# Testbeds Focus Group – Test Plans and Observed Results

Alliance for Telecommunications Industry Solutions
July 2018

ATIS-I-0000067

## Foreword

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 business priorities. ATIS' 150 member companies are currently working to address 5G, cybersecurity, robocall mitigation, IoT, artificial intelligence-enabled networks, the all-IP transition, network functions virtualization, smart cities, emergency services, 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). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

## Notice of Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

## Copyright Information

ATIS-I-0000067



Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

# Contents

# 1. Introduction

ATIS Technology and Operations Council (TOPS) Testbeds Focus Group was originally formed as a Landscape Team in 2015. At that time, a preliminary assessment was undertaken to evaluate existing testbed activities, as well as to identify common requirements that would be relevant to a range of test scenarios. The group completed its Phase 1 objectives with the 2015 publication of a report entitled, "Testbeds Assessment and Next Steps." By launching Phase 2 as a Focus Group in 2016, efforts turned to: assessing the functional use of components of existing test plans such as those from the MultiService Forum; developing detailed test plans; identifying dependencies for each test case; assessing any additional requirements for components or protocols; and evaluating the feasibility of conducting tests in phases.

# 2. Test Plans

The Testbeds Focus Group advanced test plans that validate a variety of end-to-end calling scenarios, including calls between multiple service providers (SPs). These efforts were informed by complementary ATIS' initiatives addressing mitigation techniques for illegitimate uses of caller ID spoofing and robocalling. The initial focus of testing was on the validation of the STIR protocol and the SHAKEN framework to sign and verify calling numbers to combat illegitimate caller ID spoofing. In addition, the group developed detailed test plans covering three other priority areas: Distributed Service Bureau Number Assignment; Just-in-Time Number Assignment using Existing Systems; and Routing.

To facilitate wider testing of the STIR/SHAKEN protocol, ATIS provided a Robocalling Testbed, hosted by Neustar, currently at no cost to the industry. The Robocalling Testbed supports complete, end-to-end call scenarios, including Authentication Service (STI-AS), Verification Service (STI-VS), and Certification Authority (STI-CA) SHAKEN functions, allowing companies the flexibility to test specific SHAKEN components or combinations of equipment. To date, 31 SPs and vendors have signed up to use the Robocalling Testbed.

This report is intended to provide a detailed picture of the testing structure and subsequent findings for the following key test scenarios identified by the Testbeds Focus Group:

- Just-in-Time Number (JIT) Administration
- IP Routing
    - Toll-Free IP routing
    - IP routing using LERG data
- Secure Telephone Identity (STIR/SHAKEN)

The test plans included in this document are current as of the date of publication. Maintenance of the STIR/SHAKEN test plan has been transferred to the ATIS/SIP Forum IP-NNI Task Force and may continue to be updated in the future.

## Just-in-Time Number Administration

This test's objective was to demonstrate allocation of numbering resources on a real-time, per customer basis within the framework of an established and trusted infrastructure for administering numbering resources. This is referred to as JIT number administration.

The test plan was based on number allocation to SPs using existing access methods while allowing numbers to be allocated as needed, rather than the current method of block allocations in advance. Testing was structured in phases, with incremental functionality added in each phase. The phased approach started by defining requirements, then developed a prototype testbed system for lab testing, and finally allowed for potential network testing if there was sufficient interest and approval.

Testing was completed in the lab, using the prototype system developed for this purpose, but did not include live network testing. The testing was successful, and provided a proof of concept for JIT number administration as an extension to existing number provisioning systems.

## Toll-Free IP Routing

Existing toll-free routing involves a Transaction Capabilities Application (User) Part (TCAP) query to a toll-free database that returns the routing information for the intended destination. To test toll-free routing in a SIP environment, the originating network sends a SIP invite to a Toll-Free Application Server (TFAS) that returns a "SIP 302 Moved Temp Response" indicating the new SIP-URI that is to be used to route the call. The net result is

the same, but this test uses forward-looking (SIP) interfaces rather than legacy network interfaces.

The test plan included two use cases. The first was a simplified routing case based only on the dialed number. The second use case allowed differentiated routing based on additional decision criteria, such as the originating area or Calling Party Number (CgPN), time of day, and day of week, as supported by the current SMS/800 system and SCPs.

The IP TFAS was successfully demonstrated using both scenarios detailed in the test plan. This test case validated that an IP TFAS (using SIP protocol mechanisms) can support routing of toll-free numbers and provides all functionality offered by the current toll-free routing mechanisms.

## Enhanced LERG™ Routing Guide - URI Hostnames or FQDNs

This use case tested a possible mechanism for distributing IP-based routing data as an overlay to existing NPANXX/LRN and switch-based routing data. Two IP-based routing data mechanisms were proposed, of which one of them—the use of a "routing FQDN" (fully-qualified domain name)—was tested.

In this scenario, an SP associates routing FQDNs with NPANXX and/or LRN entries as a flexible aggregation of destination codes. The routing FQDN field is published in the appropriate tables of the LERG Routing Guide (emulated for the purposes of the test). The SP then indicates on a bi-lateral basis with each interconnecting SP which pre-established set of routing paths (a "route list") the provider should use to reach any code associated with a given FQDN.

Each originating SP provisions an FQDN-to-route-list entry in its routing servers and resolves the portability-corrected NPANXX/LRN to an FQDN during call processing. NPANXX/LRNs that do not resolve to an FQDN may continue to route using the legacy routing tables in order to support transitions to IP-based routing methods or segregation of IP-reachable destinations from TDM-only destinations.

This use case confirms that IP routing information can be included in the Business Integrated Routing and Rating Database System (BIRRDS)[1] provisioning system, and then

[1] BIRRDS is managed by Telcordia Technologies, Inc., dba iconectiv.

used to provide the IP enhanced LERG information between service providers. It demonstrates the feasibility of flow-through of data from a publishing terminating SP to an originating SP's route server. Finally, it shows the use of the resulting FQDN-based routing database entries to direct calls to one or more routes across an IP-NNI interface, in a routing plan integrated with switch-based routing.

The successful completion of this testing demonstrated a method to adapt existing routing infrastructure and data exchange to support IP-based routing.

## Secure Telephone Identity (STI)

This use case exercises the Secure Telephone Identity (STI) and the Signature-based Handling of Asserted information using toKENs (SHAKEN) industry framework to allow SPs to authenticate caller ID at the call origin and verify this information at the call termination. The test scenarios verify correct implementation of SHAKEN (minimally authentication and verification), as well as the specified response to error conditions (e.g., correct error code when verification fails).

ATIS provided a Robocalling (SHAKEN) Testbed, hosted by Neustar, to support the SHAKEN implementation. The SHAKEN testbed provides an end-to-end implementation of all components involved in a SHAKEN call. This allows participants to bring individual components and remotely test their implementations against the testbed.

A total of nine companies have tested implementations of various SHAKEN components to date. These fall into the following categories:

### *Testing of Authentication Service (AS)/Verification Service (VS)*

Five test participants provided STI-VS and STI-AS implementations for remote testing. In these cases, the test participants first originated calls using their STI-AS and confirmed that the testbed STI-VS could correctly verify the caller ID content. Then the test participants terminated calls that were initiated in the testbed and confirmed that their STI-VS could correctly verify the caller ID.

### *Testing of STI Certification Authority (STI-CA) and Certificate Repository (STI-CR)*

One participant provided an STI-CA and STI-CR for TN and SPC certificates and confirmed that the testbed could correctly originate calls (STI-AS) and terminate calls (STI-VS) using a third-party implementation.

### *Testing of Third-Party AS/VS*

Two participants demonstrated the ability to query the STI-AS and STI-VS functions in the testbed over published APIs and correctly perform SHAKEN authentication and verification functions. These tests demonstrate how an SP can use third-party AS/VS services to implement SHAKEN.

### *Testing SHAKEN with Toll-Free Application Server (TFAS)*

One participant used the testbed STI-AS and STI-VS functions to sign and verify toll-free calls using an IP TFAS, verifying that toll-free calls can be signed and verified by SHAKEN. Subsequent testing is expected in support of this use case.

STI testing to date has demonstrated validity of the SHAKEN framework in various realistic network configurations and demonstrated that independent implementations can interoperate successfully. The testing has also identified some issues with initial implementations (mainly with error handling) and provided useful feedback to implementers. Testing is ongoing, and a more detailed report is expected to be published in the future.

## 3. Conclusion

The ATIS Testbeds Focus Group was initiated to identify areas where an industry testbed could facilitate the transition to an all-IP network. Four areas were identified, test plans were drafted or completed, and various tests were conducted. This report briefly summarizes the results of these tests and the value provided to the industry.

# Annex A: JIT/ITN Number Assignment for Individual TN & Block Allocation

## Introduction

This document outlines a contribution to the TLT Testbed Numbering Allocation Sub-Team - Use Cases for Just-in-Time Number allocation. It provides a reasonable framework to open the possibility of ITN assignment based on existing requirements, rules, and law.

The main objective of the trial was to demonstrate allocation of numbering resources on a real-time, per customer basis within the framework of an established and trusted infrastructure and secure management of customer-proprietary information. The test plan provided number allocation to service providers using familiar access methods and the benefits of service provider portability.

The trial plan consisted of two phases:

- Phase 1 - The numbering allocation sub-team documented a system description and requirements, any necessary regulatory waivers, test participants, and high-level test plan describing the use cases chosen by the trial participants. This phase also addressed proof-of-concept (POC) using mock numbering data.
- Phase 2 - A testbed system was developed to provide the basic functionality of a Just-In-Time (JIT) allocation system for testing by external and internal test participants. This initial system did not have all real-time verification or processing connections to the Pooling Administration System nor the NPAC but instead utilized a test environment; however, it provided end-to-end capabilities for TN assignment through the GUI. No APIs were considered or established for real-time communications with users or between internal Neustar systems during this phase. This phase was limited to scenarios within the confines of an internal test environment and did not involve any external interactions outside of Neustar's test systems.

An additional test phase involving live network testing was considered, but not completed. This report includes a discussion of factors that would need to be addressed before live network testing is considered in the future.

This report documents all phases of the Test Plan as described above.

## Overview

### System Description

Number management for an authorized service provider requires a well-defined provisioning interface or automated API to manage the ownership and information related to telephone numbers.

This test plan is based on existing requirements for the use and acquisition of telephone numbers in the North American Numbering Plan, as set forth in various documents and orders. The current legal and regulatory hierarchy is:

- Federal Law – U.S.C.
- FCC – Orders, rules
- FCC – PA and NANPA contracts with Requirements Document and NPAC requirements (NAPM, LLC and FCC)
- States – Orders, rules
- Industry Guidelines

Before this mechanism could be tested in live networks, certain modifications and/or waivers would need to be granted or allowed by the FCC for this Test Plan since there is no accommodation in current rules and requirements for individual telephone number assignment by the numbering administrators. However, this Test Plan conforms to as many current rules and requirements as possible to maintain the integrity and future of the NANP. Issues and considerations necessary for this Test Plan include, but are not limited to:

- The allowance of single telephone number assignments by the numbering administrator(s) where currently only thousands-blocks and central office (CO) codes are assigned.
- Allowances for the non-TSP administrator to be assigned and manage thousands-blocks of numbers through the Pooling Administrator and interface with the NPAC to port TNs and receive information on administrator-assigned blocks from the NPAC. This involves the assignment of a valid OCN and/or SPID from the appropriate entity.
- Awareness of departure from existing requirements and rules for testing purposes regarding: SP certifications, forecasting requirements by SPs and by the

administrator, months-to-exhaust (MTE) calculations, first-in-first-out (FIFO) application processing, and utilization reporting for NRUF.
- The allowance of communication between the Test Bed numbering administrator and the LNPA and NPAC for the assignment and management of individual numbers.

The overall design of the Test Plan makes the following assumptions for possible live network testing:

- The neutral numbering administrator is allowed to forecast the demand for ITNs in each rate center and populate those ITN pools with existing available thousands-blocks, including the acceptance of donated contaminated thousands-blocks from SPs.
- The PA can populate necessary thousands-blocks in its database system and in the NPAC with the SPID associated with the administrator and with an LRN from the donating carrier's code for routing.
- The LRN would be one TN from the donated block assuming the block and code holders were the same in the testing process.
- Rate centers and LATAs would remain as they are today; however, changes to these underlying legacy geographic restrictions would not be an issue.
- The numbering administration system would have access to the LNPA/NPAC through the NPAC GUI in order to process ports from the administrator to the SP requesting TNs.
- The numbering administration system could process requests (new TNs and/or TN disconnects) on a real-time FIFO basis.
- Test Plan participants would be required to verify compliance with all necessary regulatory and industry requirements in the Test Plan area prior to commencing testing, thus allowing for real-time, machine processing for most applications.
- All existing thousand-block and code capabilities would still be available for all users in PAS.
- Numbers ported to these JIT-created LRNs prior to assignment would automatically route to a vacant code announcement for misdialed TNs because the LRN would direct the call to the switch of the donating carrier's CO code for vacant number treatment.
- Numbers ported to valid SPID/LRN combinations after assignment would route as all other ported TNs.
- At the end of the testing all TNs would be returned to the JIT pool and would snap back to the numbering administrator's SPID and LRN.

- The numbering administration system and the NPAC would allow (probably through the NPAC GUI in the testing) the numbering administrator to port ITNs within blocks assigned to the administrator on behalf of the SP.
- At the end of the testing, all blocks in the administrator's inventory would be transferred back to the original SP that donated the block(s).
- Test Plan participants would be confined to states and/or NPAs designated to be part of the trial plan.

## Overall System Description and Functionality

The test system would be separate from the existing Pooling Administration System (PAS) and NANPA Administration System (NAS). PAS is currently built and operated by the National Pooling Administrator (PA) designated by the FCC to manage the administration of all pooled numbering resources in the United States and Puerto Rico. PAS currently has both public and secure access through its GUI portal, as well as FTP applications. The secure portion keeps all company-specific confidential information available only to authorized users. Figure 1-1 below shows the current basic configuration of public and secure access.

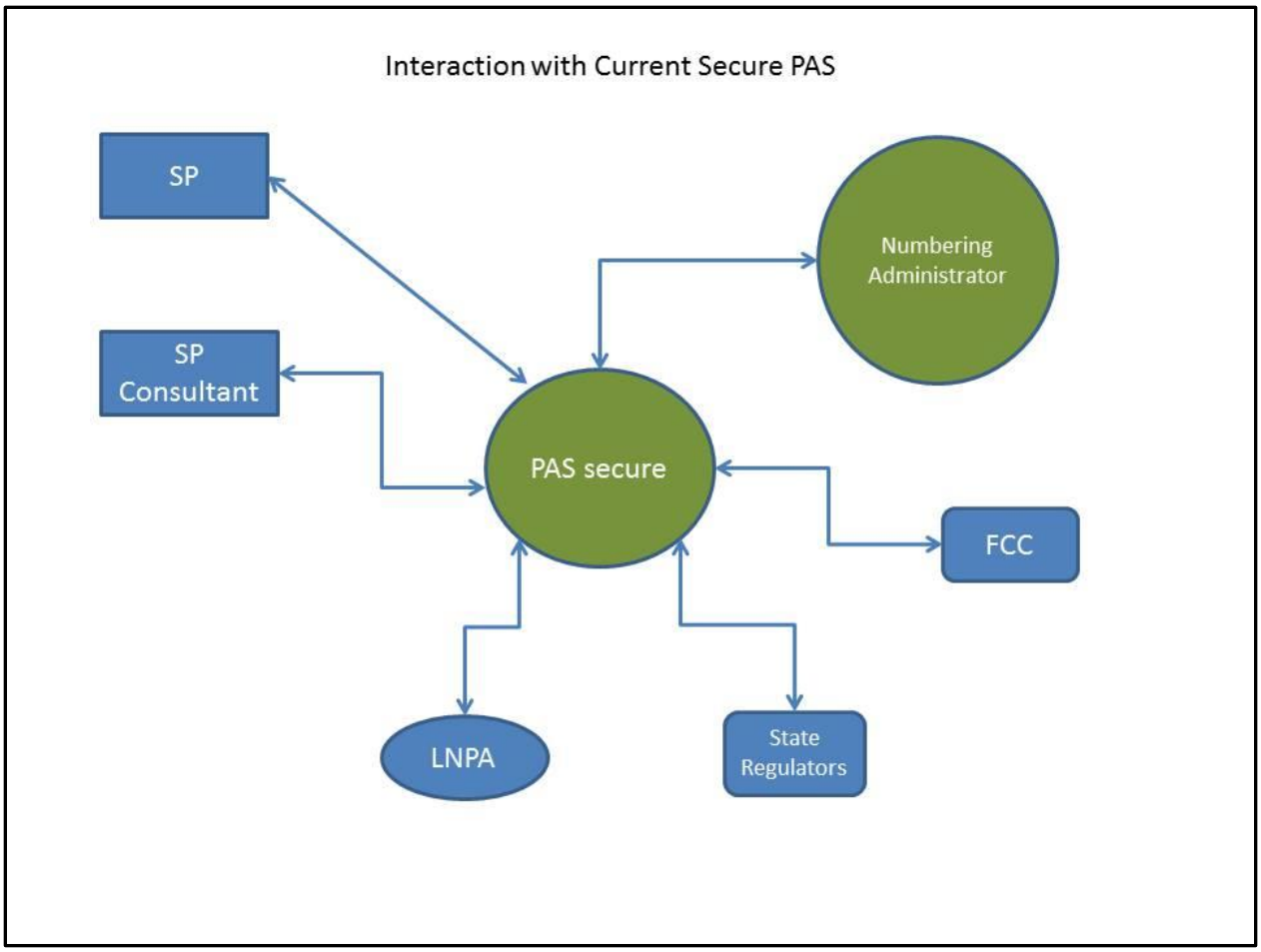



Figure 1-1. Secure Access to Pooling Administration System (PAS)

In this current configuration, each user type has access only to those portions of the system allowed under current guidelines and rules. For example, service providers have access to their own specific information, but not to related proprietary information of other service providers. Similarly, the state regulatory users only have access to proprietary information for data within their state. All users can access public information. For example, almost all information relating to assigned numbering resources is public information and can currently be accessed through the public portal.

