**ATIS/SIP Forum IP-NNI Task Force**

 **IPNNI 2015 - 00030**

**July 2015**

**Contribution**

**TITLE: Testbed Landscape Team (TLT) Draft Baseline Document**

**SOURCE: Editor**

**ABSTRACT**

This document provides the draft baseline document from the Testbed Landscape Team (TLT).

The purpose for submitting this document to the IPNNI is:

1. To request a review from the IP NNI participants and provide any comments to the TLT, and
2. To determine if there is an indication of interest from any of the IP NNI companies to participate in any of the TLT Use Cases

Each of the Test Plans is included as Attachments. The attached Test Plans are shortened for conciseness.

The TLT would appreciate your feedback and indication of interest by Friday August 21, 2015



Testbeds Landscape Team

Assessment and Next Steps

July 2015



As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry’s most pressing business priorities. ATIS’ nearly 200 member companies are currently working to address the All-IP transition, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit [www.atis.org](file:///S%3A%5CPR%5CPressReleases%5C2014%5Cwww.atis.org).

This report of the ATIS Testbed Landscape Team was developed for the Technical and Operations (TOPS) Council, and is subject to change.

This report and its recommendations of this Landscape Team represents the consensus view of its members however the consensus views expressed herein do not create a requirement or obligation for any ATIS Member Company to purchase or implement any capability or method, either during or after the testbed activity.

Published by

**Alliance for Telecommunications Industry Solutions**

**1200 G Street, NW, Suite 500**

**Washington, DC 20005**

Copyright © 2015 by Alliance for Telecommunications Industry Solutions

All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at

< http://www.atis.org >.

Printed in the United States of America.

**Trademark Acknowledgments**

iconectiv™, LERG™ Routing Guide are trademarks and the Intellectual Property of Telcordia Technologies, Inc. dba iconectiv.

# Table of Contents

(to be added prior to publication)

# Table of Figures

(to be added prior to publication)

# Executive Summary

A number of industry organizations have recognized the important role that a testbed could play in understanding how key mechanisms may evolve to support the all-IP transition. The Testbed Landscape Team (TLT) was organized to evaluate the feasibility of combining multiple single-use testbeds to assist SP when preparing their testbed capabilities related to the migration to All-IP. The cost and complexity of establishing single-use testbeds has presented challenges, and identifying and recommending where SPs can combine testbeds that utilize common infrastructure may guide and hence enable some SPs to also build a multi-functional-testbed capability to assist in their network preparation for the migration to All-IP. To accomplish this, SPs and vendors interested in utilizing a multi-functional testbed approach identified test “use cases” based upon their testing needs and interest. These use cases have been categorized below into the following categories:

* Numbering: mechanisms to support Individual and 1000’s-block Number Assignment to identify areas warranting further study.
* Routing: mechanisms that could be used for routing SIP sessions using telephone numbers (TN) as identifiers.
* Provider-to-provider metadata: mechanisms for provisioning, securely exchanging and validating metadata associated with TNs for a variety of applications including, but not limited to, draft IETF mechanisms to prevent spoofing of caller-ID.

Building upon the candidate use cases, the TLT analyzed high level requirements and assessed interest from service providers and vendors to potentially provide personnel, equipment, systems, or prototypes to participate in testing. It is worth noting that although TLT participants have expressed interest, as of yet this effort has been landscape only; there has not been any discussion of detailed configurations or formal commitment to participate in testing.

This report provides an initial assessment and indication of interest by TLT member companies to participate in one or more of the testbed use cases identified in this report. The next step is to develop a formal recommendation for an action plan based on further analysis of potential use case synergies, formal expression of interest in participating in testing and to providing the required software, equipment and personnel for the actual testing. The recommendations would propose a timeline with a focus on the initial tests and identify responsibilities for key deliverables, both in terms of technical primes and project management.

#  Background

As a result of the FCC Technology Transitions Order, FCC 11-161[[1]](#footnote-1) an all-day workshop was hosted on March 25, 2014 by the FCC’s CTO to facilitate the design and development of a Numbering Testbed. The primary goal of the Numbering Testbed described in the workshop announcement[[2]](#footnote-2) was to “provide common resources to enable research into numbering in an all-IP network, unencumbered by the constraints of the legacy network and technologies and ensuring that there is no disruption to them.”

At the workshop the Commission’s CTO indicated his interest was ultimately in the development of a policy agnostic flexible platform that would integrate numbering lifecycle management functions such as resource allocation, porting, and dissemination of routing information for all types of numbers. Such a platform should also facilitate implementation of anti-spoofing solutions for verifying caller identity and thus addressing the growing problem of robocalls and phishing calls. The CTO further expressed interest in the possibility that the platform might be distributed, supporting a federated, competitive model similar to the white space databases.

The TOPS Council recognized that Individual testbeds focus on one specific aspect of the IP transition, but duplicate many functions that are common to all testbed(s). The ATIS TOPS Council established a Testbed Landscape Team (TLT) to evaluate the feasibility of providing options for SPs when building their All-IP migration testbeds. Single-use testbeds focus on one specific aspect of the migration to IP, but many of these testbeds are inefficient being that they duplicate common functions. As a result, the use of single-use testbeds by some SPs introduces unnecessary challenges as they prepare for the transition to All-IP.

The Testbed Landscape Team was tasked to:

* evaluate existing testbed activities and proposals.
* determine if there would be value in combining separate activities into a common testbed support capability.
* identify use cases that would benefit from a common testbed infrastructure.
* prepare a report to the TOPS Council recommending next steps .

# Scope of Effort

The Testbed Landscape Team issued an open invitation to industry stakeholders inviting suggestions for Testbed use cases. The scope was expanded beyond numbering to include many aspects of the migration to an All-IP environment. Vendors and Providers were invited to contribute “use cases” of interest within the following broad categories:

* Numbering use cases
* Routing use cases
* Provider to provider specific use cases which includes Anti-Spoofing use cases.

The scope of the Use Cases solicited by the Testbed Landscape Team covered a wide spectrum from “proof-of-concept” to “validating a specific capability” and their inclusion in this report or testbed(s) does not represent industry consensus to implement a new capability or method.

The scope of the testbed(s) were dependent upon the level of support for the use cases proposing the” use cases” since Vendor and/or Provider infrastructure are required to conduct the testbed(s). Use cases may showcase a particular product or service under development by a Vendor or Provider and its inclusion in a testbed(s) does not obligate any ATIS member company to purchase or implement any capability or service during or after the testbed(s) activity.

To remain transparent and eliminate any perception of vendor favoritism, there was no limitation to type or scope of use cases and inclusion in this report or testbed(s) is not an acknowledgement for a future purchase or need of a product or service.

Based on the agreement and acceptance of the Use Cases, High Level Test Plans were developed that included 4 Phases:

* Phase 1
	+ High Level System Description of Use Case
	+ Reference Architecture
	+ Core Components
	+ Companies that are interested
* Phase 2
	+ Development of High Level Test Plan
* Phase 3
	+ Intra/Inter – Carrier tests
* Phase 4
	+ Reports

This document includes the completion of the Phase 1 portion of the Test Plans. Phase 2 of the Test Plans will be documented and completed by the companies participating in the Use Cases. Phase 3 will be when the actual tests are conducted and Phase 4 will provide a Report based on the outcome of the trial.

# Applicability

This report is the result of a voluntary effort by ATIS member companies and reflects the consensus view of participants.  The use case recommendations and testbed(s) specifications are not intended as mandates; participation in this effort does not indicate any obligation or intention by specific members to purchase or implement any capability or method described in this report. Decisions regarding the implementation of, or compliance with, these specifications appropriately will made by individual companies. Finally, it should be noted that the recommendations and specifications are not intended for use in certifying equipment and/or services.

# High Level Landscape Use Case Assessment

## Numbering Use Case

### Numbering Use Case 1 –JIT/ITN Number Assignment for individual TN & block allocation

**Description:** Explore allocation of numbering resources on a just-in-time, per customer basis within the framework of a converged platform for numbering lifecycle management

**Registry:** The Registrywould enforce numbering resource policies and provide utilization reports for regulatory authorities. Key question is whether we will have a single API that everyone can test against, or independent implementations of the API for the registry. In any case, this test is likely to involve prototype equipment rather than production equipment.

