optional for the originating carrier to use during the routing decision making.

Service	URI Scheme
H323	h323
SIP	sip or sips
IFAX	mailto
PRES	Pres
WEB	http or https
FT	ftp
EMAIL	mailto
FAX	Tel
SMS	Tel
EMS	Tel
MMS	tel, mailto
E.164 to VPIM	mailto
E.164 to VPIM LDAP	mailto
VOICE	Tel
PSTN	Tel
PSTN	Sip
VCARD	http or https
XMPP	Xmpp
IM	XMPP
VOICEMSG	sip, sips, tel, http or https
VIDEOMSG	sip, sips, http or https
UNIFMSG	sip, sips, http or https
ICAL-SCHED	http or https
ICAL-ACCESS	http or https

When a terminating device supports multiple services, e.g. both pstn and mms, an ENUM query can return multiple NAPTR records as per the following example.

```
$ORIGIN 3.2.1.0.5.5.5.5.1.2.1.e164.arpa.
    NAPTR 10 100 "u" "E2U+pstn:sip"
    "!^.*$!sip:+12155550123;npdi;spn=5xxxx@gw.example.com;user=phone!".
    NAPTR 100 10 "u" "E2U+MMS:mailto"
            "!^.*$!mailto:+1-215-555-0123@gw.example.com!"
```

As noted in Section 7.1.1 embedding of service information in NAPTRS/URIs may raise some issues and alternative DNS Resource Record (RR) types might also be considered. Such records will be important to provide a global SPID and information about service capabilities that do not easily fits in the NAPTR framework which relies on protocol URIs. Given the failure of the IETF to, so far, advance a specific alternative to NAPTRs, resort to TXT records may be required.

11 IP Routing Directory Security and Accounting Requirements

The i3 Forum believes that registries need to cover the following security requirements:

- Protect against malicious attacks (e.g. Denial of Service, man-in-the-middle) at IP and session layer protocols (e.g., ENUM/DNS, SIP, Diameter);

- Provide AAA (Authorization, Authentication, Accounting) for user login, provisioning and service query:
  - Query permission or data replication permission;
  - Carrier based authorization on selected service provider data view and update;
  - Service data access permission;
  - Usage reports, e.g., number of the total queries, percentage of the successful queries, number of network list updates in predefined common format.
- Support transaction security:
  - Provisioning transaction;
  - Querying transaction;
  - Transport and IP security has been discussed in the query interface and provisioning interface sections.
- Data integrity;
  - Integrity check while data is being exchanged between parties.
- Provide user administration.

12 IP Routing Directory Data Partitioning Requirements

The proposed solution should support logical partitioning (not necessarily physical partitioning) of data as follows:

- "Vertical partitioning" to allow different querying parties to receive different responses with respect to numbers/addresses stored in the registry. For example, only permitted parties may replicate the data of a given service provider E.164 numbers to their own domains, or only permitted parties may query but not replicate a given service provider's E.164 numbers.
- "Horizontal partitioning" to allow different subsets of the service attributes data to be presented for a specific number/address. For example, a registry might contain data for a set of service attributes of a given E.164 number but a given party may only be permitted to query or replicate a subset of those attributes. The subset can be defined as none, selected, or all service attributes available.

Note that partitioning may be achieved at different levels in a hierarchically distributed database (see e.g., Section 6.3.2.)

13 IP Routing Directory Scalability Requirements

The i3 Forum expects registries to address the following scalability requirements:

- To accommodate the transaction traffic growth and avoid a single point of overload
- The routing directory architecture is implemented in a way to avoid network wide directory registry changes due to a single point of data registry change or addition (e.g. change to an existing member's data registry or addition of a new member);
- The adopted IP addressing directory architecture shall be vendor and protocol independent;
- Additional business rules can be introduced without impacting the existing business rules and functions.

14 IP Routing Directory QoS Requirements

The following metrics are recommended quantify the QoS of the IP routing directory:

- Query response latency
- Query loss/failure
- Query service availability
- Replication service availability
- Provisioning availability
- Update latency

- Accuracy.

It is expected that Registries would also monitor the following kinds of metrics to help assure appropriate QoS:

- Operational Statistics for monitoring usage and forecasting the possible exhaustion of hardware, software and system resources with the traffic volume growth trend:
  - Examples of resources are CPU, Memory, Disk Space, Software Threads, Software Usage based Licenses (Right-To-Use).
- Query Transaction Statistics
  - Total Transactions (successful, failed, aborted etc.);
  - Transactions per destination code, destination code can be either a destination service provider ID or an information source ID to identify the owner of the addressing data;
  - Transactions per carrier origination;
  - Referral transactions to other carrier federations/consortium registry service providers.
- Database update / provisioning statistics.

15 Summary

This White Paper outlines the requirements to supply the carrier community with advanced routing and addressing schemes. The solutions discussed in this document aim to support the international carrier traffic exchange based on number portability corrected data and service based routing by considering the terminating device service characteristics and the underlying carriers' service supporting capabilities.

This White Paper specifically recommends:

- Terminating service provider identity and the service attributes of a given E.164 number need to be supported by the addressing registry;
- Carriers make the final routing decision within their own domains based on the terminating service provider and service attributes data received from the query;

ENUM is recommended as the query protocol.

Some of the challenges have been identified and require a joint effort from the industry standards bodies, the carriers, and the vendors to ultimately reach an optimized solution that works best for the international carriers. These challenges include but are not limited to:

- Development of a world-wide standard for service provider ID;
- Definition of required service and capability information to support carriers' routing needs;
- Sourcing and integration of SPID, number portability, and service/capability information into a form suitable for use by carriers' IBO systems;
- A suitable architecture or architectures for carriers to exchange the above information.

It is suggested that the most effective path forward will be to leverage the registry building efforts that service providers will pursue for their own ends, since it is service providers, some of which are also international carriers, that possess the terminating SP identity and service capability information that international carriers require.

16 Annex 1 – Registry Architecture

- It has been recognized that a variety of IP routing and addressing architectures could exist in the industry.
    - Public
    - Private
    - Fully meshed
    - Centralized
    - Distributed

16.1 Public vs. Private Architectures

In this document, public registries are those sanctioned by some authority such as the ITU-T. Private registries are those operated by a commercial party or parties. (Note: A public registry implementation of a carrier ENUM, e.g., as in RFC 5526 [3], where the service provider controls registrations for a number is different from End User ENUM as contemplated in RFC 6116 [3] where the telephone number assignee controls registration.) It is presumed that initially private registries will be used to meet the needs outlined in this document.

16.2 Fully Meshed vs. Centralized vs. Distributed Architectures

A fully meshed architecture is one in which each carrier exchanges routing and addressing data directly with each other carrier on a bilateral basis. While such architectures are feasible for a small number of carriers, they are not effectively scalable. Therefore, where needed, it is expected that addressing & routing registries will be employed.

Such registries are managed by third parties. They may be either centralized or distributed. In the centralized case all data is contained in a single registry while in the distributed case, the data is distributed across multiple databases. For example, in an ENUM implementation, the routing data for all numbers could be held in one central registry or different portions (segmented by Country Code and/or by serving service provider) could be held in multiple databases with pointer from a top level registry indicating where to find data for a specific E.164 number. The GSMA PathFinder registry discussed below provides examples of both concepts.