The proposed test system would require a completely new and separate system with a separate portal and secure access to the system that is similar in many respects to the existing PAS access. Figure 1-2 shows a simple diagram of how this might work in conjunction with existing PAS and LNPA.

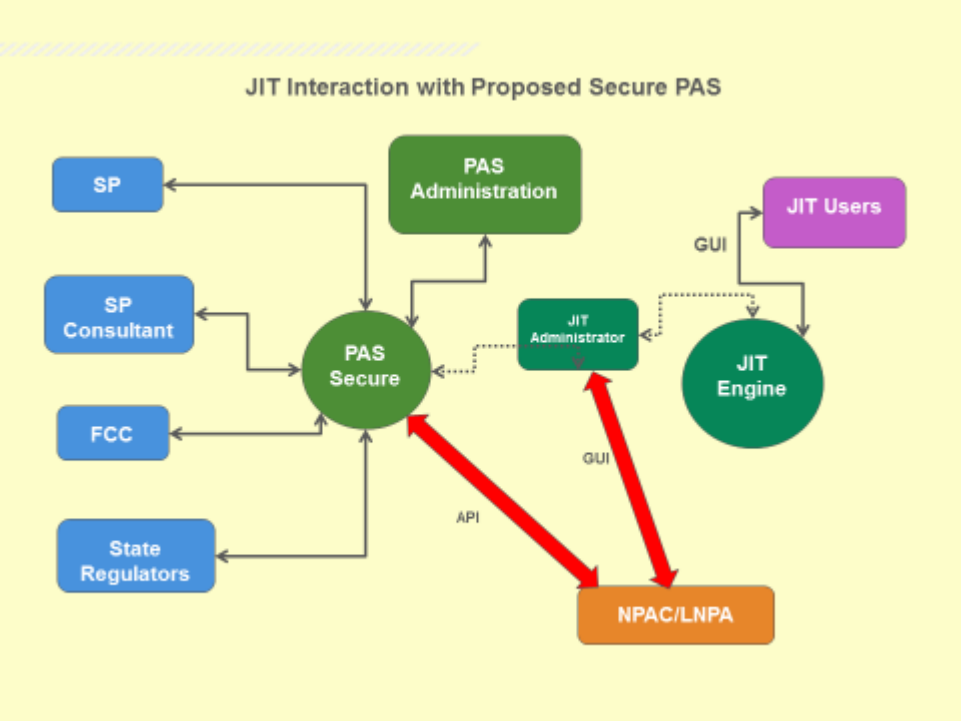



Figure 1-2. Secure Access to Pooling Administration System (PAS) with Test System Added

In this proposed configuration, a user interface would be created for the test system (e.g., donating blocks to the administrator, requesting new TN resources in blocks of 1 or greater TNs, or viewing information regarding those resources). However, because of the nature and limited size of a test system, a large portion of the potential functionality could be performed manually. Authorized test SP users would continue to have all existing functionality for a regular pooling SP user through the normal PAS GUI, and the JIT engine GUI would be totally separate and have menu items related to the requesting, management, and viewing of ITN resources.

The existing functionalities and the test system would not conflict with each other, and at the conclusion of the testing and evaluation, the test system would be eliminated and all test resources returned to their original status.

The essential components of the test system are:

- The final test configuration (i.e., potential live network testing) would require a new JIT test SP user portal for testing SPs to register in the test system as a valid user type and provide information to satisfy all current regulatory and industry requirements for numbering resources in the areas where testing would occur (e.g., two or three NPAs). This includes the ability of the JIT administrator to approve or deny any new registrations. This pre-approval process would allow for real-time processing of numbering requests through the JIT portal in most, if not all, cases without human intervention.
- Enhancements to the JIT engine would be required, including the establishment of a TN level database for keeping track of all TN level activities. This would include all necessary database management functions, such as the population of the database with available TNs, assigning and managing ITNs, and the acceptance of donated thousands-blocks.
- A link (probably the standard PAS GUI) is required between the test JIT system administrator and the PAS or NAS systems, and the LNPA/NPAC through the standard NPAC GUI or NPAC help desk. This allows for the verification of donated block information from current test participants and the porting of assigned TNs to testing SPs from the Numbering Administrator's SPID and LRN.
- The JIT engine would notify the testing SP of the assignment of the ITNs through automated processes similar to the porting notification today (email and/or work items).

## Waivers or Rule Changes for Consideration

Initial testing will not require formal changes to existing requirements or rules, due to the extremely limited nature of the testbed and the fact that existing systems are not affected. However, if testing was ever to go further than a testbed operation, some items would need to be considered:

- Permitting the assignment of TNs in less than thousands-block increments
- Allowing the JIT administrator to accept the transfer of over-contaminated blocks (greater than 10% contamination) from participating service providers.
- FIFO revisions, to allow test ITN assignment to be a separate category with FIFO within its own category. All other numbering requests would continue to be processed in their own FIFO order.
- Allowing the JIT numbering administrator to forecast and populate the ITN pools without requiring only SP forecasts

- Permitting the JIT numbering administrator to use LRNs created from a TN in a donated block to activate numbers in the NPAC prior to their assignment to SPs
- Modifying or eliminating certain other current requirements (e.g., Months-to-exhaust calculations, SP forecasting requirements, NRUF requirements). Since these requirements relate specifically to thousands-blocks, they may or may not apply in the same manner to individual numbers.

## Test Request Processing Proposal

The actual ITN request process has the following steps:

- Testing SPs register with the administrator and provide all necessary information to expedite processing of ITN requests, and
- Provide appropriate regulatory documentation for the area where testing is to occur
- The Administrator maintains populated ITN pools in areas designated by testing SPs either by block transfers from existing SP contaminated blocks or by assignment of available blocks from the pool.
- Testing SPs then sign into the test portal using their new secure sign-in ID and request resources by:
    - Selecting the NPA and rate center and the number of ITNs desired
    - Selecting from a menu or visual screen the desired TNs
        - By start of range
        - Specific TN(s)
        - Next sequential TNs in range
- The system automatically processes all requests against the SP's pre-registration information and any other current checks (e.g., Red Light Rule, NRUF on file)
- The system sends a port request to the NPAC on behalf of the requesting SP to port the requested TNs and receive confirmation and automatically notify the testing SP just as a normal port would occur, but through the JIT Numbering Administrator.

A simple diagram of this process is provided below in Figure 1-3.

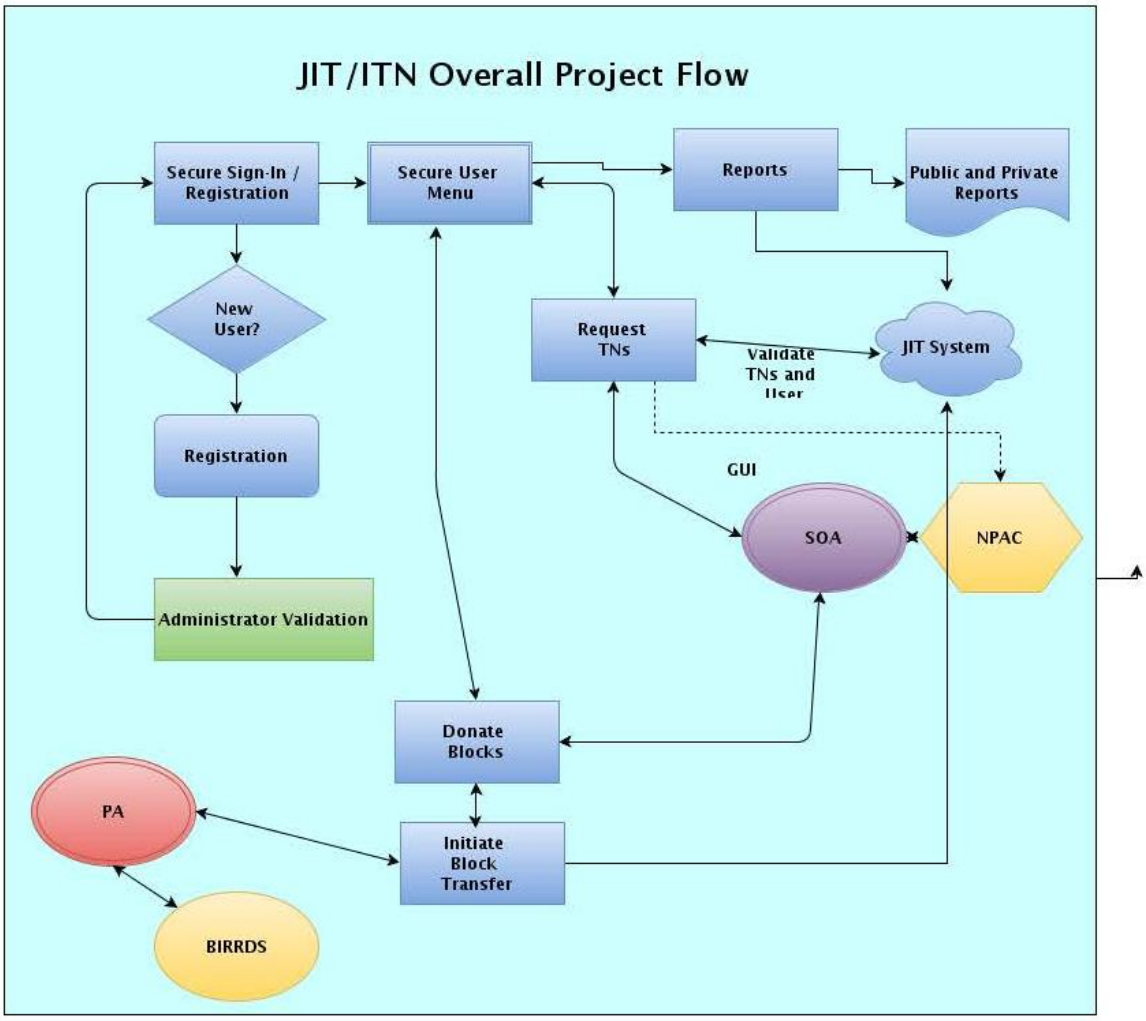



Figure 1-3. Project Flow

## Test Cases

JIT System Testing (Phase 2) includes the following test cases:

1. Development of Test Data for Phase 2 for Donations
2. Establishment of JIT User in PAS Test System
3. Establishment of JIT User and SPID in Neustar NPAC Test System
4. Testing of Block Transfer Process by JIT Administrator in PAS Test System
5. Testing of Successful Block Transfer to JIT Administrator in NPAC Test System

6. Population of JIT Test Database with Donated TNs
7. Development of JIT Test System Secure Sign-In
8. Development of GUI Screens for TN Requests
9. Development of Processes in JIT Test System for Processing TN Request(s)
10. Testing of Interaction with NPAC Test GUI to Perform Ports for Requested TNs
11. Testing of JIT Administrator Capability to Update JIT Database for Assigned TNs
12. Internal Regression Testing on all JIT System Development Processes

## Annex B: Toll Free IP Routing

### Scope

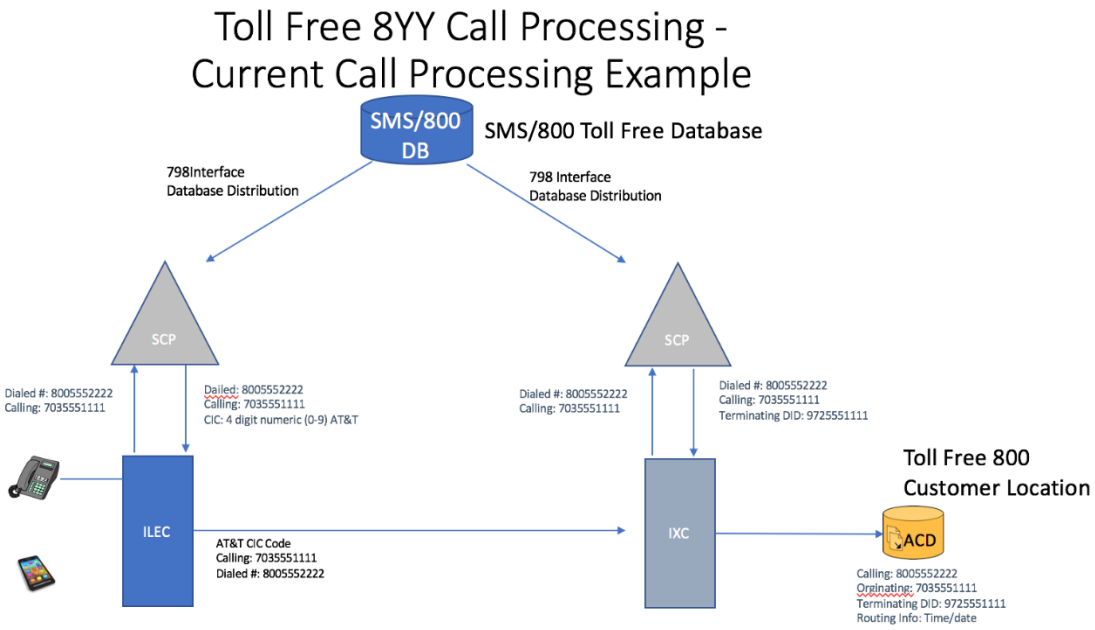
This document contains the detailed test plan for toll-free IP routing test plan using a TFAS, and providing the routing results using numbers with fully-qualified domain names