* **Indication of Interest:** AT&T, Comcast, and iconectiv.

**Service Providers/Vendors** – Provisioning systems would be used to query the registry for availability of numbers and to provision information for a number once it had been assigned.

* **Indication of Interest**: AT&T, CenturyLink, Comcast, iconectiv, JSI, and Sprint.

## Routing Use Cases

### Routing Use Case 1 – NS Records

**Description:** Demonstrate the ability to enable end to end IP connectivity with the provisioning and distribution of NS Records

**Registry** - Provide industry database for the provisioning and distribution of NS records. Registry Provider would need to provide GUI for provisioning and standard interface for downloading NS records.

* **Indication of Interest**: iconectiv, Neustar

**Service Providers/Vendors** - It is anticipated that Service Providers would work with Vendors to provide IP call routing infrastructure including but not limited to switching, local routing DBs, route servers, ENUM Servers, Ingress and Egress SBCs. SP would also provide interface to local DB (Routing Server) for receiving NS Records via Testbed Registry.

* **Indication of Interest**: AT&T and CenturyLink.

### Routing Use Case 2 – URIs

**Description:** Demonstrate the ability to enable end to end IP connectivity with provisioning and distribution of URIs.

**Registry** - Provide industry database for the provisioning and distribution of URIs. Registry Provider would need to provide GUI for provisioning and standard interface for downloading URIs. If available the Registry provider could also provide an interface (SIP/ENUM) to enable call by call query to retrieve URI.

* **Indication of Interest**: iconectiv and Neustar.

**Service Providers/Vendors** - It is anticipated that Service Providers would work with Vendors to provide IP call routing infrastructure including but not limited to switching, local routing DBs, route servers, ENUM Servers, Ingress and Egress SBCs. SP would also provide interface to local DB (Routing Server) for receiving URI via Testbed Registry.

* **Indication of Interest** – AT&T and CenturyLink.

### Routing Use Case 3 – Distributed Service Bureau

**Description:** A Distributed Service Bureau is based on the premise that a per-TN registry of routing references is hosted in a distributed fashion among various entities in the PSTN. These can include:

* Telephony service providers/Carriers
* Transit providers
* Service Bureau providers on the behalf of the above

**Service Providers/Transit Providers/Service Bureau Providers**: Provide hosting and source code implementation of a distributed registry that can be hosted in a Service Provider or service bureau provider network.

* **Indication of Interest**: AT&T, CenturyLink, Comcast, iconectiv, and Inteliquent.

**Service Providers/Vendors** - It is anticipated that Service Providers would work with Vendors to provide IP call routing infrastructure including but not limited to switching, local routing DBs, route servers, ENUM Servers, Ingress and Egress SBCs. SP would also provide interface to local DB (Routing Server) for receiving URI via Testbed Registry.

* **Indication of Interest**: AT&T, CenturyLink, Comcast, and Inteliquent.

### Routing Use Case 4 – 800

**Description:**  Demonstrate potential evolution of toll free routing leveraging the capabilities of Internet Protocols.

**800 Data Base** - enables the existing Toll-Free Number Administration System (SMS/800 Registry) to allow the industry to continue to leverage existing connectivity and provisioning processes while enabling Toll-Free routing in an IP environment

* **Indication of Interest**: SMS/800.

**Service Providers/Vendors** - Would administer IP Endpoint and IP network call routing data via the GUI or API to the SMS/800 Registry It is anticipated that Service Providers would work with Vendors to provide IP call routing infrastructure including but not limited to switching, local routing DBs, route servers, Ingress and Egress SBCs and Toll Free Application Servers. SP would also provide interface to local DB (Routing Server) for receiving NS records via Registry database.

* **Indication of Interest**: AT&T, SMS/800.

### Routing Use Case 5 – LERG™ Routing Guide IP Enhancements

**Description**: This Use Case would demonstrate proof of concept as well as the ability to enable end to end IP connectivity using aggregate level URI solution. The URI would be associated with an OCN, LRN, NXX, etc.

**Registry** - Would provide LERG™ Routing Guide files for the provisioning and distribution of URI Records. The Registry would need to provide GUI for provisioning and files for downloading.

* **Indication of Interest**: iconectiv.

**Service Providers/Vendor** - It is anticipated that Service Providers would work with Vendors to provide IP call routing infrastructure including but not limited to switching, local routing DBs, route servers, ENUM Servers, Ingress and Egress SBCs. SP would allow acceptance of LERG™ Routing Guide files with IP routing data (URIs) to support IP routing at the block level.

* **Indication of Interest**: Inteliquent.

## Provider to Provider Use Cases

### P-toP Use Case 1 - Exchange of Data Using In-band Mechanisms

**Description:** Provide test setup and source code implementation that would support provisioning, exchange, and querying of a range of metadata, including an RFC4474bis based data verification service. Common framework should support signed data including:

* Caller-id.
* CNAM.
* Advanced CNAM and subscriber metadata.

**Distributed Service Bureaus :** Certificate provisioning and distribution via Distributed Service Bureau. Certificates are provisioned on a per-TN basis by the service provider of record, or by a third party authorized by the service provider of record, and hosted in a distributed fashion among various entities in the PSTN, for validation by terminating party.

* **Indication of Interest**: Comcast, iconectiv, and InCharge Systems.

**Service Providers/Vendors** - Service provider manages corresponding private key internally.

The assumption is that each provider has their own secure mechanism for validating their customer is who they say they are, consistent with 4474bis. It is anticipated that Service Providers would work with Vendors to provide IP call routing infrastructure including but not limited to switching, local routing DBs, route servers, ENUM Servers, Ingress and Egress SBCs.

* **Indication of Interest**: AT&T, CenturyLink, and Comcast.

### P-toP Use Case 2 - Data Verification – Anti-Spoofing

**Description:** Provide test setup and source code implementation of an RFC4474bis based data verification service. Although the steps in this use case can be used for anti-spoofing mechanisms, the tests also explicitly include validation of other data such as caller-id, CNAM, advanced CNAM, and other subscriber metadata.

**Distributed Service Bureaus:** Certificate provisioning and distribution via Distributed Service Bureau. Certificates are provisioned on a per-TN basis by the service provider of record and hosted in a distributed fashion among various entities in the PSTN, for validation by terminating party.

* **Indication of Interest**: Comcast, iconectiv, and InCharge Systems.

**Service Providers/Vendors** - Service provider manages corresponding private key internally.

The assumption is that each provider has their own secure mechanism for validating their customer is who they say they are, consistent with 4474bis. It is anticipated that Service Providers would work with Vendors to provide IP call routing infrastructure including but not limited to switching, local routing DBs, route servers, ENUM Servers, Ingress and Egress SBCs.

* **Indication of Interest**: AT&T, CenturyLink, and Comcast.

### P-toP Use Case 3 - Use of TN Certificates – Anti-Spoofing

**Description:** This use case would demonstrate the use of Telephone Number (TN) certificates to verify a SIP caller’s use of a telephone number identity following the steps mentioned in RFC 4474 (also noting draft-ietf-stir-rfc4474bis) and would demonstrate the functions of a Telephone Number Certificate Authority (TN-CA) during verification.

**TN CA**: Publish TN certificates, provide the certificates for the certificate chain, and support CRLs and OCSP for checking the status of the TN Cert.

* **Indication of Interest**: iconectiv and InCharge Systems.

**Verifie**r: Be able to fetch a certificate from the TN-CA, validate the certificate, and then use it to verify the INVITE for a SIP call using a TN identity.

* **Indication of Interest**: AT&T and CenturyLink.

### PtoP Use Case 4 - Alternative Approach for Acquiring TN Certificates – Anti Spoofing

**Description:** Demonstrate an alternative approach for acquiring Telephone Number (TN) certificates to verify a SIP caller’s use of a telephone number identity. In this use case, a Reference Plane would contain URIs for TN certs.

**TN CAs:** TN Reference Plane would be a database of URIs indexed by TNs, where the stored URI for a TN points to the TN cert for that number, and where the TN cert is held by a TN-CA. In the basic case, there could be multiple TN-CAs, but each TN has only one cert (hosted by one TN-CA).

* **Indication of Interest**: iconectiv and InCharge Systems.

**Verifier**: Able to fetch a certificate using the Reference Plane’s URI for a given TN, validate the certificate, and then use it to verify the INVITE for a SIP call using a TN identity. For this use case, the Reference Plane could contain URIs for TN certs when there are one or more TN-CAs.

* **Indication of Interest**: AT&T and CenturyLink.

# Mapping of the Use Cases to the Test Plans

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Use Case** | **Sub-Team** | **Description** | **Test Plan** | **Indication of Interest** |
| 5.1.1 | Numbering | ITN Number Assignment for individual TN & block allocation | Attachment A |  AT&T, Comcast, iconectiv, CenturyLink, JSI, and Sprint |
| 5.2.15.2.2 | Routing | Resource Records | Attachment B | AT&T, CenturyLinkNeustar, and iconectiv |
| 5.2.3 | Routing | Distributed Service Bureau | Attachment C | AT&T, CenturyLink, Comcast, iconectiv, and Inteliquent |
| 5.2.4 | Routing | 800 | Attachment D | Iconectiv, AT&T, SMS/800 |
| 5.2.5 | Routing | LERG™ Routing Guide - IP | Attachment E | Iconectiv, Inteliquent |
| 5.3.15.3.25.3.35.3.4 | P-to-P | Secure Telephone Identity | Attachment F | Comcast, iconectiv, InCharge Systems, AT&T, CenturyLink |

# Recommendations for Next Steps

This report summarizes the use cases and the level of interest in providing personnel and/or equipment to potentially participate in the testing. The next step will be to develop a recommendation for an ATIS action plan to analyze: 1) the use cases with consideration for potential synergies and interest in participating in testing; and 2) more detail on the availability of equipment and personnel for testing. As part of the next steps, ATIS should liaise with other SDOs to notify them of this testbed activity, provide information about the Use Cases, solicit feedback and interest in broader participation in the trials/testbed.

The recommendations would include:

* Prioritization of use cases to identify which use cases should be tested first. This will be based on level of interest and availability of equipment and systems to do the testing. The recommendations would include a proposed timeline for the testing, with a focus on the initial tests.
* Proposed strategy to develop the detailed test objectives, configurations and plans for each use case. The role of existing ATIS committees in developing test plans will be identified, as well as the potential need for new committees or forums, if required.
* Proposed timeline for testing and developing the supporting material (e.g., test plans) with a focus on the initial tests.
* Identified responsibilities for key deliverables, both in terms of technical primes and project management.

Test Plans:

Attachment A – Numbering (TLT-2015-00048)

Attachment B – Resource Records (TLT-2015-00038)

Attachment C – Distributed Service Bureau (TLT-2015-00047)

Attachment D – 800 (TLT-2015-00063)

Attachment E – LERG™ Routing Guide - IP (TLT-2015-00055 (Hostname) and 00064 (FQDN))

Attachment F – Secure Telephone Identity (TLT-2015-00046)

# Attachment A: TLT Testbed Numbering Allocation Sub-Team JIT/ITN Number Assignment for Individual TN & Block Allocation

## A.1 Phase 1 – Overview

### A.1.1 System Description

Number management from an authorized service provider requires a well-defined provisioning interface (API) to perform functions in relation to managing the ownership and information related to telephone numbers.

Based on the comprehensive set of requirements ATIS has defined (see Section 4.1) this proposal addresses the necessary interface components in the context of a service bureau (either distributed or not).

Basic interface flow include:

* Query for unallocated number(s) based on criteria (e.g., NPA NXX).
* Allocation/Assignment, individual and block level could be supported, including 1k number blocks.
* Update/Transfer/Port.

De-allocation/Return of number(s) to pool.

Security will be addressed with a timestamp/signing procedure to validate an authorized service provider performed a valid operation on the service bureau information as well as providing traceability in the case of any potential conflicts or errors.

Timing is addressed with a target of second or sub-second level transaction completion depending on the operation (for both distributed and not).



Figure A.1 - Architectural Overview

Service Provider interface to service bureau over HTTP/RESTful interface.

NTP Time Server is queried for timestamps to avoid allocation timing conflicts and race conditions.

Service Providers, when designated as Service Bureau administrators by the regulatory authority will be given a private key/public key pair which will be used for transactions with the Service Bureau for security and log validation purposes.

NOTE 1: This key pair is different from the 4474bis per TN key pair.

NOTE 2: A Distributed Service Bureau will have same architecture and API.



Figure A.2 - Service Bureau Provisioning API

The focus of this section is the interface between the Service Provider OSS/provisioning console and the Service Bureau.

This should be an HTTPS interface.

This will support all of the capabilities described in the requirements of the letter to the FCC.

## A.2 Reference Architecture

This portion of the document is intended to provide a reference architecture, core components and a high-level test plan to determine compatibility of the trial participant’s systems with the Registry systems prior to actual interconnection. It is also intended to support the trial participant’s decisions regarding systems to be used in Phase 2 and 3 of the trial, when actual systems are being interconnected.



Figure A.3 – Reference Architecture

## A.3 Reference Architecture – Provisioning API

Query

The Service Bureau will maintain a list of unallocated telephone numbers as part of its shared data store, these telephone numbers will have no information associated with them in the state of “unallocated”.

Support for single number (blocksize=1) or other contiguous block size requests (e.g. blocksize = 1k)

Have explicit support for common queries NPA, NPA NXX, LATA, Rate Center, State level queries.

OSS has option to aggregate queries independently for more customized level of query.

**HTTP GET – Query available numbers**

***Operation****:*

Get block of available numbers based on NPA, NPA-NXX, LATA, State or Rate Center.

GET /latas/:lata/blocksizes/:blocksize

GET /npas/:npa/blocksizes/:blocksize

GET /npanxxs/:npanxx/blocksizes/:blocksize

GET /states/:state/blocksize/:blocksize

GET /ratecenters/:ratecenter/blocksize/:blocksize

***Description****:*

Retrieve block of available numbers

***Request****:*

Pass type of telecom map (NPA, NPANXX,..) and count of available numbers in the URI

***Response****:*



***Example (using cURL)****:*

Request

$ curl -i -X GET http://sb1.example.com/*npanxxs*/215555/blocksize/1

Response

HTTP/1.1 200 OK

Content-Type: application/json

..............

[“+12155551000”, “+12155551003”, “+12155551212”, …]

**Allocation/Assignment**

Once the administrator has decided to allocate a given single or block level set of telephone numbers there is a PUT command that allocates the number, given the number wasn’t already allocated between the GET and the PUT.

This condition is handled in the service bureau implementation behind the scenes within the PUT. A two-phase commit, which also handles potential race conditions in the case of a distributed service bureau.

First phase, the state of the number is verified to be “unallocated”, second phase the allocation and update of entry information is committed. Even in the second phase, the success of the transaction shall be validated to make sure there aren’t any potential for error conditions or collisions of two service providers trying to simultaneously allocate the same number.

As a result of a successful allocation, the telephone number will be removed from the unallocated bucket.

As part of the allocation, the service provider will be required to provide following information:

* publicID: telephone number in e.164 format (e.g., +12155551212).
* serviceID: “pstn" by default, other services potentially in future.
* routingID: SIP URI with telephone number + domain representing service provider of record (e.g., sip:+12155551212@pstn.example.com).
* timestamp: a timestamp retrieved from a common NTP server representing time of allocation, used for validating which service provider allocated first in race condition scenarios, and just for logging and historical reference in general.
* public\_key: used for 4474bis validation.
* signature: using an service provider level public key/private key, the service provider shall sign the information above to prove that the approved service provider made the change to the registry.

**HTTP POST – Allocate numbers**

***Operation****:*

Service provider request to assign a number or block of numbers (public ID)

***Description****:*

Retrieve single or block of available numbers

***Request****:*



***Response***:



***Example (using cURL)****:*

Request

$ curl -i -H "Content-Type: application/json" -X POST -d ‘{”publicID”:”+12155551212”,”service”:”pstn”,”routingID”:”+12155551212@pstn.example.org”,”timestamp”:”1422980496943”,”public\_key”:”*PUBLIC\_KEY*”,”signature”:”*SIGNATURE*”}’ http://sb1.example.com

Response

HTTP/1.1 201 OK

**Update Entry/Port**

If a service provider needs to update information related to an allocated entry, such as, public key update, modify routingID, etc. or if there is a port where a new service provider will overwrite the entry with new information, the API is the same.