### Scenarios Tested

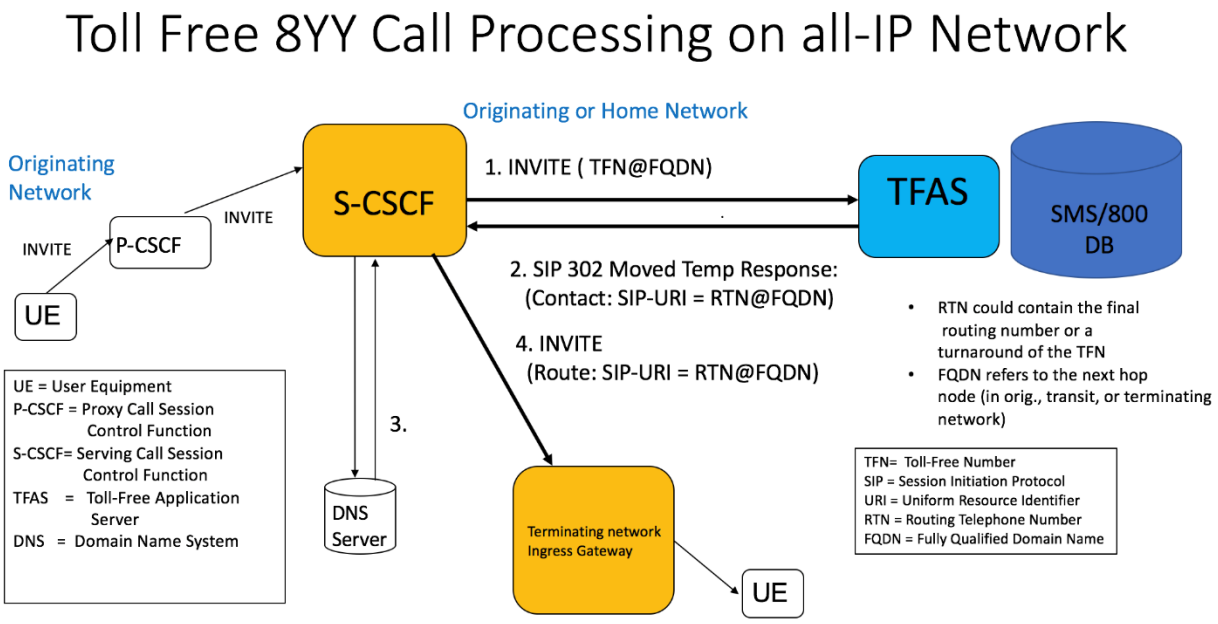
- Scenario 1 - Routing Based on Toll-Free Number (TFN) Only
- Scenario 2 - Routing on TFN and Originating NPA-NXX

### Functional Components

Current toll-free call processing diagram:


Toll Free 8YY Call Processing -
Current Call Processing Example
SMS/800
DB
SMS/800 Toll Free Database
798Interface
Database Distribution
798 Interface
Database Distribution
SCP
SCP
Dialed #: 8005552222
Calling: 7035551111
Dailed: 8005552222
Calling: 7035551111
CIC: 4 digit numeric (0-9) AT&T
Dialed #: 8005552222
Calling: 7035551111
Dialed #: 8005552222
Calling: 7035551111
Terminating DID: 9725551111
Toll Free 800
Customer Location
ILEC
AT&T CIC Code
Calling: 7035551111
Dialed #: 8005552222
IXC
ACD
Calling: 8005552222
Orginating: 7035551111
Terminating DID: 9725551111
Routing Info: Time/date

Toll Free IP Call processing diagram:




## Test Cases

### Test Case 1: Routing Based on Toll-Free Number (TFN) Only

- Input Parameter: Called Party ID (Toll-Free Number [TFN]) SIP Message Source: IN-VITE: **To** Header: SIP URI User field
- SIP Response Populated: SIP 302: Contact Header: SIP URI User Field

This simplified routing case excludes any other decision criteria, such as routing on the originating area or CgPN, and excludes all other decision nodes (such as time of day, or day of week) supported by the current SMS/800 system and SCPs. For the purposes of the testing, the cited FQDNs are not validated against carrier information or reference data describing any business agreements between the carriers and the toll-free service providers (Resp Orgs for the TFNs).

### Test Case 2: Routing on TFN and Originating NPA-NXX

This case is Case #2, where the originating NPA-NXX in the CgPN is also used as a decision criterion for call routing in addition to the TFN.

| Input Parameters | Extracted from SIP Message Source: |
|---|---|
| Called Party ID (Toll-Free Number [TFN]) | INVITE: To Header: SIP URI User field |
| User ID (Calling Party Number [CgPN]) | INVITE: P-Asserted-Identity Header: SIP URI User, if present <Else> INVITE: From Header: SIP URI User |

The combination of the TFN and CgPN NPA-NXX would be used as inputs to the simulated CR decision criteria in this case. The RTN and Destination FQDN are the outputs. This would correspond to the use of the 6-DIGIT decision node in current SMS/800 toll-free customer records.

SIP Response Populated: SIP 302: Contact Header: SIP URI User Field (Contact: sip:+1NPANXXXXXX@providerA.net; user=phone)

## Test Results

In both Test Cases the originating soft switch was able to query the TFAS via SIP INVITE. The TFAS built the response with the corresponding routing information (SIP-URI) based on the decision criteria information extracted for the INVITE. The originating soft switch successfully routed the calls utilizing the SIP-URI contained in the SIP 302 Moved Temporarily response from the TFAS. This test demonstrated the feasibility of using IP routing mechanisms for toll-free numbers.

# Annex C: Enhancing the LERG™ Routing Guide to Accommodate URI Hostnames or FQDNs

## Scope

This section contains the detailed test plan for the route provisioning and routing execution portions of the IP Enhanced LERG™[2] Routing Guide test plan as documented in "Phase 1", and in particular, the provisioning and execution for the "Variation 1" architecture using fully-qualified domain names (FQDNs) published in the LERG Routing Guide[3]. This scenario assumes FQDNs would be added to test scenarios and test cases for the Business Integrated Routing and Rating Database System (BIRRDS)[4] provisioning, and that BIRRDS would distribute the IP enhanced LERG information between carriers.

### List of Test Cases

The test cases are listed in table 1 below.

**Table 1: Tests**

| Test Case | Test Label | Test Title |
|---|---|---|
| 1 | | LERG Enhancements – BIRRDS provisioning/LERG distribution |
| | LE-RtLERG-001 | LERG Enhancements – Observe BIRRDS NPANXX Record Data Provisioned w/o FQDN; LERG Distribution |
| | LE-RtLERG-002 | LERG Enhancements – Observe BIRRDS LRN Provisioned Data w/FQDN; LERG Distribution |
| | LE-RtLERG-003 | LERG Enhancements – Observe BIRRDS NPANXX Data Provisioned w/FQDN; LERG Distribution |
| | LE-RtLERG-004 | LERG Enhancements – Observe BIRRDS LRN provisioned w/FQDN; LERG Distribution |
| | | |
| 2 | | LERG Enhancements – Route Server Provisioning |

[2] LERG™ Routing Guide is a trademark of Telcordia Technologies, Inc. dba iconectiv, and may be referenced as "LERG" in this document.
[3] References in this document to the LERG Routing Guide represent data that will be entered into the underlying database of the LERG Routing Guide; however, output for the test plan could conceivably be separate from the existing/production LERG Routing Guide set of files.
[4] BIRRDS is managed by Telcordia Technologies, Inc., dba iconectiv.

| | | |
|---|---|---|
| | LE-RtProv-001 | Provision route server for NPANXX/LRN with no FQDN association |
| | LE-RtProv-002 | Provision route server for NPANXX/LRN with FQDN association |
| | | |
| 3 | | LERG Enhancements – Routing Execution |
| | LE-RtEx-001 | Route call via NPANXX/LRN with no FQDN association |
| | LE-RtEx-002 | Route call via NPANXX/LRN with FQDN association |
| | LE-RtEx-003 | Route call via LRN with FQDN association, where corresponding NPANXX has no association |

## Test Scenario

### Association of Routing FQDNs to NPANXX and/or Location Routing Number (LRN) and routing via FQDN

This scenario tests the provisioning and use of routing FQDNs (referred to as "variation #1" in the Phase 1 document). The flow-through of data from a publishing terminating carrier to an originating carrier's route server, and the use of the resulting routing database entries to direct calls were verified.

# Functional Components

## Function Diagram for Test Cases 1 and 2: Provisioning

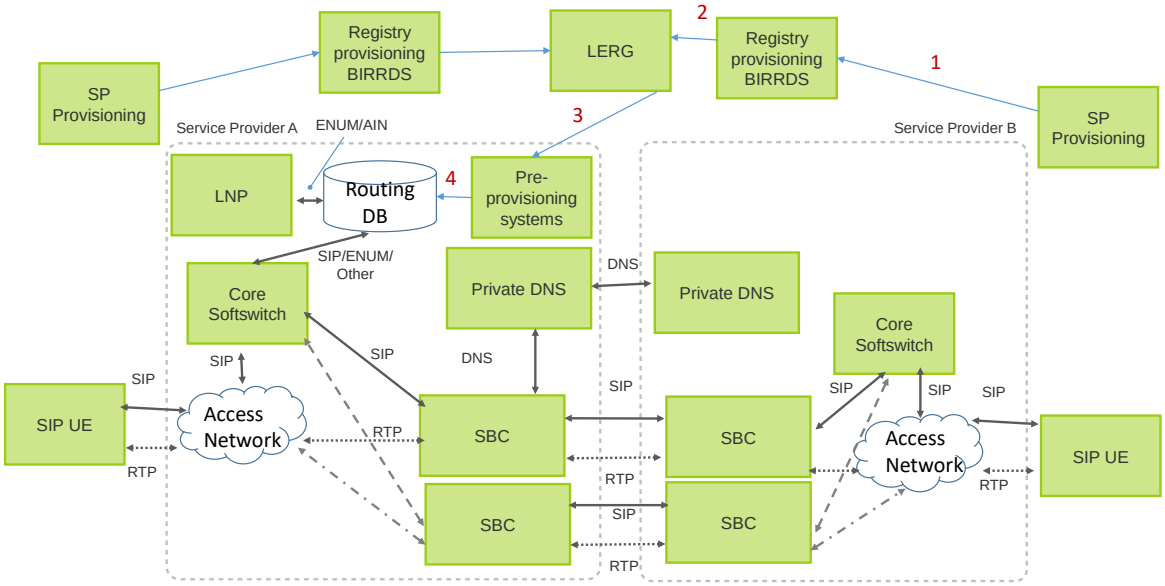



Fig.1 – IP-Enhanced LERG provisioning flow

## Function Diagrams for Test Case 3: Routing Execution

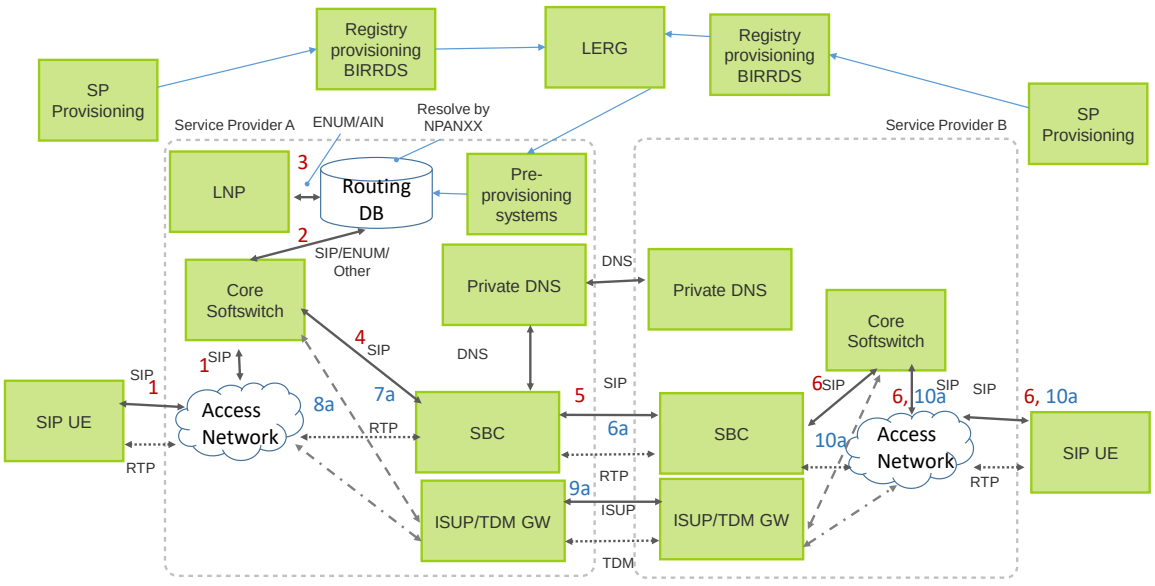


Fig. 2 – Session between IP-based access networks for destinations without routing FQDNs

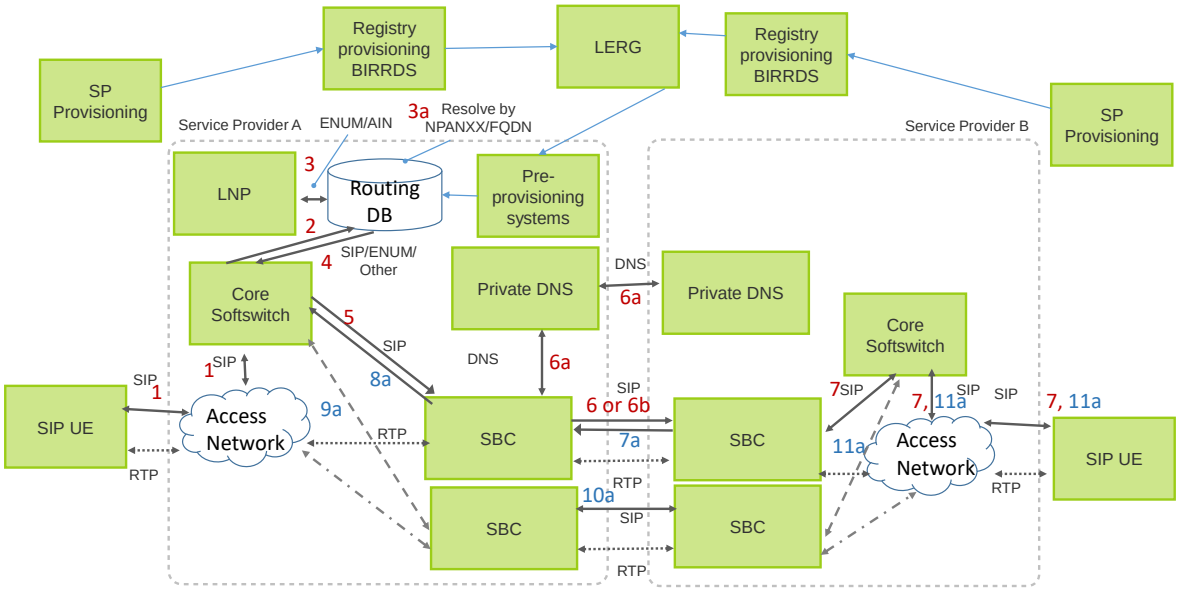



Fig. 3 – Session between IP-based access networks for destinations with provisioned routing FQDNs

## Test Cases

### Test Case 1: Test LE-RtLERG-001

*Test Case Title*

Observe BIRRDS NPANXX Record Data Provisioned w/o FQDN; LERG Distribution

*Test Case Label*

Test LE-RtLERG-001

*Purpose*

To observe and validate BIRRDS provisioned NPANXX data w/o FQDN information and distribute corresponding NPANXX LERG data.

### *References*

- *Testbeds Landscape Team Assessment and Next Steps, Version 2*
- LERGINFO.DOC
- LERGSPEC.DOC

### *Resource Requirements*

- Routing-registry personnel to process and distribute LERGTEST data files
- Service provider personnel to receive and validate LERGTEST data

### *Discussion*

This test scenario utilizes preexisting NPANXX BIRRDS/LERG data that already exists in the service provider's route servers. There is no FQDN data association; therefore, no additional BIRRDS provisioning is required.

## Test Setup

### *Equipment Configuration*

- Emulated routing-registry for data provisioning and LERG file distribution
- Emulated service provider systems for LERG data reception.

### *Preconditions*

As a precondition to this test case, a valid preexisting CO Code is selected, i.e. a CO Code assigned in accordance with the CO Code Assignment Guidelines (COCAG) maintained by the ATIS Industry Numbering Committee (INC). The COCAG principles and functions for assigning a CO Code include:

- The Assignment must be in compliance with all applicable local governmental, state, federal and the NANP area governmental regulations relative to the services a company wishes to provide.
- Assignment is provided by the NANP Administrator, via the NANP Administration System (NAS), to the service provider for use at a Switching Entity or Point of Interconnection the service provider owns or controls.

- Establishment of an Assigned CO Code Data Record by the NANP Administrator in BIRRDS.
- Establishment of an NPANXX Block Record by the service provider or its administrative agent in BIRRDS to specify additional attributes associated with the CO Code Data Record.

### *BIRRDS Test Input Data*

The following BIRRDS fields specify the NPANXX Block Record data entered by the administrative operating company that is authorized to modify the BIRRDS record information. No FQDN information is specified for an IP Route for this scenario; however, the IP Route information is specified only for the associated LRN as shown in the subsequent Test LE-RtLERG-002.

**Table 2: Service Provider 1 (SP1) NPANXX Block Record**

| Field | Field Description | Test Data Entry |
|---|---|---|
| NPANXX | Numbering Plan Area code (Area Code) in which the Central Office (CO) Code (NXX) has been assigned. NPANXX must be one assigned by Code Administration to the service provider in support of its normal course of business. | NPANXX(1)-SP1 |
| OCN | Operating Company Number identifies the CO Code holder company | OCN-SP1 |
| AOCN | Administrative Operating Company Number identifies a company or its agent that is authorized to create and modify the given BIRRDS record information | OCN-SP1 |
| BLOCK ID | Always "A" | A |
| STATUS | "E" indicates the establishment of a new record. "M" indicates a modification to an existing record. | E |
| EFF DATE | Future date that the FQDN routing will be effective (for the test case) (Y)es or (N)o. Must be Y to enable input of the FQDN in the IP-Voice field | 12/10/07 |
| IP Capable NXX | (Y)es or (N)o. Must be Y to enable input of the FQDN in the IP-Voice field | Y |
| IP-Voice | Hostname/FQDN | No Entry |

There are other BIRRDS fields associated with the NPANXX record that are not pertinent to provisioning FQDN information; therefore, they are not referenced in this table.

**Table 3: Service Provider 2 (SP2) NPANXX Block Record**

| Field | Field Description | Test Data Entry |
|---|---|---|
| NPANXX | Numbering Plan Area code (Area Code) in which the Central Office (CO) Code (NXX) has been assigned. NPANXX must be one assigned by Code Administration to the service provider in support of its normal course of business. | NPANXX(1)-SP2 |
| OCN | Operating Company Number identifies the CO Code holder company | OCN-SP2 |
| AOCN | Administrative Operating Company Number identifies a company or its agent that is authorized to create and modify the given BIRRDS record information | OCN-SP2 |
| BLOCK ID | Always "A" | A |
| STATUS | "E" indicates the establishment of a new record. "M" indicates a modification to an existing record. | E |
| EFF DATE | Future date that the FQDN routing will be effective (for the test case) (Y)es or (N)o. Must be Y to enable input of the FQDN in the IP-Voice field | 02/03/17 |
| IP Capable NXX | (Y)es or (N)o. Must be Y to enable input of the FQDN in the IP-Voice field | Y |
| IP-Voice | Hostname/FQDN | No Entry |

There are other BIRRDS fields associated with the NPANXX record that are not pertinent to provisioning FQDN information; therefore, they are not referenced in this table.

*LERG Test File Distribution*

For this test case, IP Capable NXX is "Y" and there is no FQDN IP route option; therefore, the LERG17TEST file will be generated with this test NPANXX; however, since there is no FQDN, the test participant(s) will route based on preexisting LERG6 data for Service Provider NPANXXs.

*Procedure*

Step 1 – LERG Distribution

- The LERG6TEST NPANXX data file, which includes preexisting LERG data for Service Provider NPANXXs is distributed to the test participant(s).
- If IP Capable NXX is "Y", then the LERG17TEST output fixed data file is generated with the test NPANXX data, which includes associated FQDN information, where applicable. The LERG17TEST file is subsequently distributed to service provider test participant(s).

Step 2 – The service provider test participant(s) receive the LERG6TEST and LERG17TEST NPANXX fixed data file.

Step 3 – The service provider test participant(s) validate the LERG6 and LERG17TEST NPANXX data in preparation for route server pre-provisioning.

*Observable Results*

The test data for Service Provider NPANXXs will be reflected in the LERG6TEST data file; however, since there is no corresponding FQDN IP route option, there will be no corresponding FQDN entry in the LERG17TEST data file for the test NPANXXs.

*Pass/Fail Criteria*

Files are distributed, and the data appears as expected (and as described in observable results).

## Test Case 1: Test LE-RtLERG-002

*Test Case Title*

Observe BIRRDS LRN Provisioned Data w/FQDN; LERG Distribution

### *Test Case Label*

Test LE-RtLERG-002

### *Purpose*

To observe and validate BIRRDS/LERG LRN provisioned data w/ FQDN information. This test case offers service providers or their agents the ability to identify an IP Route by establishing associations between an FQDN and an IP Capable LRN.

### *References*

- *Testbeds Landscape Team Assessment and Next Steps, Version 2*
- LERGINFO.DOC
- LERGSPEC.DOC

### *Resource Requirements*

- Routing-registry personnel to process and distribute LERGTEST data files.
- Service provider personnel to receive and validate LERGTEST data.

### *Discussion*

Multiple LRN records (based on the same NPANXX) can be created to address different combinations of service routes. For LRN records in BIRRDS, an IP Capable OCN field is today populated by the CO Code Holder to indicate the Operating Company Number (OCN) to which the LRN is associated and whereby termination via IP to the designated OCN is available.

Only when the IP Capable OCN field is populated can a new IP-Voice field be concurrently populated, via an FQDN in this test case. This would provide the ability to establish one route per LRN record. Since an NPANXX can technically serve as the basis for multiple (different) LRN records by variations in the last four digits of the LRN, each of which, in turn, may have different FQDNs.

## Test Setup

### *Equipment Configuration*

- Emulated routing-registry for data provisioning and LERG file distribution.
- Emulated service provider systems for LERG data reception.

### *Preconditions*

As a precondition to this test case, a valid preexisting CO Code is selected, i.e. a CO Code assigned in accordance with the CO Code Assignment Guidelines (COCAG) maintained by the ATIS Industry Numbering Committee (INC). The COCAG principles and functions for assigning a CO Code include:

- The Assignment must be in compliance with all applicable local governmental, state, federal and the NANP area governmental regulations relative to the services a company wishes to provide.
- Assignment is provided by the NANP Administrator, via the NANP Administration System (NAS), to the service provider for use at a Switching Entity or Point of Interconnection the service provider owns or controls.
- Establishment of an Assigned CO Code Data Record by the NANP Administrator in BIRRDS.
- Establishment of an NPANXX Block Record by the service provider or its administrative agent in BIRRDS to specify additional attributes associated with the CO Code Data Record.

### *BIRRDS Test Input Data*

The following BIRRDS fields specify LRN record information needed to provision an IP route in BIRRDS/LERG via an FQDN:

**Table 4: SP1 LRN Record**

| Field | Field Description | Test Data Entry |
|---|---|---|
| LRN | This is an existing or newly created LRN based on the first six digits of an assigned NPANXX. | LRN(1)-SP1 |
| STATUS | "E" indicates the establishment of a new LRN record. "M" indicates a modification to an existing LRN record. | M |
| EFF DATE | Future date that the FQDN routing will be effective (for the test case) | 06/26/16 |

| | | |
|---|---|---|
| IP CAPABLE OCN | This is the OCN of the CO Code Holder or may be the OCN of a company the CO Code Holder has identified for IP routing. | OCN-SP1 |
| IP-Voice | Hostname/FQDN | FQDN-SP1 (region1) e.g.: region1.sp1.example |
| OCN | OCN (of the Code Holder) | OCN-SP1 |
| There are other BIRRDS fields associated with the LRN record that are not pertinent to provisioning FQDN information; therefore, they are not referenced in this table. | | |

**Table 5: SP2 LRN Record**

| Field | Field Description | Test Data Entry |
|---|---|---|
| LRN | This is an existing or newly created LRN based on the first six digits of an assigned NPANXX. | LRN(1)-SP2 |
| STATUS | "E" indicates the establishment of a new LRN record. "M" indicates a modification to an existing LRN record. | E |
| EFF DATE | Future date that the FQDN routing will be effective (for the test case) | 10/26/17 |
| IP CAPABLE OCN | This is the OCN of the CO Code Holder or may be the OCN of a company the CO Code Holder has identified for IP routing. | OCN-SP2 |
| IP-Voice | Hostname/FQDN | FQDN-SP2 (Region 1)e.g.: region1.sp2.example |
| OCN | OCN (of the Code Holder) | OCN-SP2 |
| There are other BIRRDS fields associated with the LRN record that are not pertinent to provisioning FQDN information; therefore, they are not referenced in this table. | | |

### *LERG Test File Distribution*

The LERG12TEST file includes Location Routing Numbers (LRNs) that are or will be used in relationship to telephone numbers that are routed via Local Number Portability

routing concepts. This file identifies the company that has established the LRN as well as the switch to which that LRN should be associated.

The LERG16TEST file currently includes only select LRN test records and where the Code Holder (OCN appearing on the LRN record) has chosen to identify the availability of IP connectivity by population of the IP CAPABLE OCN.

The LERG16TEST file includes an IP-Voice field, which is populated with an FQDN when such is concurrently entered with the IP CAPABLE NXX field in BIRRDS. It is used in conjunction with LERG12TEST LRN Record data.

LERG12TEST and LERG16TEST distribution information will be used in subsequent route server provisioning tests performed by the participating service provider.

The following table illustrates the data field specifications for the LERG16Test file:

**Table 6: LERG16Test-File Field Specifications**

| LERG Field Description | Length | Position |
|---|---|---|
| LRN | 10 | 1-10 |
| Status E = Establish, M = Modify | 1 | 11 |
| Effective Date (mmddyy) | 6 | 12-17 |
| IP Capable OCN | 4 | 18-21 |
| OCN (of the Code Holder) | 4 | 22-25 |
| AOCN | 4 | 26-29 |
| *IP-Voice* | *255* | *30-284* |
| *Filler* | *16* | *285-300* |

*Procedure*

Step 1 – LERG Distribution –

- The LERG12TEST data file, which includes the test LRN Record data is generated and distributed to the service provider test participant(s).
- In addition, for this test scenario, an IP Capable OCN, the IP-Voice FQDN, and the effective data for which IP Routing is available for this test LRN is provisioned in BIRRDS; therefore, the LERG16TEST file is generated with the LRN information specified in the preceding table and is distributed to the test participant(s) for route server provisioning.

Step 2 – The service provider test participant(s) receive the LERG12TEST and LERG16TEST LRN fixed data file.

Step 3 – The service provider test participant(s) validate the LERG12TEST and LERG16TEST LRN data in preparation for route server pre-provisioning.

*Observable Results*

LRN test data will be reflected as an entry in the LERG12TEST data file and its corresponding FQDN information will be reflected in the LERG16TEST data file.

*Pass/Fail Criteria*

Files are distributed, and the data appears as expected (and as described in observable results).

## Test Case 1: Test LE-RtLERG-003

*Test Case Title*

Observe BIRRDS NPANXX Data Provisioned w/FQDN; LERG Distribution

*Test Case Label*

Test LE-RtLERG-003

*Purpose*

To observe and validate BIRRDS/LERG NPANXX provisioned data w/ FQDN information. This test case offers service providers or their agents the ability to identify an IP Route by establishing the association between an FQDN and an existing effective NPANXX "A" block record assigned to them. Testing of existing effective NPANXX assignments will keep tests focused on the process for provisioning FQDN information in BIRRDS/LERG, and not divert focus on other incidental industry processes/requirements that are necessary for obtaining new NPANXX assignments.

*References*

- *Testbeds Landscape Team Assessment and Next Steps, Version 2*

- LERGINFO.DOC
- LERGSPEC.DOC

### *Resource Requirements*

- Routing-registry personnel to process and distribute LERGTEST data files.
- Service provider personnel to receive and validate LERGTEST data.

### *Discussion*

To support IP-based route server provisioning and IP session routing, the LERG test data will include new "*IP-Voice"/* FQDN information in relation to NPANXX and LRN records.

For NPANXX "A" records in BIRRDS, an *IP Capable NXX* (Y/N) indicator is today populated by the CO Code (NXX) Holder to indicate, for any assigned *non-ported telephone numbers* (TNs) using that NPANXX, that termination via IP to the Code Holder company is available.

Only when the IP Capable NXX indicator is set to "Y" can a new IP-Voice field be concurrently populated and is to be an FQDN in this test case.

## Test Setup

### *Equipment Configuration*

- Emulated routing-registry for data provisioning and LERG file distribution.
- Emulated service provider systems for LERG data reception.

### *Preconditions*

As a precondition to this test case, a valid preexisting CO Code is selected, i.e. a CO Code assigned in accordance with the CO Code Assignment Guidelines (COCAG) maintained by the ATIS Industry Numbering Committee (INC). The COCAG principles and functions for assigning a CO Code include:

- The Assignment must be in compliance with all applicable local governmental, state, federal and the NANP area governmental regulations relative to the services a company wishes to provide.

- Assignment is provided by the NANP Administrator, via the NANP Administration System (NAS), to the service provider for use at a Switching Entity or Point of Interconnection the service provider owns or controls.
- Establishment of an Assigned CO Code Data Record by the NANP Administrator in BIRRDS.
- Establishment of an NPANXX Block Record by the service provider or its administrative agent in BIRRDS to specify additional attributes associated with the CO Code Data Record.

### *BIRRDS Test Input Data*

The following BIRRDS fields specify the NPANXX "A" record data, that would exist in BIRRDS included with FQDN information needed to provision an IP route in BIRRDS/LERG:

**Table 7: Service Provider 1 (SP1) NPANXX Block Record**

| | Field | Field Description | Test Data Entry |
|---|---|---|---|
| | NPANXX | Numbering Plan Area code (Area Code) in which the Central Office (CO) Code (NXX) has been assigned. NPANXX must be one assigned by Code Administration to the participating company in support of its normal course of business. | NPANXX(1)-SP1 |
| | OCN | Operating Company Number identifies the CO Code holder company | OCN-SP1 |
| | AOCN | Administrative Operating Company Number identifies a company or its agent that is authorized to create and modify the BIRRDS record. | OCN-SP1 |
| | BLOCK ID | Always "A" | A |
| | STATUS | "M" indicates a modification to an existing NXX record. | E |
| | EFF DATE | Future date that the FQDN routing will be effective (for the test case) | 12/10/07 |
| | IP Capable NXX | (Y)es or (N)o. Must be Y to enable input of the FQDN in the IP-Voice field | Y |
| | IP-Voice | Hostname/FQDN | FQDN-SP1 (Region 2)e.g.: region2.sp1.example |

| | | | |
|---|---|---|---|
| | | | |
| There are other BIRRDS fields associated with the NPANXX record that are not pertinent to provisioning FQDN information; therefore, they are not referenced in this table. | | | |

**Table 8: Service Provider 2 (SP2) NPANXX Block Record**

| | Field | Field Description | Test Data Entry |
|---|---|---|---|
| | NPANXX | Numbering Plan Area code (Area Code) in which the Central Office (CO) Code (NXX) has been assigned. NPANXX must be one assigned by Code Administration to the participating company in support of its normal course of business. | NPANXX(1)-SP2 |
| | OCN | Operating Company Number identifies the CO Code holder company | OCN-SP2 |
| | AOCN | Administrative Operating Company Number identifies a company or its agent that is authorized to create and modify the BIRRDS record. | AOCN-SP2 |
| | BLOCK ID | Always "A" | A |
| | STATUS | "M" indicates a modification to an existing NXX record. | E |
| | EFF DATE | Future date that the FQDN routing will be effective (for the test case) | 02/03/17 |
| | IP Capable NXX | (Y)es or (N)o. Must be Y to enable input of the FQDN in the IP-Voice field | Y |
| | IP-Voice | Hostname/FQDN | FQDN-SP2 (Region 2)e.g.: region2.sp2.example |
| There are other BIRRDS fields associated with the NPANXX record that are not pertinent to provisioning FQDN information; therefore, they are not referenced in this table. | | | |

### *LERG Test File Distribution*

The LERG6TEST file includes information associated with NPANXX "A" records.