There is a GET operation to read the current entry information, if the OSS needs this information, (e.g., read/modify/write).

There also is a PUT operation that will write the updated entry information. This will require a new timestamp and signature to validate the security of the operation and logging/historical purposes.

**HTTP GET – Retrieve number entry**

***Operation****:*

Retrieve a entry for a given publicID/serviceID combination

GET /publicids/:publicid/services/:serviceid

***Description****:*

Retrieve the entry information for a given telephone number for a given service

***Request****:*

User publicID and serviceID as parameters in the URI

***Response****:*



***Example (using cURL)***

Request

$ curl -i -X GET http://sb1.example.com/publicids/+12155551212/services/pstn

Response

HTTP/1.1 200 OK

Content-Type: application/json

..............

{”publicID”:”+12155551212”,”service”:”pstn”,”routingID”:”+12155551212@pstn.example.org”,”timestamp”:”1422980496943”,”public\_key”:”*PUBLIC\_KEY*”,”signature”:”*SIGNATURE*”}

**HTTP PUT – Update Entry**

***Operation****:*

Change one or more attributes associated with publicID/serviceID combination

***Description****:*

Use this API to update an entry (e.g., for public key management or for porting)

***Request****:*



***Response****:*



***Example (using cURL)****:*

Request

$ curl -i -H "Content-Type: application/json" -X POST -d ‘{”routingID”:”+12155551212@pstn.example.org”,”timestamp”:”1422980496943”,”public\_key”:”*PUBLIC\_KEY*”,”signature”:”*SIGNATURE*”}’ http://sb1.example.com

Response

HTTP/1.1 201 OK

**Removal/de-allocation**

If a service provider wants to remove an entry for the case where a customer disconnects his service and no longer wants the number, a DELETE operation will be provided that will delete the entry, and for the case of a telephone number, will put the telephone number back in the pool of unallocated numbers.

**HTTP DELETE – Delete Entry**

**Operation**:

DELETE /publicids/:publicid/services/:serviceid/tel

Delete row associated with a public ID / service ID combination, where the public ID is a telephone number.

**Description:**

The following action needs to be taken

1. The associated row must be deleted from the registry (data store).
2. PublicID is added to the list of available numbers

**Request**

Pass the public ID and service ID as parameters in the URI.

**Response**

HTTP/1.1 **200** OK

Example (using cURL)

Request

$ curl -i -X DELETE http:// sb1.example.com/publicids/+12155551212/services/pstn/tel

Response

HTTP/1.1 **200** OK

## A.4 Reference Architecture – JIT Distributed Service Bureau Provisioning



Figure A.4 – Provisioning Reference Architecture

## A.5 Provisioning

1. Authority provides “authorized” service provider a private key/public key pair, makes public key available in a repository accessible by all other “authorized” service providers
2. Service Provider Customer requests account with associated telephone number
3. SP1 queries Service Bureau for available telephone numbers
4. SP1 selects, via customer interaction or automated algorithm, a telephone number to allocate and allocates number with SP1 specific information
5. Telephone number allocation is propagated to all other Service Bureaus
6. Telephone call is initiated and routed (skip detailed step for this, covered in Routing documents)
7. Customer closes account and telephone number is no longer needed
8. SP1 sends delete command to local Service Bureau for telephone number and telephone number is put back into the available pool of telephone numbers

## A.6 Reference Architecture – JIT Distributed Service Bureau Porting

****

Figure A. 5 – Porting Reference Architecture

## A.7 Porting

1. Authority provides “authorized” service provider a private key/public key pair, makes public key available in a repository accessible by all other “authorized” service providers
2. Service Provider 1 Customer requests port of associated telephone number from SP2
3. SP1 (optionally) validates telephone number is currently allocated
4. SP1 sends porting request to Distributed Service Bureau
5. Service Bureau propagates porting request to SP2
6. Telephone call is initiated and routed to SP1 instead of SP2 (skip detailed step for this, covered in Routing documents)

# Attachment B: TLT Testbed Routing Sub-team Trial Test Plan for Resource Records – NS & NAPTRS Utilizing a Registry

## B.1 Phase 1 – Overview

### B.1.1 System Description

This use case involves using a purpose-built Registry as the data exchange mechanism for an IP routing industry framework. A Registry can enable authorized Service Providers of Record (SPRs) to start directly exchanging routing information dynamically to enable session setup end-to-end over IP networks.

The Registry could vastly reduce the NS or NAPTR record set by supporting policy-based NS provisioning. For example, a resource record value could be assigned to each Operating Company Number (OCN) rather than to each telephone number or, to each unique Service Provider ID (SPID) and/or NPA/NXX or Location Routing Number (LRN). This could also differ by TN and be at the discretion of the number holder.

The Registry would optimize session setup time by providing resource records as a download to local cache at each originating service provider. In addition, the Registry can optimize the Service Providers internal queries by optionally provisioning and exchange NAPTR records instead of NS records. This could be optional according to terminating service provider discretion and would be transparent to the originating service provider.

Allow for different NS records depending on the originating & terminating service provider combination, and then the Registry could be configured with policy for source based resolution using a “Recipient Group” feature.

## B.2 Reference Architecture

This portion of the document is intended to provide a reference architecture, core components and a high-level test plan to determine compatibility of the trial participant’s systems with the Registry systems prior to actual interconnection. It is also intended to support the trial participant’s decisions regarding systems to be used in Phase 2 and 3 of the trial, when actual systems are being interconnected.

## B.3 Reference Architecture – Provisioning



Figure B.1 – Provisioning Reference Architecture

## B.4 Provisioning

* Steps 1 and 2 - Allows authorized Service Providers to create, change, and/or modify NS or NAPTRs in the Registry. The Registry will accommodate routing data for any participating SP’s telephone number, central office code (NPA-NXX) or thousand block (NXX-X) in the segments of the US numbering plan agreed upon for the trail. Routing data may take the form of either:
	+ A “Tier 2” NAPTR-type ENUM record containing the service-specific URI of the terminating SP’s IP interconnection entry point, or
	+ A “Tier 1” NS-type ENUM record identifying the domain name of the terminating SP’s Tier 2 name server.
* Step 3 - All NS Records/NAPTRs are sent to the local cache of all participating service providers.
* Step 4 - The local administration also provisions internal routing information into its own database. This includes providing both intra-network routing information (e.g., end-point URIs) and the resolution of domain names to an IP address.
* Step 5 - Service providers negotiate interconnection and exchange and provide IP-Address (A/AAAA) records for their IBCFs.
* Step 5A - These IP addresses correspond to the destination service provider’s IBCFs that constitute the application layer POIs. Each service provider provisions the records received from the other service provider in its internal DNS.

## B.5 Reference Architecture – NS Record Call Flow



Figure B.2 – NS Records Call Flow Reference Architecture

* Step 1 - A session is initiated.
* Step 2 - The Call Session Control Function (CSCF) initiates a query to the Routing DB for a routing lookup (potentially using ENUM) in its local database.
* Step 3 - The local database returns an NS record with the host name of a Delegated Tier 2 Name Server where specific VoIP routing information can be found.
* Step 4 - The originating Service Provider resolves the FQDN in the NS record to the IP address of the terminating service provider’s Tier 2 ENUM server.
* Step 5 - The Routing Server sends an ENUM query to the terminating network’s Tier 2 Name Server.
* Step 6 - The terminating network’s Tier 2 Name Servicer returns interconnect information in the form of one or more Naming Authority Pointer (NAPTR) records within the ENUM response. The response could also include other Resource Records such as A/AAAA or SRV records.
* Step 7 - The originating Service Provider resolves a NAPTR to a SIP URI and then the hostname in the SIP URI to obtain the IP address of an agreed upon terminating Service Provider’s ingress IBCF.
* Step 8 - A SIP INVITE is sent to egress IBCF of the Originators Network that has layer 3 connectivity to the ingress IBCF of Terminating Network.
* Step 9 - The SIP INVITE is forwarded to the ingress IBCF of the Terminating Network.
* Step 10 - Terminating Network terminates the call to its end user.