The LERG17TEST file includes only NPANXX "A" records where the Code Holder (OCN appearing on the NPANXX "A" record) has chosen to identify the availability of IP connectivity by turning the IP Capable NXX indicator "on" (i.e. value = "Y").

The LERG17TEST file includes an IP-Voice field, which is populated with an FQDN when such is concurrently entered with the IP Capable NXX field in BIRRDS.

LERG6TEST and LERG17TEST file distribution information will be used in subsequent route server provisioning tests performed by the participating service provider.

For this test case, the IP Capable Indicator field for the designated NPANXXA Block Record is "Y" and a FQDN routing option is provided. As a result, this test NPANXX is included in the LERG17TEST distribution file provided to the test participant.

The following table illustrates the data field specifications for the LERG17 Test file:

**Table 9: LERG17 Test-File Field Specifications**

| | LERG Field | Length | Position |
|---|---|---|---|
| | NPA | 3 | 1-3 |
| | NXX | 3 | 4-6 |
| | BLOCK (A block only) | 1 | 7 |
| | Status | 1 | 8 |
| | Effective Date (mmddyy) | 6 | 9-14 |
| | IP Capable NXX (Y/N) | 1 | 15 |
| | OCN | 4 | 16-19 |
| | SWITCH | 11 | 20-30 |
| | AOCN | 4 | 31-34 |
| | *IP-Voice* | *255* | *35-289* |

| | | | |
|---|---|---|---|
| | *Filler* | *11* | *290-300* |

### *Procedure*

Step 1 – LERG Distribution

- The LERG6TEST NPANXX data file, which includes preexisting LERG data for Service Provider NPANXXs is generated and distributed to the test participant(s).
- If IP Capable NXX is "Y", then the LERG17TEST output fixed data file is generated with the test NPANXX data, which includes associated FQDN information. The LERG17TEST file is subsequently distributed to service provider test participant(s).

Step 2 – The service provider test participant(s) receive the LERG6TEST and LERG17TEST fixed data files.

Step 3 – The service provider test participant(s) validate the LERG6TEST and LERG17TEST NPANXX/FQDN data in preparation for route server pre-provisioning.

### *Observable Results*

The test data for Service Provider NPANXXs will be reflected in the LERG6TEST data file. The FQDNs information associated with the NPANXX assignments will appear in the LERG17TEST data file.

### *Pass/Fail Criteria*

Files are distributed and the data appears as expected (and as described in observable results).

### *Message Flow*

### *Known Issues*

## Test Case 1: Test LE-RtLERG-004

### *Test Case Title*

Observe BIRRDS LRN provisioned w/FQDN; LERG Distribution Test Case Label

Test LE-RtLERG-004

### *Purpose*

This test case offers service providers or their agents the ability to identify in the BIRRDS input database an IP Route by establishing associations between an FQDN and an IP Capable LRN.

### *References*

- *Testbeds Landscape Team Assessment and Next Steps, Version 2*
- LERGINFO.DOC
- LERGSPEC.DOC

### *Resource Requirements*

- Routing-registry personnel to process and distribute LERGTEST data files.
- Service provider personnel to receive and validate LERGTEST data.

### *Discussion*

Multiple LRN records (based on the same NPANXX) can be created to address different combinations of service routes. For LRN records in BIRRDS, an IP Capable OCN field is today populated by the CO Code Holder to indicate the Operating Company Number (OCN) to which the LRN is associated and whereby termination via IP to the designated OCN company is available.

Only when the IP Capable OCN field is populated can a new IP-Voice field be concurrently populated, with population intended to be an FQDN. This would provide the ability to establish one route per LRN Record. Note that an NPANXX can technically serve as the basis for multiple (different) LRN records by variations in the last four digits of the LRN, each of which, in turn, may have different FQDNs.

### *Test Setup*

#### *Equipment Configuration*

- Emulated routing-registry data provisioning and LERG file distribution
- Emulated service provider systems for LERG data reception.

*Preconditions*

As a precondition to this test case, a valid preexisting CO Code is selected, i.e. a CO Code assigned in accordance with the CO Code Assignment Guidelines (COCAG) maintained by the ATIS Industry Numbering Committee (INC). The COCAG principles and functions for assigning a CO Code include:

- The Assignment must be in compliance with all applicable local governmental, state, federal and the NANP area governmental regulations relative to the services a company wishes to provide.
- Assignment is provided by the NANP Administrator, via the NANP Administration System (NAS), to the service provider for use at a Switching Entity or Point of Interconnection the service provider owns or controls.
- Establishment of an Assigned CO Code Data Record by the NANP Administrator in BIRRDS.
- Establishment of an NPANXX Block Record by the service provider or its administrative agent in BIRRDS to specify additional attributes associated with the CO Code Data Record.

*BIRRDS Test Input Data*

The following BIRRDS fields specify LRN record information needed to provision an IP route via a FQDN in BIRRDS/LERG:

**Table 10: SP1 LRN Record**

| | Field | Field Description | Test Data Entry |
|---|---|---|---|
| 1 | LRN | This is an existing or newly created LRN based on the first six digits of an assigned NPANXX. | LRN(2)-SP1 |
| 2 | STATUS | "E" indicates the establishment of a new LRN record. "M" indicates a modification to an existing LRN record. | M |
| 3 | EFF DATE | Future date that the FQDN routing will be effective (for the test case) | 06/26/16 |
| 4 | IP CA-PABLE OCN | This is the OCN of the CO Code Holder or may be the OCN of a company the CO Code Holder has identified for IP routing. | OCN-SP1 |
| 5 | IP-Voice | Hostname/FQDN | FQDN-SP1 (Region 2) e.g.: region2.sp1.ex-ample |
| 6 | OCN | OCN (of the Code Holder) | OCN-SP1 |
| There are other BIRRDS fields associated with the LRN record that are not pertinent to provisioning FQDN information; therefore, they are not referenced in this table. | | | |

**Table 11: SP2 LRN Record**

| | Field | Field Description | Test Data Entry |
|---|---|---|---|
| 1 | LRN | This is an existing or newly created LRN based on the first six digits of an assigned NPANXX. | LRN(2)-SP2 |
| 2 | STATUS | "E" indicates the establishment of a new LRN record. "M" indicates a modification to an existing LRN record. | E |
| 3 | EFF DATE | Future date that the FQDN routing will be effective (for the test case) | 10/26/16 |

| | | | |
|---|---|---|---|
| 4 | IP CA-PABLE OCN | This is the OCN of the CO Code Holder or may be the OCN of a company the CO Code Holder has identified for IP routing. | OCN-SP2 |
| 5 | IP-Voice | Hostname/FQDN | FQDN-SP2 (Region 2) e.g.: region2.sp2.example |
| 6 | OCN | OCN (of the Code Holder) | OCN-SP2 |
| There are other BIRRDS fields associated with the LRN record that are not pertinent to provisioning FQDN information; therefore, they are not referenced in this table. | | | |

### *LERG Test File Distribution*

The LERG12TEST file includes Location Routing Numbers (LRNs) that are or will be used in relationship to telephone numbers that are routed via Local Number Portability routing concepts. This file identifies the company that has established the LRN as well as the switch to which that LRN should be associated.

The LERG16TEST file currently includes only select LRN test records and where the Code Holder (OCN appearing on the LRN record) has chosen to identify the availability of IP connectivity by population of the IP CAPABLE OCN.

The LERG16TEST file includes an IP-Voice field, which is populated with an FQDN when such is concurrently entered with the IP CAPABLE NXX field in BIRRDS. It is used in conjunction with LERG12TEST LRN data.

LERG12TEST and LERG16TEST distribution information will be used in subsequent route server provisioning tests performed by the participating service provider.

The following table illustrates the data field specifications for the LERG16 Test file:

**Table 12: LERG16 Test-File Field Specifications**

| | **LERG Field Description** | **Length** | **Position** |
|---|---|---|---|
| 1. | LRN | 10 | 1-10 |
| 2. | Status E = Establish, M = Modify | 1 | 11 |

| | | | |
|---|---|---|---|
| 3. | Effective Date (mmddyy) | 6 | 12-17 |
| 4. | IP Capable OCN | 4 | 18-21 |
| 5. | OCN (of the Code Holder) | 4 | 22-25 |
| 6. | AOCN | 4 | 26-29 |
| 7. | IP-Voice | 255 | 30-284 |
| 8. | Filler | 16 | 285-300 |

### *Procedure*

Step 1 – LERG Distribution

- The LERG12TEST data file, which includes the test LRN information is generated and distributed to the service provider test participant(s).
- In addition, for this test scenario, an IP Capable OCN, the IP-Voice FQDN, and the effective data for which IP Routing is available for this test LRN is provisioned in BIRRDS; therefore, the LERG16TEST file is generated with the LRN information and corresponding FQDN and is distributed to the test participant(s) for route server provisioning.

Step 2 – The service provider test participant(s) receive the LERG12TEST and LERG16TEST LRN fixed data file.

Step 3 – The service provider test participant(s) validate the LERG12TEST and LERG16TEST LRN data in preparation for route server pre-provisioning.

### *Observable Results*

Service Provider's LRN test data will be reflected as an entry in the LERG12TEST data file and its corresponding FQDN information will be reflected in the LERG16TEST file.

### *Pass/Fail Criteria*

Files are distributed and the data appears as expected (and as described in observable results).

## Test Case 2: Test LE-RtProv-001

### *Test Case Title*

Provision route server for NPANXX without FQDN association

### *Test Label*

LE-RtProv-001

### *Purpose*

To validate the baseline routing procedure to provision routing using standard methods without a routing FQDN.

### *References*

Phase 1 document

LERG References

Routing server references

### *Resource Requirements*

Systems as described under "equipment configuration," below

Personnel representing the originating service provider to administer and test the routing policy

### *Discussion*

This test demonstrates route provisioning to IP-NNI and/or TDM paths or some combination without referring to IP enhanced LERG data. In an IP transition phase, voice network routing may utilize a mixture of FQDN-based routing and non-FQDN-based routing.

### *Test Setup*

#### *Equipment Configuration*

Enhanced LERG Database (the relevant database records will not contain IP-based information)

Pre-provisioning system and flow-through provisioning system (may be emulated)

Route Server

LNP SCP (used as part of a test routing query)

#### *Test Pre-conditions*

One or more route lists are provisioned

Routes to terminating SP network exist from originating SP network. Route lists are not associated with FQDNs in the originating SP route server

An NPANXX of the terminating SP had not yet been provisioned in the originating SP route server, and the corresponding LERG entry does not contain a routing FQDN value.

Originating SP has downloaded LERG data containing new (not yet provisioned) records

#### *Procedure*

This is an expansion of "Step 4" from Fig. 1, above.

Step 4a: Pre-provisioning system reads updated records, or records not yet provisioned in the routing server from LERG and provides them to the flow-through provisioning subsystem

Step 4b: Flow-through provisioning system creates route update transaction

Step 4c: Flow-through provisioning system executes route update transaction

Administrator executes test routing query, which includes portability correction, and reads result.

*Observable Results*

Routing entry for NPANXX resolves to a route list containing the expected routes without first resolving to a FQDN.

Test query chooses expected route list

*Pass/Fail Criteria*

Expected routing is provisioned and executes correctly

## Test Case 2: Test LE-RtProv-002

*Test Case Title*

Provision route server for NPANXX/LRN with FQDN association

*Test Label*

LE-RtProv-002

*Purpose*

To validate the procedure to provision routing based on routing FQDNs.

*References*

Phase 1 document

LERG References

Routing server references

*Resource Requirements*

Systems as described under "equipment configuration," below

Personnel representing the originating service provider to administer and test the routing policy

### *Discussion*

This test validates a procedure for provisioning routing based on an FQDN associated with NPANXX/LRN records. The method of provisioning is implementation-dependent, and could include one of the following:

A routing server that supports identification of route lists by an FQDN-style name may support direct resolution using the FQDN as the label for the route list. In this case the FQDN name is provisioned directly as the route list name and the reference in the NPANXX/LRN routing entry.

Where a routing server that does not directly support identification of route lists by an FQDN-style name, consuming the FQDN may require that FQDNs be hashed or indexed to a value in the name-space supported by the routing server. In this case the FQDN is only used at provisioning time to group NPANXX/LRNs to a routing pattern and not at routing execution time.

Where a routing server takes the form of an ENUM/DNS server or can use DNS procedures directly, the routing query could be thought of as a combination of an ENUM query to resolve a TN to a URI (containing the exchanged FQDN), followed by a NAPTR/SRV/A-AAAA query to resolve the FQDN-portion of the URI to a list of egress SBCs. Note that this is an internal-side query not related to resolving a terminating peer SBC address. Also note that using ENUM/Domain name resolution in this way has the limitations that it cannot take into account factors other than the destination TN and it can only provide one translation to URI, whereas the originating carrier may want to pass different URI parameters (such as trunk group or terminating peer information) to different egress gateways. Variations could use a combination of an equipment-specific routing lookup to determine an associated FQDN followed by an internal DNS lookup.

### *Test Setup*

#### *Equipment Configuration*

Enhanced LERG Database

Pre-provisioning system and flow-through provisioning system (may be emulated)

Route Server

LNP SCP (used as part of a test routing query)

*Test Pre-conditions*

One or more route lists are provisioned

Routes to terminating SP network exist from originating SP network, and route lists are associated with FQDNs in originating SP route server

Terminating SP has initiated an NPANXX and/or LRN record update in BIRRDS to include a new or modified FQDN field

Originating SP has downloaded LERG data containing updated records

*Procedure*

This is an expansion of "Step 4" from Fig. 1, above.

Step 4a: Pre-provisioning system reads updated records from LERG and provides them to the flow-through provisioning subsystem

Step 4b: Flow-through provisioning system creates route update transaction

Step 4c: Flow-through provisioning system executes route update transaction

Administrator executes test routing query, which includes portability correction, and reads result.

*Observable Results*

Routing entry for NPANXX and/or LRN resolves to FQDN, which in turn resolves to route list containing the expected routes

Test query chooses expected route list

*Pass/Fail Criteria*

Expected routing is provisioned and executes correctly

## Test Case 3: Test LE-RtEx-001

### *Test Case Title*

Route call via NPANXX/LRN with no FQDN association

### *Test Label*

LE-RtEx-001

### *Purpose*

To validate the baseline case of routing by NPANXX/LRN with no associated routing FQDN entry

### *References*

Phase 1 document

### *Resource Requirements*

Equipment configuration as described below

Traces, Logs, and CDRs to verify operation

Personnel representing the originating service provider to initiate calls and validate routing operation

Personnel representing the terminating service provider to validate call completion

### *Discussion*

This test represents the baseline routing procedure, where a portability-corrected TN is used to directly select a route list, as opposed to referencing an IP-based FQDN that further resolves.

### *Test Setup*

#### *Equipment Configuration*

UEs (e.g. SIP client and/or access SBC)

Originating access network (includes access SBC)

Originating network softswitch

Route Server

LNP SCP

Originating network egress SBCs

Terminating network ingress SBCs

Originating network egress TDM gateway and terminating network ingress TDM gateway

Terminating softswitch, access network, and endpoint or test termination

### *Test Pre-conditions*

Originating and Terminating SPs have exchanged routing and signaling information.

Originating SP has route lists built in its routing server

An NPANXX has provisioned route list entries not tied to a FQDN. Route lists may contain IP-NNI routes and/or TDM routes

A ported or non-ported TN exists that resolves in LNP to the routed NPANXX

### *Procedure*

Step 1 – UE initiates a call to the ported number

Step 2 – Softswitch/access SBC initiates a routing query

Step 3 – Route server dips LNP database to portability-correct the destination TN

Step 4 – Route server resolves LRN to a route list directly and returns the response to the softswitch/access SBC

Step 5 – Access SBC/softswitch routes call to a selected egress SBC

Step 6 – Egress SBC INVITEs to terminating ingress SBC – if using an interconnection FQDN in the route list, execute DNS resolution to IP address (6a) and then INVITE (6b)

Step 7 – Terminating network (Ingress SBC, softswitch, terminating access network) completes call

Variation/regression: Non-ported number resolves based on NPANXX without a routing FQDN:

Step 1 – UE initiates a call to the non-ported number

Step 2 – Softswitch/access SBC initiates a routing query

Step 3 – Route server dips LNP database to portability-correct the destination TN

Step 3a – Route server looks up NPANXX and returns a route list directly

Step 4 – Route server returns the selected route list to the softswitch/access SBC

Step 5 – Access SBC/softswitch routes call to a selected egress SBC or TDM gateway

Step 6 – Egress SBC INVITEs to terminating ingress SBC – if using an interconnection FQDN in the route list, execute DNS resolution to IP address (6a) and then INVITE (6b)

Step 7 – Terminating network (Ingress SBC, softswitch, terminating access network) completes call

Variation "a" – attempting to second route in route list when first route is unavailable:

Steps 1-6 as in main procedure

Step 7a – First terminating network ingress SBC signals an error to the originating egress SBC (e.g. 503 temporarily unavailable)

Step 8a – Originating egress SBC signals failure to ingress SBC/softswitch

Step 9a – Originating ingress SBC/softswitch signals to egress SBC anchoring the second route in route list

Step 10a – Second egress SBC signals to second ingress terminating SBC

Step 11a – Terminating network completes call to UE as in main procedure Step 7

*Observable Results*

Call completes via expected path and reaches a termination

CDRs and traces record the expected routes chosen by FQDN

*Pass/Fail Criteria*

Call completes via the expected path

## Test Case 3: Test LE-RtEx-002

*Test Case Title*

Route call via NPANXX/LRN with FQDN association

*Test Label*

LE-RtEx-002

*Purpose*

To validate call routing based on routing FQDNs.

*References*

Phase 1 document

*Resource Requirements*

Equipment configuration as described below

Traces, Logs, and CDRs to verify operation

Personnel representing the originating service provider to initiate calls and validate routing operation

Personnel representing the terminating service provider to validate call completion

### *Discussion*

The exact routing method using FQDN depends on route server and provisioning capabilities (see test LE-RtProv-002 for discussion). The second described method, hashing or indexing FQDNs to route list identifiers is the most likely place to start, with ENUM/DNS-based routing procedures a possible second demonstration.

### *Test Setup*

#### *Equipment Configuration*

UEs (e.g. SIP client and/or access SBC)

Originating access network (includes access SBC)

Originating network softswitch

Route Server

LNP SCP

Originating network egress SBCs

Terminating network ingress SBCs

Terminating softswitch, access network, and endpoint or test termination

#### *Test Pre-conditions*

Originating and Terminating SPs have exchanged routing and signaling information.

Originating SP has route lists built and has associated one or more routing FQDNs with one or more route lists

Enhanced LERG information with FQDN associated to NPANXX (to LRN as a variation) has been shared

An NPANXX and an LRN have provisioned routing entries tying them to an FQDN

*Procedure*

Step 1 – UE initiates a call

Step 2 – Softswitch/access SBC initiates a routing query

Step 3 – Route server dips LNP database to portability-correct the destination TN

Step 3a – Route server looks up NPANXX and returns an FQDN

Step 4 – Route server resolves FQDN to a route list and returns the response to the softswitch/access SBC

Step 5 – Access SBC/softswitch routes call to a selected egress SBC

Step 6 – Egress SBC INVITEs to terminating ingress SBC – if using an interconnection FQDN in the route list, execute DNS resolution to IP address (6a) and then INVITE (6b)

Step 7 – Terminating network (Ingress SBC, softswitch, terminating access network) completes call

Variation: Call fails to first selected route and originating softswitch route advances to next egress SBC/terminating peer:

Steps 1-6 as in main procedure

Step 7a – First terminating network ingress SBC signals an error to the originating egress SBC (e.g. 503 temporarily unavailable)

Step 8a – Originating egress SBC signals failure to ingress SBC/softswitch

Step 9a – Originating ingress SBC/softswitch signals to egress SBC anchoring the second route in route list

Step 10a – Second egress SBC signals to second ingress terminating SBC

Step 11a – Terminating network completes call to UE as in main procedure Step 7

*Observable Results*

Call completes via expected path and reaches a termination

CDRs and traces record the expected routes chosen by FQDN

*Pass/Fail Criteria*

Call completes via the expected path

## Test Case 3: Test LE-RtEx-003

*Test Case Title*

Route call via LRN with FQDN association, where corresponding NPANXX is routed without an FQDN association.

*Test Label*

LE-RtEx-003

*Purpose*

To validate LRN-based call routing based on routing FQDNs as an exception to NPANXX routing without utilizing routing FQDNs.

*References*

Phase 1 document

*Resource Requirements*

Equipment configuration as described below

Traces, Logs, and CDRs to verify operation

Personnel representing the originating service provider to initiate calls and validate routing operation

Personnel representing the terminating service provider to validate call completion

### *Discussion*

This test represents the use of a routing FQDN (in practice this might be a secondary LRN associated with a set of NPANXXs) provisioned in the enhanced LERG to indicate an IP-based set of routes that may be different from the set of routes associated with the NPANXX or main LRN.

### *Test Setup*

#### *Equipment Configuration*

UEs (e.g. SIP client and/or access SBC)

Originating access network (includes access SBC)

Originating network softswitch

Route Server

LNP SCP

Originating network egress SBCs

Terminating network ingress SBCs

Originating network egress TDM gateway and terminating network ingress TDM gateway

Terminating softswitch, access network, and endpoint or test termination

### *Test Pre-conditions*

Originating and Terminating SPs have exchanged routing and signaling information.

Originating SP has route lists built and has associated one or more routing FQDNs with one or more route lists

Enhanced LERG information with FQDN associated to an LRN has been shared

An NPANXX has provisioned route list entries not tied to a FQDN and an LRN has a route list entry tied to a routing FQDN. Route lists may contain IP-NNI routes and/or TDM routes

A TN exists that is ported to the LRN associated with a routing FQDN

A non-ported number exists that is in the range of the NPANXX (not associated with a routing FQDN)

*Procedure*

Step 1 – UE initiates a call to the ported destination TN

Step 2 – Softswitch/access SBC initiates a routing query

Step 3 – Route server dips LNP database to portability-correct the destination TN

Step 3a – Route server looks up LRN associated with ported number and returns an FQDN

Step 4 – Route server resolves FQDN to a route list and returns the response to the softswitch/access SBC

Step 5 – Access SBC/softswitch routes call to a selected egress SBC

Step 6 – Egress SBC INVITEs to terminating ingress SBC – if using an interconnection FQDN in the route list, execute DNS resolution to IP address (6a) and then INVITE (6b)

Step 7 – Terminating network (Ingress SBC, softswitch, terminating access network) completes call

Variation/regression "a": Non-ported number resolves based on NPANXX without a routing FQDN:

Step 1 – UE initiates a call to the non-ported destination TN

Step 2 – Softswitch/access SBC initiates a routing query

Step 3 – Route server dips LNP database to portability-correct the destination TN

Step 3a – Route server looks up NPANXX and returns a route list directly (for testing purposes one that is different from the one resolved to the test LRN)

Step 4 – Route server returns the selected route list to the softswitch/access SBC

Step 5 – Access SBC/softswitch routes call to a selected egress SBC or TDM gateway

Step 6 – Egress SBC INVITEs to terminating ingress SBC – if using an interconnection FQDN in the route list, execute DNS resolution to IP address (6a) and then INVITE (6b)

Step 7 – Terminating network (Ingress SBC, softswitch, terminating access network) completes call

*Observable Results*

Call completes via expected path and reaches a termination

CDRs and traces record the expected routes chosen by FQDN for IP-provisioned LRN and by route list not associated with FQDN for routes to original NPANXX.

*Pass/Fail Criteria*

Call completes via the expected path

# Annex D: Secure Telephone Identity (STI) Test Plan

## 1 Scope

This document contains a test plan for Service Provider (SP) to SP use cases related to Secure Telephone Identity (STI). Specifically, it describes a set of test cases in support of the Signature-based Handling of Asserted information using toKENs (SHAKEN) industry framework [ATIS-1000074]. This framework specifies an end-to-end X.509-based cryptographic authentication and verification of the telephone number (TN) identity (and

potentially other information) in an Internet Protocol (IP)-based SP voice network. Underlying the SHAKEN framework are several Internet Engineering Task Force (IETF) documents, especially those being managed by the Secure Telephone Identity Revisited (STIR) Working Group. As the currently defined SHAKEN framework is expanded, it is anticipated that this document will be updated with additional test cases. This document also incorporates test cases to demonstrate successful acquisition of certificates as specified in: "SHAKEN: Governance Model and Certificate Management", PTSC-2017-00093R000, or ATIS-1000080 when approved).

## 1.1 STI Test Plan Scope

STI is defined to refer to the scope of functions being tested. It comes from STIR, the name of the IETF Working Group focused on RFC 4474bis, Personal Assertion Token (PASSporT) and STI credentials (based on digital certificates).

This test plan focuses on the use of E.164 TNs as SIP identities, and on securing these identities using cryptographic signatures. The test plan focuses on an E.164 TN being asserted as the calling number and how the SIP INVITE message will be signed and validated as part of an end-to-end SIP session.

This version of the test plan document primarily focuses on the SHAKEN framework as defined in ATIS-1000074. Its scope includes the format of STI tokens (including identity claims), the mapping of these tokens to SIP and the Authentication and Verification Services involved in signing and validating telephone calls. More specifically, this version of the test plan will demonstrate that the required Identity header field is created and processed correctly as specified. The intent is to provide assurance that the calling number is a secure telephone identity.

As noted earlier, as the SHAKEN framework is expanded, it is anticipated that this document will be updated with additional test cases. This document also incorporates test cases to demonstrate successful acquisition of certificates as specified in: "SHAKEN: Governance Model and Certificate Management", PTSC-2017-00093R000. To facilitate initial testing, informal procedures will be used as needed for configuring the components involved in testing. Examples include the public key certificate generation and management, as well as local policy-based decisions based on a positive or negative verification of the signature.

This test plan will focus on the description of call flows involving originating and terminating SPs but not initially involving transit SPs. For reference, it also defines network entities based on the 3GPP IMS architecture. Such a network entity definition is not intended to mandate any particular deployment and/or implementation. It also takes a specific network call flow approach to make test configurations consistent, while recognizing that there isn't a single network configuration that could be used for STI. These assumptions, taken together, are intended to limit the number of test points and terminology references for the testing described herein.

This version of the test plan assumes that public key certificates (or digital certificates) will be available via HTTPS at a minimum as a reference point for future STI Certificate Repositories (STI-CRs). Note that RFC 4474bis also identifies the use of DNSSEC as an alternate way of retrieving a digital certificate for the verification of signatures. However, DNSSEC is not part of the currently defined SHAKEN framework in ATIS-1000074.

This version of the test plan further assumes a basic and straightforward approach towards credentials or X.509-based digital certificate provisioning. There will be a limited number of Root Certification Authorities (CAs) that sign digital certificates. These, along with an STI Policy Administrator (STI-PA) will authorize an SP, for example, to sign telephone calls. SPs, themselves, can be Root CAs to support initial testing. The associated private keys are expected to be held securely and locally, and digital certificates will be publicly available via HTTPS. The digital certificate for a TN should be retrievable within the appropriate environment via the "info" parameter in the RFC4474bis Identity header field.

## 1.2 STI Use Case Scope

This test plan supports a set of SP use cases based on the SHAKEN framework, as primarily defined in ATIS-1000074, for demonstrating anti-spoofing. In brief, the scope of these use cases and the expected testing output between originating and terminating SPs include:

- Demonstrating that the appropriate SIP header fields used for digital signing and validation are created and processed correctly across SPs, in order to provide assurance that the calling number is a secure telephone identity;
- Demonstrating the use of STI-CRs in digital certificate validation;
- Testing the interworking between different implementations of STI functions;

- Identifying and collecting issues that could arise when digital signing and validation are used for STI anti-spoofing services;
- Testing different types of telephone calls and associated treatment, including local policy-based decisions and use of the SIP Reason header field (per RFC 3326):
    - Successfully verifying properly signed calls (200 'OK' response code)
    - Testing a call with a Date header field value that is older than the local policy for freshness permits (403 'Stale Date' response code)
    - Testing unsigned calls (428 'Use Identity Header' response code) is optional as not initially recommended for SHAKEN
    - Testing a URI that cannot be dereferenced (436 'Bad-Identity-Info' response code)
    - Testing an unsupported credential or improper digital certificate chain (437 'Unsupported credential' response code)
    - Testing improperly signed calls (438 'Invalid Identity Header' response code)
- Testing of specific systems/subsystems:
    - Authentication Service and Verification Service
    - X.509-based digital certificate retrieval and validation, to include testing revoked and outdated certificates used for signing
    - Specific cases of error generation and response

# 2 STI Overview

This section gives a brief overview of the SHAKEN framework for STI as currently defined in ATIS-1000074. It consists of a System Description, Reference Architecture, Functional Components and Reference Call Flow.

## 2.1 System Description

STI employs asymmetric key pairs to digitally sign and validate SIP INVITE messages in the particular case when E.164 TNs are used as SIP identities for originating calls. The testing in this version of the document focuses primarily on the format of STI tokens (including identity claims), the mapping of these tokens to SIP and the Authentication and Verification Services involved in signing and validating telephone calls. The systems to be used for this testing are based on the SHAKEN Reference Architecture (reproduced herein as Figure 1).

A number of assumptions are embodied in this version of the test plan and summarized below:

- E.164 TNs are used as SIP identities (i.e., the "orig" and "dest" claims are of type "tn"),
- Each TN used for testing is associated with a private and public key pair,
- Private keys are held securely by the originating SP,
- Public keys are contained in X.509-based digital certificates held by a STI-CR,
- Digital certificates are retrieved via the "info" parameter in the RFC4474bis Identity header field (or cached by the verifying service provider) within the environment under test,
- Digital signing is performed by the originating SP,
- The full form of PASSporT tokens is used and includes all of the baseline claims, as well as the SHAKEN extension claims (i.e., "ppt" PASSporT header parameter with a value of "shaken"), and
- Validation is performed by the terminating SP.

Note that identifying and collecting issues that could arise when digital signing and validation are used for STI anti-spoofing services is an important objective of testing.

## 2.2 Reference Architecture

This section illustrates the SHAKEN reference architecture for STI testing. The key network entities (using the 3GPP IMS architecture by example) and STI components include:

| Acronym | Description |
|---|---|
| STI-AS | The STI Authentication Service that performs the function of the authentication service defined in RFC 4474bis. It should either itself be highly secured and contain the SKS of private key(s) or have a secure interface to the SKS. |
| STI-VS | The STI Verification Service that performs the function of the verification service defined in RFC 4474bis. It has an HTTPS interface to the STI-CR to retrieve digital certificates for validation. |
| SKS | The Secure Key Store provides secure storage of private key information used directly by the STI-AS. |
| STI-CR | The STI Certificate Repository or Repositories are publicly accessible and store X.509-based digital certificates. It supports an HTTPS interface. |

| | |
|---|---|
| CSCF | The Call Session Control Function or SIP Registrar and Routing Function. It also has a SIP application server interface. |
| IBCF/TrGW | The Interconnection Border Control Function/Transition Gateway or ingress and egress point for SIP calls between SPs. |
| SIP UA | SIP User Agent, acting as initiating and terminating actors of end-to-end SIP calls. When under direct management control of an SP, the SP can assert the calling party identity in originating SIP INVITE messages initiated by the SIP UA. |
| CVT | Call Validation Treatment after a digital signature is positively or negatively verified (outside the scope of this test plan document). |
| Certificate Provisioning Service | Service used to provision digital certificates (this version of the test plan document assumes and describes a basic and straightforward approach towards digital certificate provisioning). |

Below, Figure 1 (as reproduced from ATIS-1000074) illustrates a reference architecture for STI testing. The focus of testing for this version of the document is primarily on the STI-AS and STI-VS functionality and the relevant SIP signaling and interfaces.