## B.6 Reference Architecture – NAPTR Call Routing



Figure B.3 – NAPTR Call Flow Reference Architecture

* Step 1 - A call is initiated.
* Step 2 - Originators CSCF queries internal route server.
* Step 3 - Route server responds with one or more NAPTR records containing the URI(s) for various services.  In this case, the voice-service (SIP) URIs are shown as examples passed back to CSCF.
* Step 4 - CSCF resolves the hostname in the SIP URI to obtain the IP address of an agreed upon Terminating Network’s ingress IBCF.
* Step 5 - A SIP INVITE is sent to egress IBCF of the Originators Network that has layer 3 connectivity to the ingress IBCF of Terminating Network.
* Step 6 - The SIP INVITE is forwarded to the ingress IBCF of the Terminating Network.
* Step 7 - Terminating Network terminates the call to its end user.

# Attachment C: TLT Testbed Routing Sub-Team Trial Test Plan for Distributed Service Bureau Using SIP URIs

## C.1 Phase 1 – Overview

### C.1.1 System Description

A Distributed Service Bureau is based on the premise that a per-TN registry of routing references is hosted in a distributed fashion among various entities in the PSTN. These can include:

* Telephony service providers/Carriers.
* Transit providers.
* Service Bureau providers on the behalf of the above.



Figure C.1 - Distributed Service Bureau High-Level Deployment Architecture

The Distributed Service Bureau Protocol would be a simple protocol based on well-known distributed database technique using a gossip protocol.

**The Gossip Protocol Implementation Overview**

* Peer to Peer communication model where a given node (registry) is not aware of the total number of nodes (registries) as long as every node (registry) is reachable by at least one path from every other node (registry). In other words, as in the previous example, there is no requirement for a full mesh connectivity for all nodes, and therefore can be easily manageable as a loosely connected set of nodes, (e.g., a tree or hub-and-spoke model).
* Each Service Bureau node maintains a list of other Service Bureau nodes it has arranged to have connectivity to and from which it receives and forwards gossip messages.
* This uses a mechanism called Scuttlebutt reconciliation which ensures a registry never transmits updates that is already known to the receiving registry.
* Real-time Update - When a Service Bureau provisions/update/add/delete its registry, the updates are propagated to all the registries in its list, which propagates the update to their respective nodes.
* Complete Update - Periodically, for data integrity, each Service Bureau propagates all information pertinent to the data it owns, this might happen hourly or nightly or weekly all depending on what is practical and reasonable.
* Each registry maintains a version number for each type of update (Real-time and Complete) and is propagated to the peer registries. Versioning is used to determine if an update is already known to the receiver.

## C.2 Reference Architecture

This portion of the document is intended to provide a reference architecture, core components and a high-level test plan to determine compatibility of the trial participant’s systems with the Distributed Service Bureau systems prior to actual interconnection. It is also intended to support the trial participant’s decisions regarding systems to be used in Phase 2 and 3 of the trial, when actual systems are being interconnected.

****

Figure C.2 - Call Routing Distributed Service Bureau Reference Architecture

## C.3 Provisioning

The proposal is that the protocol for provisioning would be HTTP based with a two basic read/write operations, additionally there will be other read/write/modify variations that can be extended easily as needs are identified.

### C.3.1 DSBP - POST/provisioning example

***Operation****:*

POST

***Description****:*

New entry provisioning a routing ID which maps to a public ID associated with a Service.

***Request****:*

|  |  |  |
| --- | --- | --- |
| **Property** | **Type** | **Description** |
| publicID | String | Publicly known identity string, e.g., e.164 telephone numbers |
| serviceID | String | Identifier for service type, e.g., PSTN or VoLTE or RCS |
| routingID | string | Service specific routing identifier e.g., SIP URI with domain of service provider of record |

***Response****:*

Returns the HTTP status of 201 if provisioning is successful

***Example (using cURL)****:*

Request

$ curl -i -H "Content-Type: application/json" -X POST -d ‘{”publicID”:”+15555551212”,”service”:"PSTN","routingID":"sip:+15555551212@pstn.example.com"}' http:// sb.example.com

*Response:*

HTTP/1.1 201 Created

### C.3.2 DSBP - GET/retrieval example

***Operation****:*

GET /publicids/:publicID/serviceids/:serviceID.

***Description****:*

Retrieve routing ID across entire registry.

***Request****:*

Returns the HTTP status of 201 if provisioning is successful.

***Response****:*

|  |  |  |
| --- | --- | --- |
| **Property** | **Type** | **Description** |
| routingID | String | Service Specific routing identity |

***Example (using cURL)****:*

Request

$ curl -i -X GET http://sb.example.com/publicids/+12155551212/services/pstn

Response

HTTP/1.1 200 OK

Content-Type: application/json

..............

{"routingID":"+15555551212@pstn.example.com"}

## C.4 Reference Architecture –Call Flow

****

Figure C.3 – Call Flow Reference Architecture

1. Local DNS is provisioned with internal SIP routing information to peering IBCFs corresponding to SP2 peering points.
2. Service Provider 2 allocates a telephone number (TN2) in local Service Bureau.
3. SP2 Service Bureau distributes telephone number information to all connected Service Bureaus including SP1 Service Bureau.
4. SIP UE in SP1 network initiates a call to TN2 from TN1, INVITE is sent to CSCF.
5. CSCF performs ENUM query for TN2.
6. SP1 Routing DB maps query to Service Bureau HTTP/DB query.
	1. If it exists in Service Bureau, the SIP URI response provides indication of whether telephone number is IP or IMS routable.
	2. If no entry exists, ENUM query should respond with NULL which will result in keeping the TEL URI as is.
7. CSCF inspects R-URI for SIP URI or TEL URI.
	1. For SIP URI, there is a default route to the SP Routing DB. SP Routing DB will inspect source and destination telephone numbers, including inspecting destination number domain to determine service provider of record. A local table lookup, or optionally a direct query to SP2 will be used to provider the actual routable SIP URI. The R-URI is replaced and a 302 redirect is sent back to CSCF.
	2. For TEL URI, there is a default route to BGCF where legacy routing can be initiated.
8. Based on localDNS configuration, CSCF routes INVITE toward IBCF egress point with cooresponding NNI interface to SP2 IBCF.
9. Call termination to CSCF and to SIP UE happens as normal.

# Attachment D: TLT Testbed Routing Sub-Team Trial Test Plan for: Toll-Free Routing in an All-IP Network: IP Overlay Transition Approach

## D.1 Phase 1 – Overview

### D.1.1 System Description

A solution that enables the existing Toll-Free Number Administration System (SMS/800 Registry) to allow the industry to continue to leverage existing connectivity and provisioning processes while enabling Toll-Free routing in an IP environment. This will enable the existing TDM, Hybrid and IP only networks to acquire, provision and route calls to Toll-Free numbering resources by overlaying the TDM capabilities of the existing system with IP functionality and connectivity.

The industry is in transition and networks today terminate calls on both TDM and IP networks. Currently TFN data is accessed by a variety of different entities for different purposes.  Responsible Organizations (Resp Orgs) utilize the system for Toll-Free number administration and the provisioning of TF numbering resources. They may or may not also acquire the routing data for call processing purposes in their network if they own a network using the SCP Owner/Operator data distribution method provided by SMS/800.  SCP O/Os do not have to be Resp Orgs and may simply interface with the TFN system for the purpose of acquiring the data for call processing purposes.

 The industry does exchange some IP termination and interconnection data, however it is limited in scope and has not been adopted throughout all registration and routing databases that provide legacy services. Currently, the SMS/800 Registry supports provisioning terminating endpoints of POTS, 8XX number, CIC and end intercepts. However, with enhancements to accept IP queries and IP termination information, service providers will be able to utilize the SMS/800 Registry for both IP and TDM routing data. As the number of IP carriers and hybrid networks, enabling carriers to provision and receive IP network routing information becomes more and necessary.

An efficient and effective methodology for addressing Toll-Free in an all-IP ecosystem is an overlay solution that: allows service providers to optimize on their existing PSTN infrastructure, CAPEX and OPEX expenditures; introduces the ability to provision and distribute IP data for use today; and prepares for a migration to an all IP environment.  Enhancing the SMS/800 registry would also maintain the ease of number administration and provisioning for the Toll-Free ecosystem (Responsible Organizations, Carriers, and consumers) with a consistent and known neutral third party administrator (SMS/800, Inc. was appointed by the FCC for this role) providing the ability to search, reserve, provision and distribute routing information for Toll-Free numbering resources.