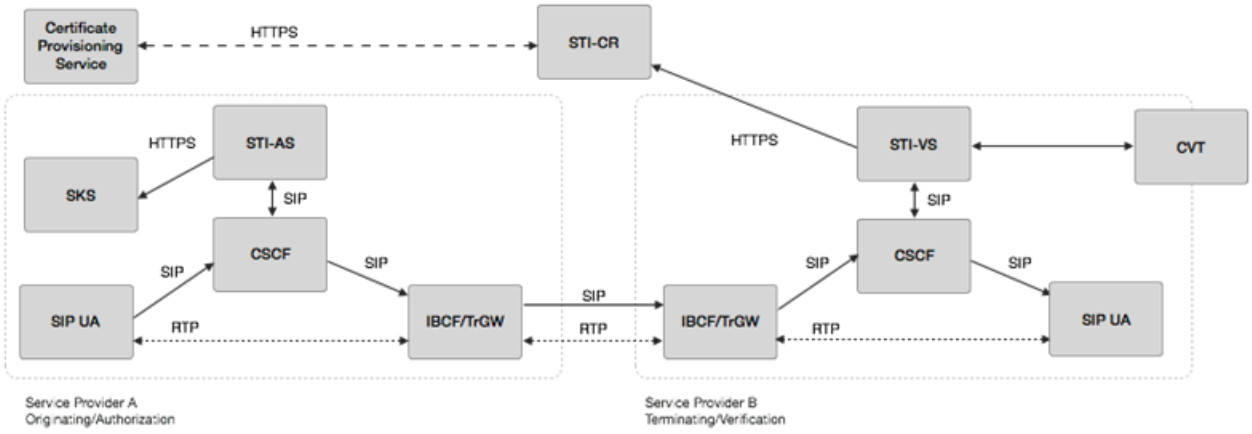



**Figure 1. SHAKEN Reference Architecture**

## 2.3 Functional Components

This section describes core testing requirements for the functional entities directly related to the digital signing and validation functions. The scope is the use of E.164 TNs as calling numbers.

| Functional Entity | Implementation | Hardware/Software Required | Implementer |
|---|---|---|---|
| STI-AS | Application Server configured via an interface from the CSCF | Application Server software | Originating SP |
| STI-VS | Application Server configured via an interface from the CSCF | Application Server software with HTTPS interface to STI-CR | Terminating SP |
| SKS | Private Key database | At a minimum, a small secure database to store private key(s) if not part of the STI-AS | Originating SP |
| STI-CR | Certificate Repository Server(s) | At a minimum, server software to store and provide access to X.509-based digital certificates | STI-CR Provider or SP |
| CSCF | 3GPP IMS SIP Registrar and Routing Server or equivalent | Server software supporting SIP Registrar and Routing function (ability to initiate originating and terminating call triggers and add a P-Asserted-Identity header field asserting that the calling number is a secure telephone identity | Originating and Terminating SP |
| IBCF/TrGW | Session Border Controller (if/as needed) | Session Border Controller or equivalent | Originating and Terminating SP (if/as needed) |
| SIP UA | SIP Client | Command line SIP client software or equivalent that is authenticated by the SP network | Originating and Terminating SP |
| CVT | Outside scope of test plan | | |

| Functional Entity | Implementation | Hardware/Software Required | Implementer |
|---|---|---|---|
| Certificate Provisioning Service | Outside scope of this version of test plan | For initial testing, software to acquire a digital certificate from a Root CA. SPs, themselves, can be Root CAs to support initial testing. The associated private key(s) are held in the SKS, and digital certificates stored in a STI-CR | Root CA Provider and/or Originating SP |

## 2.4 Reference Call Flow

This section describes the use of the Reference Architecture for anti-spoofing testing. Figure 2 (as also contained in ATIS-1000074) shows a flow for a digitally signed and validated call for a SIP session from an originating SP to a terminating SP.

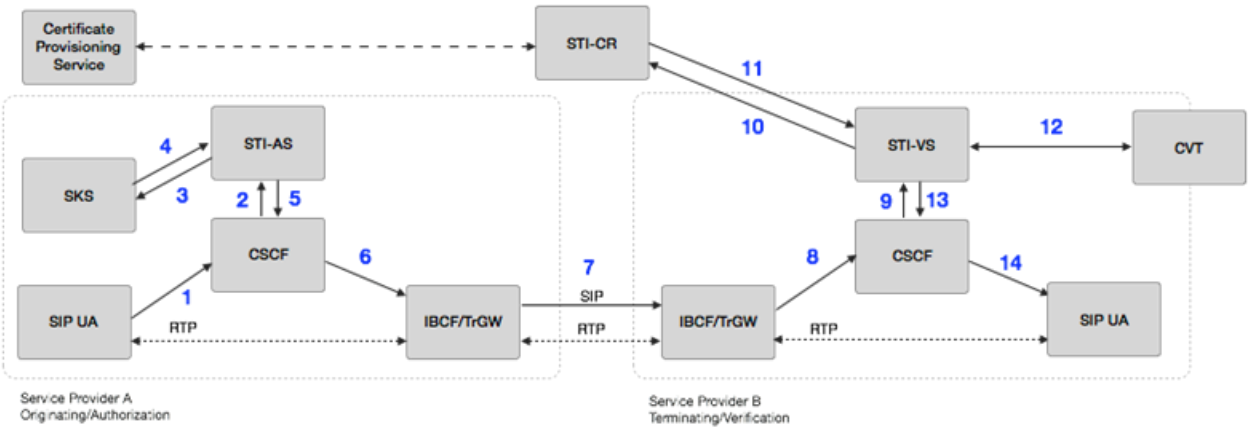



**Figure 2. Reference Call Flow for STI Testing**

A summary of the steps in the call flow for the digitally signing and validating of a SIP INVITE message for STI testing is outlined below. It is assumed that the following have taken place before the call is originated:

- The originating SP (i.e., SP A) provisions its test X.509-based digital certificate(s) in a STI-CR.
- SP A provisions its test private key(s) in the SKS.

1. The originating SIP UA, which first REGISTERs and is authenticated to the CSCF, creates a SIP INVITE with a TN identity.
2. The CSCF of SP A adds a P-Asserted-Identity header field asserting the TN identity of the SIP UA. The CSCF then initiates an originating trigger to the STI-AS for the SIP INVITE message.
3. The STI-AS of SP A first determines the legitimacy of the TN identity being used in the SIP INVITE message. The STI-AS then securely requests its private key from the SKS.
4. The SKS provides the private key in the response, and the STI-AS signs the SIP INVITE message and adds an Identity header field per RFC 4474bis using the TN identity in the P-Asserted-Identity header field.
5. The STI-AS passes the SIP INVITE message back to the SP A CSCF.
6. The originating CSCF, through standard resolution, routes the call to the egress IBCF.
7. The SIP INVITE message is routed to the terminating SP (i.e., SP B) through the standard inter-domain routing configuration.
8. The SP B ingress IBCF receives the SIP INVITE message from SP A.
9. The terminating CSCF initiates a terminating trigger to the STI-VS for the SIP INVITE message (note that the STI-VS must be invoked before terminating call processing).
10. The STI-VS of SP B uses the "info" parameter information in the Identity header field per RFC 4474bis to determine the STI-CR URI and makes an HTTPS request to the STI-CR.
11. The STI-VS checks revocation status of the digital certificate, validates it and then extracts the public key. It constructs the RFC 4474bis format and uses the public key to verify the signature in the Identity header field, which validates the TN identity used when signing the SIP INVITE message on the originating service provider STI-AS.
12. The CVT is an optional function that can be invoked to perform call spam analytics or other mitigation techniques and return a response related to what should be

signaled to the terminating SIP UA for a legitimate or illegitimate call. This function is out of the scope for this test plan.

13. Depending on the result of the STI validation, the STI-VS determines that the call is to be completed with any appropriate indicator and the SIP INVITE message is passed back to the terminating CSCF which continues to set up the call to the terminating SIP UA.
14. The terminating SIP UA receives the SIP INVITE message and normal SIP processing of the call continues, returning "200 OK" or optionally setting up media end-to-end.

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

A sequence diagram of events for the reference call flow for anti-spoofing testing is shown in Figure 3.

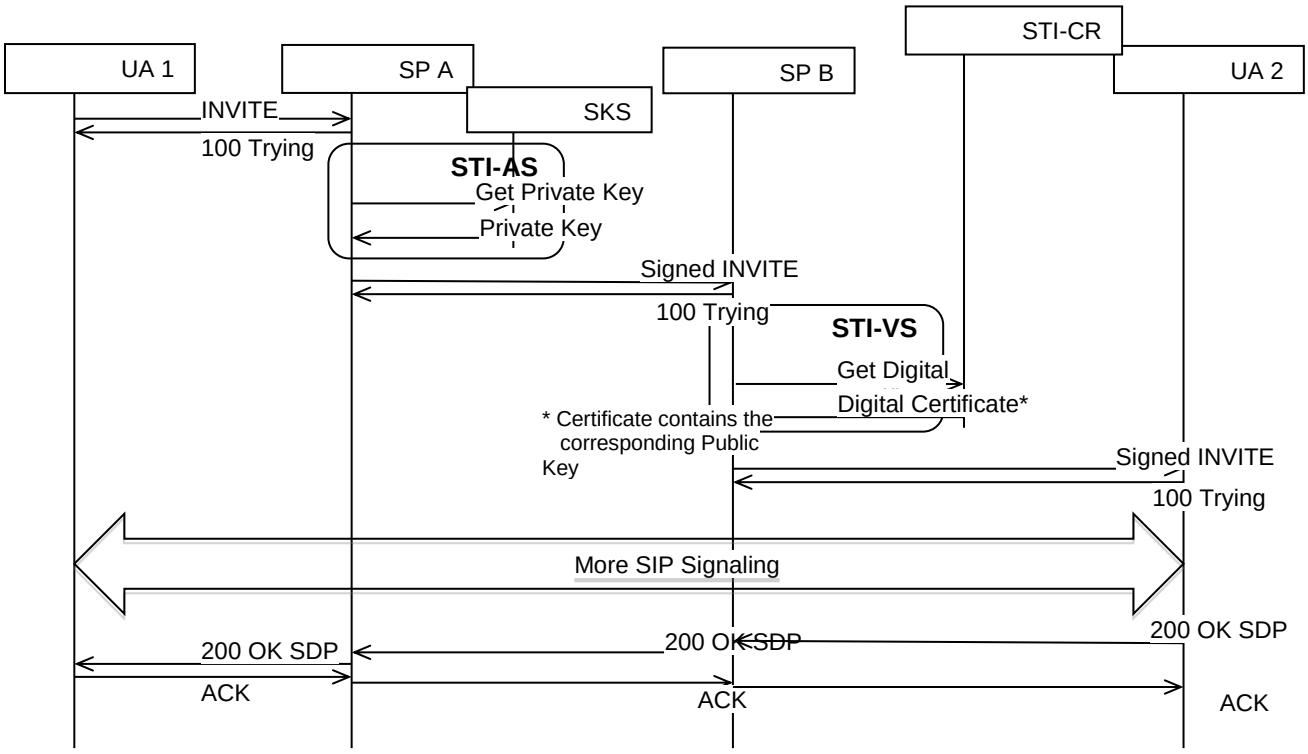



**Figure 3: STI-AS and STI-VS Call Flow Sequence Diagram**

## 2.5 STI Certificate Management Framework Overview

This section describes the certificate management framework for SHAKEN [ATIS-1000074], which establishes an end-to-end architecture that allows an originating Service Provider (SP) to authenticate and assert a telephone identity and provides for the verification of this telephone identity by a terminating service provider. The SHAKEN framework defines a profile, using protocols standardized in the IETF Secure Telephone Identity Revisited (STIR) Working Group (WG). "SHAKEN: Governance Model and Certificate Management", PTSC-2017-00093R000, provides recommendations and requirements for implementing these IETF specifications, draft-ietf-stir-passport, draft-ietf-stir-rfc4474bis, and draft-ietf-stir-certificates, to support management of Service Provider level certificates within the SHAKEN framework.

The SHAKEN framework uses X.509 certificates, as defined in "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", IETF [RFC 5280], to verify the digital signatures associated with Session Initiation Protocol (SIP) identifiers. PTSC-2017-00093R000 describes how the certificates are managed and created using the recommended governance model where there is a central STI Policy Administrator (STI-PA) who authorizes Service Providers (SPs) to acquire certificates from trusted Certification Authorities (CAs).

### *2.5.1 System Description*

The SHAKEN governance model for certificate management from PTSC-2017-00093R000 is reproduced below in Figure 4.

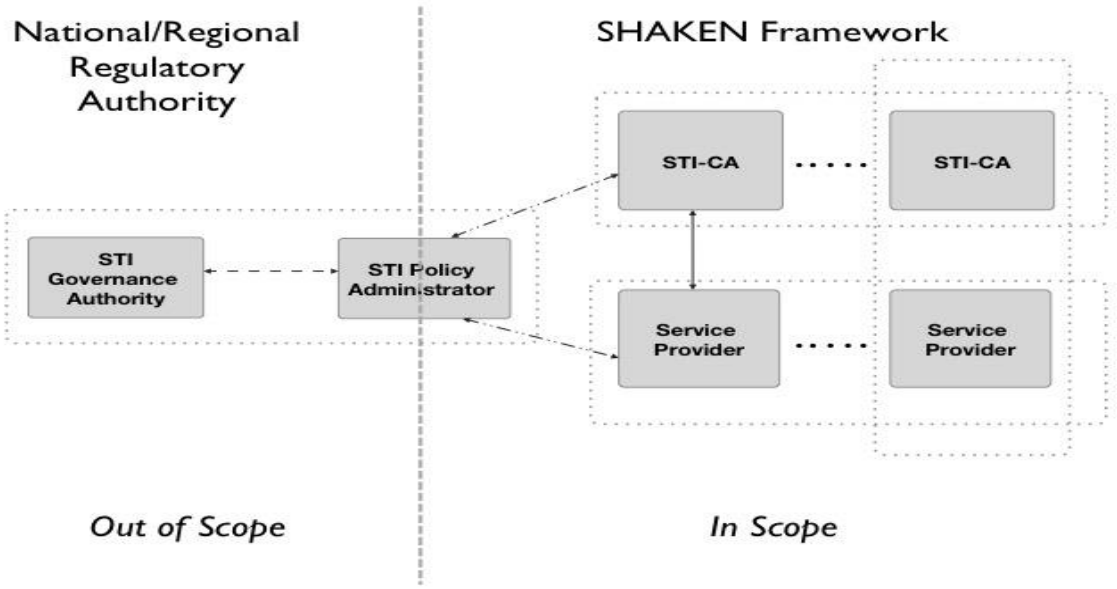



**Figure 4. SHAKEN Governance Model and Certificate Management**

The figure identifies the following roles associated with governance and certificate management:

- Secure Telephone Identity Governance Authority (STI-GA)
- Secure Telephone Identity Policy Administrator (STI-PA)
- Secure Telephone Identity Certification Authority (STI-CA)
- Service Provider (SP)

The STI-GA provides the interface to the SHAKEN framework for the enactment of policies established by a National/Regional Regulatory Authority (NRRA). The STI-GA is responsible for:

- Defining the policies and procedures around who can acquire certificates.
- Establishing policies around who can manage the PKI and issue certificates.

The STI-PA role satisfies the requirement "to apply the policies and procedures established for certificate management." The protocols and message flows between the STI-PA, the SPs, and STI-CAs to support the issuance and management of certificates to support STI are described in PTSC-2017-00093R000.

### 2.5.2 *Reference Architecture*

The SHAKEN certificate management architecture is illustrated in Figure 5 below.