## D.2 Reference Architecture

This portion of the document is intended to provide reference architecture, core components, and a high-level test plan to determine compatibility of the trial participant’s systems prior to actual interconnection. It is also intended to support the trial participant’s decisions regarding systems to be used in Phase 2 and 3 of the trial, when actual systems are being interconnected.

The type of IP data provisioned and formats would be determined by the participants in the testing. Service Providers would need to provide IP call routing infrastructure including but not limited to switching, local routing DBs, route servers, Ingress and Egress SBCs and Application Servers. SP would also provide interface necessary to receive IP TF Routing Data via SMS/800 registry.

## D.3 Reference Architecture – Expanded Provisioning & Distribution Capabilities



Figure D.1 – Provisioning Reference Architecture

## D.4 Provisioning

* Step 1 – Responsible Organization provisions IP End Point (URL, URI Hostname Etc.) into the SMS/800 Registry and associates IP End Points and IP network information with the Resp Org ID. Other Carrier Information can be associated here as well, CICs ACNA and the IP routing data, URI Host Name and other network information and routing relationships can also be established. A Resp Org can also add associated carriers to the IP network data as well as Carrier Agreements with Entities in order to facilitate peering arrangements. Currently the SMS/800 Registry supports these types of agreements and routing partnerships, and the addition of IP agreements and routing associations to that functionality will be enhanced for the testing.
* Step 2– Service providers will establish in their networks any provisioning or translations necessary to support the IP endpoint routing data and/or any peering relationships required for the testing. This could include the exchange of IP-Address (A/AAAA) records for their Interconnect Border Control Functions (IBCFs) as well as DNS records for Internal Domain Name Server Provisioning.
* Step 3 - Resp Org queries SMS/800 for 8XX number and reserves it. The Resp Org then provisions the URL, POTS, or Dial number and any other IP network data necessary.
* Step 4 – Resp Org Activates number and the SMS/800 sends the 8XX number and the associated routing data to the SCP’s (TDM Network elements) and to IP network elements to enable routing of the 8XX number.
* Step 5 – Detailed test plan activities occur and results are reported to the appropriate interested parties.

# Attachment E: TLT Testbed Routing Sub-Team Trial Test Plan for: Enhancing LERGTM Routing Guide to Accommodate URL Hostnames

## E.1 Phase 1 – Overview

### E.1.1 System Description

A solution that enhances the LERG™ Routing Guide would allow the industry to continue to leverage existing processes for data exchange of the URI Hostnames.

The existing industry framework supports the exchange of Time Division Multiplexing (TDM) and a limited set of IP routing and interconnection data. Currently, the LERG™ Routing Guide supports an indicator noting if an NXX (non-ported telephone numbers (TNs) only) or a Location Routing Number (LRN) is IP enabled. However, with an enhancement to include the URI Hostname, service providers can provide an IP point of interconnection, analogous to TDM, as well as exchange this information on a mechanized basis. As the number of IP interconnection points grows, exchanging data becomes administratively more cumbersome if not done through a centralized process that is common to all parties.

A solution to utilize LERG™ Routing Guide to provision Hostname information would allow service providers to continue to manage effectively process evolution as it pertains to IP routing and interconnection. Enhancing the LERG™ Routing Guide would also maintain consistency of data exchange across the multi-service provider ecosystem, as opposed to a third party’s tiered solution where it would be difficult to maintain a consistent quality of service benchmark across service providers.

## E.2 Reference Architecture

This portion of the document is intended to provide reference architecture, core components, and a high-level test plan to determine compatibility of the trial participant’s systems prior to actual interconnection. It is also intended to support the trial participant’s decisions regarding systems to be used in Phase 2 and 3 of the trial, when actual systems are being interconnected.

## E.3 Reference Architecture – Provisioning



Figure E.1 – Provisioning Reference Architecture

## E.4 Provisioning

* Step 1 - Service provider updates BIRRDS with switch/POI information [e.g., actual switch, points of interface, trunk gateways, call agents, Signaling Transfer Points (STPs), etc.], tandem homing arrangements, Location Routing Numbers (LRNs), and detailed information supporting NPA/NXX and NPA/NXX-X assignments. This data is integrated with other BIRRDS data elements (e.g., Rate Centers) maintained by the BIRRDS administrator. URI Hostnames could be associated with OCN, at the highest order, or can be associated with other LERG™ Routing Guide data, e.g., NPA-NXX level. The URI Hostname association would need to be agreed upon by service providers. To reduce data entry error, it may be reasonable for service providers to create a URI Hostname “record” in BIRRDS that can then be crosschecked when using the Hostname on other BIRRDS records and to house any pertinent high level information relative to that Hostname. As an option, it may be advisable to add a field to indicate Hostname Class, e.g., Name Server = N, Session Initiation Protocol (SIP) URI = V.
* Step 2 - The LERG™ Routing Guide is generated from current BIRRDS data and is provided to service providers monthly for theirpre-provisioning systems. As an option, augmented daily-activity is provided nightly**.**
* Step 3 - Based on service providers’ local methods and procedures, the LERG™ Routing Guide data is loaded into service providers’ pre-provisioning systems and is used for switch translations, trunk engineering, numbering administration, legal and regulatory support, forecasting, intercompany billing support, and numerous other functions within the company.
* Step 4 - Based on service providers’ local methods and procedures, the LERG™ Routing Guide data in service providers’ pre-provisioning systems is made accessible to switch translations engineers to configure translations and routing tables.
* Step 5 - Service providers negotiate an interconnection agreement and exchange IP-Address (A/AAAA) records for their Interconnect Border Control Functions (IBCFs).
* Step 5A - These IP addresses correspond to the destination service provider’s IBCFs that constitute the application layer Points of Interfaces (POIs). Each service provider provisions the records received from the other service provider in its internal Domain Name Server (DNS).

## E. 5 Reference Architecture – URI Hostname Call Flow



Figure E.2 – Call Flow Reference Architecture

**Session 1 – IP Session via Public Switched Telephone Network (PSTN) Interconnection**

* Step 1 - A session is originated and sent to the Call Session Control Function (CSCF).
* Steps 2 &3 - The CSCF performs an internal query to its routing server to retrieve routing data for the called number.
* Step 4 - If the CSCF determines that the called number requires interconnection via the PSTN to Terminating Service Provider 1, and then the session is routed to the appropriate trunk gateway where it is converted to TDM.
* Step 5 - The session is routed internally to the trunk gateway and point of interconnection for Terminating Service Provider 1. The call is converted back to IP within the terminating service provider’s network.
* Steps 6 & 7 - Terminating Service Provider 1 then signals the terminating CSCF to complete the call. Terminating Service Provider 1 may be an IP network but the means of interconnection is still via the PSTN. It is probable, per the illustration, that the terminating service provider offers both media gateways and IBCFs to accept sessions during the IP transition phase.

**Session 2 – IP Session via IP-IP Interconnection**

* Step 1 - A session is originated and sent to the Call Session Control Function (CSCF).
* Step 2 - The CSCF performs an internal query to its routing server to retrieve routing data for the called number.
* Step 3 - The routing server returns a URI and the CSCF determines that the called number can accommodate an IP-NNI to the Terminating Service Provider.
* Step 3a - The CSCF will then query its local DNS to resolve the URI to the IP address of the IBCF of the terminating network.
* Step 8 - A SIP invite is sent to the egress IBCF of the originating network that has connectivity to the ingress IBCF of the terminating service provider.
* Step 9 - A SIP Invite is forwarded to the terminating service provider’s ingress IBCF. Route selection is based on IP peering agreement between service providers as well as service attributes, least cost routing, etc.
* Steps 6 & 7 – (Same as Steps 6 and 7 above) Terminating Service Provider 2 signals to the appropriate CSCF and the end-to-end session is established.

# Addendum to Annex E: TLT Testbed Proposed Variation to the Draft Test plan for IP Enhanced LERGTM Routing Guide

## E.6 Introduction

The “IP Enhanced LERG” test plan envisions adding a “URI hostname” field to various LERG data records (NPANXX, LRN, OCN, Switch, etc.) as a means of enabling IP-based network-to-network connectivity. The method of using this information in the current test plan write-up involves carriers exchanging hostname-to-IP-address mappings (such as by means of A/AAAA DNS records), and using these to directly translate a given hostname into IP addresses representing particular ingress SBCs at the NNI border of the terminating network. An alternative way to use a hostname, or more generally a fully-qualified domain name (FQDN) provisioned with LERG records is as an aggregation that points to a list of pre-established routes between the originating and terminating carriers that all traffic resolving to the same FQDN will use. The “route list” will identify the egress SBCs, the terminating ingress SBCs that each egress SBC has connectivity to, and other parameters to drive the call-attempt procedure such as specific SIP agents within the egress and ingress SBCs, route preference, or load distribution across routes. The industry-shared FQDN may or may not be used to further identify ingress SBCs in the terminating network, which may instead be resolved through pre-exchanged IP addresses or more granular FQDNs that are applicable to specific routes from specific originating carriers.

## E.7 Proposed Variations to the “Phase 1” System Description & Reference Architecture

Based on the use of LERG-provisioned FQDNs as aggregations for use in origination-network routing, the following describes a variation to the proposed system description and reference architecture of the LERG enhancements contribution reflecting the use of a FQDN to select route lists, as opposed to directly choosing terminating network SBCs by IP address:

Under “Reference Architecture – Provisioning:”

Step 1-3 are essentially unchanged, except that the hostname/FQDN is identified as a routing aggregation as opposed to a pointer to a DNS object.

Step 5: (Note that step 5, establishing interconnection and routes is a pre-requisite for entering switch translations as in “Step 4”, so here it is listed first).

 As part of agreeing to interconnection, service providers establish routes of one or more egress SBCs to one or more ingress SBCs.

In the exchanged information, egress SBCs are identified at a minimum by one or more IP addresses or IP prefixes for IP routing and access control purposes.

Ingress SBCs are identified by one or more fixed IP addresses, an aggregate FQDN (same as provisioned to a LERG object) or one or more “connection FQDNs” that may be of local significance to particular routes. The terminating service provider also specifies the method to resolve the FQDN to a set of ingress SBCs applicable to the route (such as NAPTR/SRV/A-AAAA records in a private DNS server). The terminating service provider also provides IP prefixes to be used for IP routing and access control purposes at the interconnection points. Provided individual IP addresses or addresses the connection FQDN will resolve to must fall within the specified prefix ranges.

Service providers agree to one or more “route lists,” each containing one or more ordered and/or proportioned routes to be associated with one or more aggregate FQDNs. The terminating service provider further specifies the FQDN-to-route-list mapping.

Step 4: In switch routing tables, the originating service provider maps route lists to corresponding FQDNs, and maps LERG route selection destination objects (largely NPANXX and/or LRN) to the corresponding provisioned FQDN. Where a FQDN is not specified at a level that can be mapped to a routing destination object, or where a route list has not been agreed to for a provisioned FQDN, existing route list selections will be maintained.

Under “Reference Architecture – URI Hostname (FQDN) call flow – Session 1”:

Note that as an abstraction, a route list associated with an FQDN could contain PSTN/TDM routes mixed with IP-NNI-based routes. For this variation, we will first consider LERG destination objects with no provisioned FQDN or with a provisioned FQDN but no associated route list shared between terminating and originating carrier.

Step 1-3: No change in procedure

Step 4: The CSCF/softswitch first looks for a FQDN associated with the destination object (NPANXX or LRN) but does not find one. It then falls back to normal routing methods (such as route lists directly associated with individual NPANXXs or LRNs). In this case, we assume the route list does not contain IP-based routes.

Step 5-7: No change in the procedure, but note that there is no requirement that the terminating network has an IP/IMS core with TDM-based interconnection (for TDM termination the connecting network is more likely a circuit-switched core).

Under “Reference Architecture – URI Hostname (FQDN) call flow – Session 2”:

Steps 1-2: No change in procedure

Step 3: The routing server contacts an LNP resolution service to resolve the destination to a routing NPANXX/LRN (note that all geographic routing is assumed to be done on an LNP-corrected basis). The routing server in this case finds an FQDN associated with the routing destination information and further translates the FQDN to a route list.

Step 3a: The CSCF/softswitch resolves each entry in the route list to an egress SBC/IBCF and one or more associated ingress terminating SBC/IBCF by either IP address or connection FQDN which may or not be the same as the routing aggregation FQDN as provisioned in the LERG entry. Where the route entry contains one or more connection FQDNs, these may or may not be resolved to a terminating network SBC IP address at the CSCF/softswitch, as this is not necessarily needed to send the call to the next hop (an egress SBC). There may be advantages to resolving this name at the edge of the network based on DNS records maintained and updated by the terminating service provider.

Step 8: The CSCF/softswitch INVITEs to an egress SBC/IBCF based on the route distribution discipline specified in the route list (sequential, round-robin, proportion, etc.). The egress SBC/IBCF resolves any terminating network ingress FQDN(s) provided in the forwarded route information to an IP address or addresses if necessary.

Step 9: The egress SBC/IBCF attempts the call to one or more of the IP addresses forwarded directly from the CSCF/softswitch or resolved from one or more FQDNs. If successful, the call continues (Steps 6 and 7 in the original call scenario) and is completed to the terminating endpoint.

Step 9a: If the call is not successful to one or more terminating SBCs from the first chosen egress SBC, the call is released to the CSCF/softswitch. Depending on the type of release, the call may be reattempted to a different egress SBC/terminating ingress SBC combination in the route list. Steps 8 and 9 are repeated with potentially different terminating SBCs until the call is completed, runs out of routes, or is otherwise released with final treatment.

Steps 6,7: Essentially no change from the original scenario.

# Attachment F: Phase 1 TLT Test Plan for Provider to Provider Use Cases Related to Secure Telephone Identity

## F.1 Introduction

This document contains a draft Phase 1 test plan for Provider to Provider use cases related to Secure Telephone Identity. It focuses on the approach begun in RFC 4474 and under development in Internet Draft “draft-ietf-stir-rfc4474bis” (currently at version -03). The scope of the testing is to exercise the protocols involved in signing and validating the SIP INVITE when an E.164 telephone number is used as the calling number. The main objective is to demonstrate that the Identity header and the Identity-Info header are created correctly and processed correctly. The intent is to provide assurance that the calling number is a secure telephone identity. An additional objective is to demonstrate an application of data exchange between service providers by testing using signed data for CNAM.

## F.2 Test Plan Scope

First, this document suggests the use of STI (for Secure Telephone Identity) to refer to the functions being tested. It comes from STIR (for Secure Telephone Identity Revisited), the name of the IETF working group that is developing the successor to RFC 4474.

Second, this document suggests that testing focus on the use of E.164 telephone numbers as SIP identities, and on securing these identities using cryptographic assurances. The approach discussed in RFC 4474 and in Internet Draft “draft-ietf-stir-rfc4474bis” describes how, when an E.164 telephone number is asserted as the calling number, the SIP INVITE messages used to set up calls will be signed and validated.

Third, this document suggests that testing focus on the protocols and related functions involved in signing and validating. In particular, testing would demonstrate that the required headers are created correctly and processed correctly. These headers are the Identity header and the Identity-Info header. The optional Identity-Reliance header is out of scope for this testing.

Fourth, this document suggests that provisioning and other functions not directly related to protocol testing are out of scope for this testing. It is expected that informal procedures will be used as needed for configuring the components involved in testing. For example, both the Authentication Service and the Verification Service, as described in draft-ietf-stir-rfc4474bis, may involve policy based decisions as well as interactions with other components. It is suggested that the scope of testing be limited to providing suitable support for the functions involved in protocol testing and demonstrating basic functionality. However, it is an important objective that non-protocol issues related to implementing anti-spoofing be collected as part of the testing activity.

Fifth, this document describes call flows involving originating and terminating SPs but not involving transit SPs. It also suggests that signing and validation be controlled by the Call Session Control Function (CSCF) rather than by SIP User Entities or other components. These taken together are intended to limit the number of test points for the protocol testing described here. Since, for example, any entity along a call flow could validate a signed INVITE, there could be a number of possible architectural alternatives for such test cases. Therefore, the approach described here is suggested as more appropriate for an initial architecture for performing basic protocol testing.

Sixth, this document suggests that basic protocol testing can be performed in two different environments, the public Internet environment and a constrained deployment environment based on the Distributed Service Bureau architecture. In the public Internet environment, TN certificates that contain public keys are held in one or more TN Certificate Authorities (CAs). In the Distributed Service Bureau architecture, TN certificates are held by the Registry.

Seventh, this document suggests a basic and straightforward approach towards credentials. The essential use of credentials is signing using the private key associated with a TN and validating using the public key contained in the certificate associated with that TN. Accordingly, it is suggested that there be one private key and one certificate for each TN. It is suggested that private keys be held securely and locally, that certificates be published by a TN-CA or contained in a Registry configured to support this testing, and that the certificate for a TN should be retrievable within the appropriate environment via the URI in the Identity-Info header.

Finally, in order to demonstrate an application of data exchange between service providers, this document suggests an approach for testing that involves signed CNAM data. The SIP invite may contain a CNAM-related header. (Details are currently being discussed in the IETF STIR and DISPATCH working groups: the “display-name” parameter is currently being suggested for use; vCard consideration is out of scope for this document.) This CNAM-related header would be in addition to TO, FROM, PAID, and other headers that are signed/hashed.

## F.3 Use Case Scope

The Assessment and Next Steps document (ATIS-I-0000047) contains four Provider to Provider use cases. All four involve Anti-Spoofing use cases based on the current version of draft-ietf-stir-rfc4474bis. Therefore, it is necessary to consider a framework for this testing that is based on the basic protocol functions discussed in draft-ietf-stir-rfc4474bis. In addition, it is necessary to consider how such a framework supports testing of signed CNAM data.

Accordingly, this test plan proposes a set of test cases based on this common framework for demonstrating anti-spoofing. In brief, the proposed test cases fall into three categories and include:

* Call-related testing.
	+ Successfully validating properly signed calls.
	+ Testing unsigned calls (428 'Use Identity Header' Response Code).
	+ Testing an unusable URI (436 'Bad Identity-Info' Response Code).
	+ Testing improperly signed calls (438 'Invalid Identity Header' Response Code).
* Certificate-related testing.
	+ Successfully validating valid certificates.
	+ Testing certificate validation failures (437 'Unsupported Certificate' Response Code).
	+ Retrieving certificates from a TN-CA or Registry.
	+ Acquiring certificates via optional Reference Plane queries.
* CNAM-related testing.
	+ Successfully validating CNAM-related headers.
	+ Successful end-to-end insertion and retrieval of CNAM data.

It is also an objective of this testing that observations be collected about issues that could bear on the implementation of STI anti-spoofing. For example, handling the result of a validation could involve a number of policy and business issues. How, if at all, should a calling party, or a called party, be informed of a validation failure? These aspects will be important to collect.

## F.4 Phase 1 – Overview

This section gives the Phase 1 Overview for Provider to Provider use cases related to Secure Telephone Identities (STI). It consists of a System Description, Reference Architecture and Call Flow figures, and Core Requirements.

## F.5 System Description

The P-to-P use cases for STI involve the use of asymmetric key pairs to sign and validate SIP Invites in the particular case when E.164 telephone numbers are used as SIP identities for originating calls. The proposed testing focuses on the protocol aspects that are performed by an Authentication Service and a Verification Service. The systems to be used for this testing are based on the Testbed Common Reference Architecture, and to which those two services and some additional components related to certificates and private keys are added.

A number of assumptions are embodied in this Phase 1 Test Plan:

* E.164 telephone numbers (TNs) are used as SIP identities,
* Each TN has a unique private key and a unique public key,
* Private keys are held securely and locally by the originating Service Provider (SP),
* Public keys are contained in certificates held by a TN Certificate Authority (TN-CA) or by a Distributed Service Bureau Registry,
* Certificates are retrieved via URIs (or cached by the relying service provider) within the environment under test,
* Signing is performed by the originating SP,
* Validation is performed by the terminating SP,
* Testing is focused on protocol aspects,
* Testing of provisioning and non-protocol aspects is out of scope,
* Testing of signed CNAM data is experimental, and
* Collecting observations about implementing STI anti-spoofing is an important objective.

## F.6 Reference Architecture

This section describes the reference architecture for STI testing. This architecture begins with the Testbed Common Reference Architecture and overlays additional components to support functions required for STI testing. This is a functional approach to a high-level description.

New or modified components include:

* STI (4474) Secure Key Store,
* STI (4474) Authentication Service,
* STI (4474) Verification Service,
* STI (4474) Telephone Number Certificate Authority (TN-CA) for the public Internet environment,
* Distributed Service Bureau Registry - modified to support Certificate Repository functions - for the Distributed Service Bureau environment,
* STI (4474) Reference Plane (optional), and
* CSCF (Call Session Control Function) - modified to interoperate with these new/modified components.

For testing involving signed CNAM data:

* The Authentication Service may provide CNAM data for a TN based on locally held subscriber data. (Whether CNAM data is contained in the Registry is out of scope.)



Figure F.1 - Reference Architecture for Secure Telephone Identity Testing

## F.6 Call Flow Architecture for Anti-Spoofing Testing

This section describes the use of the STI Reference Architecture for anti-spoofing testing. The following figure shows a functional description of the call flow for a signed and validated call, with optional use of a TN-CA Reference Plane, for a SIP call from an originating SP to a terminating SP.



Figure F.2 - Architecture and Call Flow for STI Anti-Spoofing Testing

The steps in the call flow in the above figure describe the signing and validating of a SIP INVITE for anti-spoofing testing. The steps below are those involved in the successful validation of a signed call with the optional use of the Reference Plane.

1. The originating SIP UE creates a SIP INVITE with the E.164 calling number.
2. The originating CSCF determines that the SIP INVITE is to be signed.
3. The originating SP’s Authentication Service (AS) retrieves the private key for the calling number.
* For CNAM testing, the AS may provide CNAM data based on locally held subscriber data for the calling number.
1. The Secure Key Store provides the calling number’s private key.
2. The AS signs the INVITE by forming the identity signature, inserting the Identity Header, and inserting the Identity-Info Header.
* For CNAM testing, the AS includes the CNAM-related header as part of the identity signature.
1. The originating CSCF continues to set up the SIP call.
2. The terminating CSCF continues to set up the SIP call.
3. The terminating CSCF determines that the call is to be validated.
4. The terminating SP’s Verification Service (VS) determines the calling number. The VS determines whether the calling number’s certificate is cached. If not, the VS determines if the TN-CA Reference Plane is to be used to obtain the URI for the certificate (optional).
5. The TN-CA Reference Plane provides the URI for the calling number’s certificate (optional).
6. If the certificate was not cached, the VS determines the URI to use for the calling number’s certificate, either from the INVITE or optionally from the TN-CA Reference Plane.
11′. For the public Internet environment, the certificate is stored in the TN-CA.
11″. For the Distributed Service Bureau environment, the certificate is stored in the Registry.
7. The certificate for the calling number is provided (if a cached copy is not used).
12′. For the public Internet environment, the certificate is retrieved from the TN-CA.
12″. For the Distributed Service Bureau environment, the certificate is retrieved from the Registry.
8. The VS validates the certificate, extracts the public key, and validates the signed SIP INVITE.
* For CNAM testing, assuming STI validation is successful, the VS validates the CNAM-related header information. The VS determines if there is CNAM data present.
1. Depending on how the result of the STI validation is to be handled, the terminating CSCF continues to set up the call with the terminating SIP UE or it determines that the call is to be terminated with the appropriate RFC 4474-defined response code.
2. Depending on how the result of the STI validation is to be handled, the terminating CSCF continues in effect to set up or tear down the call by signalling to the originating CSCF.
3. The originating CSCF and terminating CSCF continue to set up the call by signalling to the originating SIP UE until the call is answered with 200-OK.

Testing to demonstrate error cases that generate appropriate response codes can be performed based on straightforward modifications to the above steps.

For CNAM testing, the use of CNAM data is not formally specified.

## F.7 Call Flow Architecture for Anti-Spoofing Testing

The sequence of events in the call flow for anti-spoofing testing is shown in the following two diagrams. The first sequence is for signing and validation when the optional use of the Reference Plane is not involved. The second sequence shows the use of the Reference Plane.



Figure F.3 - Authentication and Verification flow without TN-Reference-Plane



Figure F.4 - Authentication and Verification flow with TN-Reference Plan

1. [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)