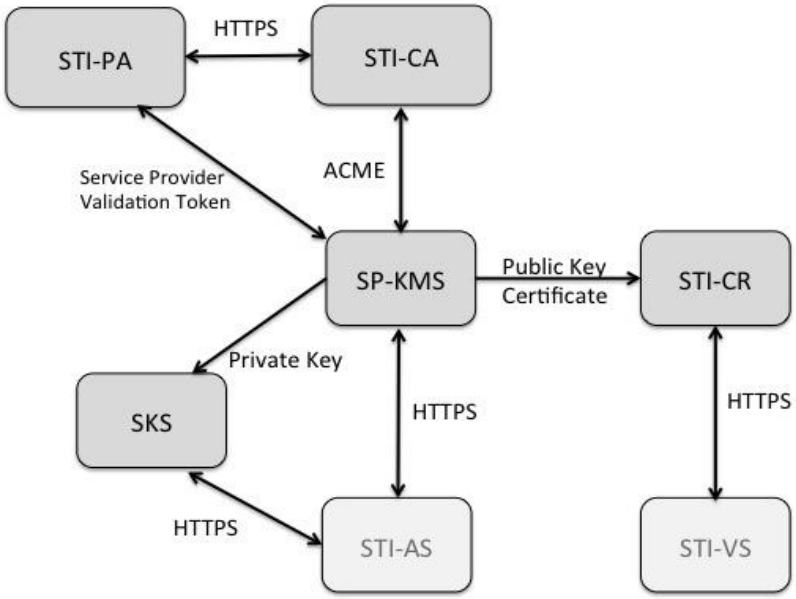



**Figure 5. SHAKEN Certificate Management Architecture**

The above SHAKEN certificate management architecture introduces the following additional elements:

- Service Provider Key Management Server (SP-KMS) - The service provider's server that generates private/public key pair(s) for signing, requests a certificate from the STI-CA, and receives the STI-CA signed public key certificate(s).
- Secure Key Store (SKS) - The store for private keys used by the originating service provider Authentication Service.
- Secure Telephone Identity Certificate Repository (STI-CR) - The HTTPS server that hosts the public key certificates used by the destination service provider's Verification Service to validate signatures.

Note that the STI-PA functional element also plays a key role in the certificate management architecture and related procedures.

### *2.5.3 Functional Components*

For this version of the test plan, the following sections describe the procedures and process steps related to test cases demonstrating the successful acquisition of certificates per PTSC-2017-00093R000. There are three major components: STI-PA, STI-CA, and SPs. They are involved in the following sets of procedures viewed from an SP perspective:

| **Test Case** | **Primary Components** |
|---|---|
| STI-PA Registration | SP and STI-PA |
| STI-CA Registration | SP and STI-CA |
| Service Provider Code (SPC) Token Request | SP and STI-PA |
| Certificate Signing Request (CSR) | SP and STI-CA (with STI-CA reliance on STI-PA) |

Some components shown in Figure 5 may be internal to or at the discretion of SPs.

### *2.5.4 Reference Process Steps*

For this version of the test plan, the Certificate Management Framework procedures and process steps refer to a set of test cases demonstrating an SP's successful acquisition of a service provider certificate – identified by a Service Provider Code (SPC) – corresponding to a key pair used to sign and validate calls originated by that SP.

These test cases, including readiness and provisioning steps, are summarized in the following table.

| Step Title | Description | Notes |
|---|---|---|
| Step 0. Configuration Readiness | STI-PA and STI-CA are configured | STI-CA is on STI-PA's list of valid STI-CAs |
| Step 1. STI-PA Registration | SP registers with STI-PA | SP acquires list of valid CAs |
| Step 2. STI-CA Registration | SP registers with STI-CA | SP establishes ACME credentials |
| Step 3. SPC Token Request | SP requests from STI-PA | SP receives signed SPC token |
| Step 4. Certificate Signing Request | SP requests from STI-CA | SP receives signed certificate |
| Step 5. SP Provisioning | SP is ready for SHAKEN calls | SP stores certificate and URL |

The procedures for these steps are described in the following sections.

#### 2.5.4.1 *Step 0. Configuration Readiness*

- The STI-PA maintains a list of approved/valid STI-CAs.
    - The list includes each STI-CA's public key certificate and account registration URL.
- The PA has a PA-admin certificate.
- The STI-PA has access to resources for validating SPs and their SPCs [likely OCNs].

#### 2.5.4.2 *Step 1. STI-PA Registration*

- The SP registers with the STI-PA using a username, password, and SPC.
- The STI-PA validates the SP and its SPC.
- The STI-PA provides the client_id/client_secret to the SP.
- The STI-PA provides access to the list of approved STI-CAs to the SP.
- [The SP acquires the list of approved STI-CAs from the STI-PA.]

#### 2.5.4.3 *Step 2. STI-CA Registration*

- The SP selects one STI-CA from the list of approved STI-CAs.
- The SP generates a CA-account key pair.

- The SP sends a new registration request to the selected STI-CA.
    - The request includes the public CA-account key.
    - The request is signed with the private CA-account key.
- The STI-CA validates the request and responds with a 201 OK.

#### 2.5.4.4 *Step 3. SPC Token Request*

- The SP requests a SPC token from the STI-PA.
    - The SP sends a request with username and password.
    - The request includes the client_id/client_secret in the header.
    - The SP provides its SPC.
    - The SP provides the fingerprint of its public CA-account key.
- The STI-PA validates the request.
- The STI-PA constructs the signed SPC token.
        - The token includes the URL of the STI-PA's PA-admin certificate.
        - The token includes the SP's SPC.
        - The token includes the fingerprint of the SP's public CA-account key.
        - The token includes the STI-PA's signature using its private key.
- The STI-PA sends a 200 OK response to the SP.
    - The response includes the signed SPC token.

#### 2.5.4.5 *Step 4. Certificate Signing Request*

- The SP generates a call-signing key pair.
    - The SP stores its private call-signing key.
- The SP constructs a CSR.
    - The SP provides its SPC using TN Authorization List extension.
    - The SP provides its public call-signing key.
- The SP sends its request to the STI-CA.
    - The SP includes the CSR in the request.
    - The SP includes a time frame in the request.
    - The SP signs the request with its private CA-account key.
- The STI-CA processes the certificate signing request.
    - The STI-CA extracts the SPC from the CSR.
- The STI-CA sends an authorization challenge response to the SP.
    - The response includes the URL for retrieving authorization details.
- The SP retrieves the authorization challenge details using the supplied link.

    - The challenge details include the SPC.
    - The challenge details include the URL for responding to the challenge.
- The SP sends a response to the URL it retrieved for responding to the challenge.
    - The response includes the (signed) SPC token the SP received from the STI-PA.
    - The response is signed with the SP's private CA-account key.
- The STI-CA validates the challenge response it received from the SP.
    - The STI-CA retrieves the STI-PA's certificate and extracts the PA-admin public key.
    - The STI-CA validates the signed SPC token.
    - The STI-CA creates the certificate.
    - The STI-CA sets the status to valid.
- The SP polls the STI-CA until it detects that the status has been set to valid.
- The SP sends a request for its certificate to the STI-CA.
- The SP receives a 200 OK response from the STI-CA.
    - The response includes the call-signing certificate.
    - The response includes other links and certificates.

#### 2.5.4.6 *Step 5. SP Provisioning*

- The SP stores the call-signing certificate in its STI-CR.
- The SP associates its URL for the SHAKEN public key certificate with its corresponding SPC private key.

# 3 STI Test Cases

The six test families are:

1. End-to-end functional tests
2. Detailed tests of protocol/data objects
3. STI Authentication Service testing
4. STI Verification Service testing
5. Interface testing
6. Supplemental testing

*Note: A number of the table entries are placeholders for further work.*

**End-to-End Functional Testing**

This family consists of tests demonstrating three of the most expected call scenarios: a valid signed call, an invalid signed call, and an unsigned call. Interactive Voice Response (IVR) messages are suggested as one way to convey the result to the caller.

| **Test #** | **Test Title** | **Test Purpose** | **Comments/Suggestions** |
|---|---|---|---|
| 3.1 | End-to-End Functional Testing | | Demonstrate expected call scenarios. |
| 3.1.1 | Valid Signed Call | Successful end-to-end signed call | Valid certificate associated with calling TN.<br>IVR: valid signed call |
| 3.1.2 | Invalid Signed Call (Response code 436) | 'Bad Identity info' | Can't retrieve certificate.<br><br>IVR: invalid, Response code 436 |
| 3.1.3 | Invalid Signed Call (Response code 437) | 'Unsupported Credential' | Can't validate certificate.<br><br>IVR: invalid, Response code 437 |
| 3.1.4 | Invalid Signed Call (Response code 438) | 'Invalid Identity Header' | Valid certificate not associated with calling TN.<br><br>IVR: invalid, Response code 438 |
| 3.1.5 | Unsigned Call (Response code 428) | 'Use Identity Header' | IVR: unsigned call, Response code 428 |
| 3.1.6 | Date Freshness<br><br>(Response code 403) | "Stale Date" | Date header field value is older than the local policy (e.g., 60 sec) for freshness.<br><br>IVR: date is older than 60 sec, Response code 403 |

**Detailed Protocol Testing**

This family of tests is intended for detailed testing of the protocols involved. In particular, they include the data objects used by the protocol.

| Test # | Test Title | Test Purpose | Comments/Suggestions |
|---|---|---|---|
| 3.2 | Detailed Protocol Testing | | Examine the protocol/data objects used in STIR/SHAKEN |
| 3.2.1 | Certificate Testing | Examine certificate-related errors | Tests errors in validation, contents, and revocation |
| 3.2.1.1 | Certificate Validation and Contents Testing | Certificate validation or content errors | - Invalid dates<br>- Invalid signature |
| 3.2.1.2 | Certificate Revocation Status Testing | Certificate revocation status failures | - CRL/OCSP checking |
| 3.2.1.3 | Trust Anchor Testing | Chain of trust failures | - Invalid chain of trust<br>- Invalid trust anchor |
| | | | |
| 3.2.2 | Identity Header Testing | Examine header-related errors | |
| 3.2.2.1 | Valid PASSporT token | Identity header validation | |
| 3.2.2.2 | "ppt" parameter | Identity header validation | |
| 3.2.2.3 | "info" parameter | Identity header validation | |
| | | | |
| 3.2.3. | PASSporT object Testing | Examine object-related errors | |
| 3.2.3.1 | "typ" attribute | PASSporT token header validation | |

| | | | |
|---|---|---|---|
| 3.2.3.2 | "alg" attribute | PASSporT token header validation | |
| 3.2.3.3 | "x5u" attribute | PASSporT token header validation | |
| 3.2.3.4 | "iat" attribute | PASSporT token claim validation | |
| 3.2.3.5 | "orig" attribute | PASSporT token claim validation | |
| 3.2.3.6 | "dest" attribute | PASSporT token claim validation | |
| 3.2.3.7 | "attest" attribute | PASSporT token claim validation | |
| 3.2.3.8 | "origid" attribute | PASSporT token claim validation | |

**STI Authentication Service Testing**

This family of tests exercises the Authentication Service subsystem.

| Test # | Test Title | Test Purpose | Comments/Suggestions |
|---|---|---|---|
| 3.3 | STI Authentication Service Subsystem Testing | | |
| 3.3.1 | AS Functional Tests | | |
| 3.3.1.1 | If PAI used as Secure Telephone Identity | Test whether PAI is given priority over From | Rules/Criteria:<br><br>(a) "PAI" (if present) else "From" |
| 3.3.1.2 | E.164 number in the SIP URI is identified as a TN | URI user-part of the form "+17005551008" in the SIP URI with | For instance,<br><br>sip:+15552223333@example.com;user=phone |

| | | | |
|---|---|---|---|
| | | "user=phone" parameter in it. | |
| 3.3.1.3 | E.164 number in the TEL URI is identified as a TN | URI user-part of the form "+17005551008" in the TEL URI | For instance,<br><br>tel:+15552223333 |

***STI Verification Service Testing***

This family of tests exercises the Verification Service subsystem.

| **Test #** | **Test Title** | **Test Purpose** | **Comments/Suggestions** |
|---|---|---|---|
| 3.4 | STI Verification Service Subsystem Testing | | |
| 3.4.1 | VS Function Testing | | |
| 3.4.1.1 | Success with valid certificate | Verification to succeed if the certificate is validated to be from trusted source | |
| 3.4.1.2 | Failure with expired certificate | Verification to fail if the certificate has expired | |
| 3.4.1.3 | Failure due to Certification Revocation check | Verification to fail if the certificate is found to have been revoked | |
| 3.4.1.4 | Date Freshness Test | If the Date parameter freshness test fails, a 403 – 'Stale Date' should be returned | The assumption is that the Date value is within 60 seconds from the current time (configurable) |
| 3.4.1.5 | Success on Missing Identity Header | 428 – 'Use Identity Header' error should **NOT** be is returned if no Identity header received | ATIS SHAKEN recommends not to return a 428 until wider adoption of SHAKEN. |
| 3.4.1.6 | Failure on Bad Identity Info | 436 – 'Bad Identity Info' should be returned if the URL in the 'info' parameter couldn't be dereferenced | |
| 3.4.1.7 | Failure on Unsupported credential | 437 – 'Unsupported credential' when the verifier doesn't | |

| | | | |
|---|---|---|---|
| | | support/trust the certificate chain | |
| 3.4.1.8 | Failure on Signature Verification Error | 438 – 'Invalid Identity Header' returned when the signature verification fails | |
| 3.4.1.9 | Use of PAI as STI | If present, PAI must be used to derive the orig claim | |

***Interface Testing***

This family of tests is designed to exercise certain interfaces within a service provider, between a service provider and an external component, or between service providers.

| Test # | Test Title | Test Purpose | Comments/Suggestions |
|---|---|---|---|
| 3.5 | Interface Testing | | |
| 3.5.1 | Private Key Access | | |
| 3.5.2 | CSCF-CSCF Interworking | | (includes NNI) |
| 3.5.3 | Certificate Retrieval | Support call-processing validation and signing requirements | Cover basic certificate, OCSP, and CRL requests. Optionally, test certificate creation/revocation status |
| 3.5.4 | Originating UA Testing | | |
| 3.5.5 | Terminating UA Testing | | |

**Supplemental Testing**

This family of tests demonstrates the use of additional components or functions that are not necessarily part of the common functional architecture or other five test families above.

| Test # | Test Title | Test Purpose | Comments/Suggestions |
|---|---|---|---|
| 3.6 | Supplemental Testing | | |

| | | | |
|---|---|---|---|
| 3.6.1 | Distributed Service Bureau Infrastructure | | |
| 3.6.2 | Reference Plane | | |

## 3.1 End-to-End Functional Testing

### *3.1.1 Valid Signed Call*

#### 3.1.1.1 *Purpose*

The purpose of this test is to validate a successful end-to-end signed call.

#### 3.1.1.2 *Test Setup*

##### 3.1.1.2.1 Test Pre-conditions

The following test pre-conditions apply:

1. Test environments are reachable, preferably over the public Internet
2. Routing attributes of ingress IBCF/TrGW are shared
3. The test E.164 numbers are shared
4. Public certificate(s) required are issued
5. Share URI (https recommended) to resolve to associated public certificate used as the "info" parameter (or "x5u" claim) in the SIP Identity header
6. Agreement on the accepted codecs (minimum GSM, PCMU, PCMA)
7. Confirm whether both UDP and TCP transports are supported for call signaling. At a minimum, UDP transport should be supported
8. Support for "jumbo" UDP packets is required throughout the test environment to avoid restrictions on UDP packet sizes larger than 1,500 bytes and an outcome of a 403 Forbidden response code
9. Confirm whether both the EC and RSA key algorithms are supported. Use of EC is encouraged since it results in substantially smaller Identity headers
10. For the Verification Service, all suitable trust-related materials are provisioned

##### 3.1.1.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header included in the INVITE message includes the full form of the PASSporT token

3. Confirm that the call is established and both the calling party and the called party can communicate with each other

#### 3.1.1.3 *Observable Results*

##### 3.1.1.3.1 Message Flows

The associated message flow for this test is Figure 3. This assumes that the optional use of the Reference Plane is not involved.

##### 3.1.1.3.2 Pass/Fail Criteria

This test will pass if the call setup is successful and the two parties can communicate.

This test will fail if the call could not be setup due to some error.

#### 3.1.1.4 *Trace Capture*

The SIP trace capture should be enabled to document test and diagnose any errors.

#### 3.1.1.5 *Known Issues*

None at this time.

### *3.1.2 Invalid Signed Call (Can't retrieve certificate)*

#### 3.1.2.1 *Purpose*

The purpose of this test is to validate that a SIP 436 response code is returned if referenced certificate can't be retrieved.

#### 3.1.2.2 *Test Setup*

Same as for a Valid Signed Call (see Section 3.1.1.2).

##### 3.1.2.2.1 Test Pre-conditions

Same as for a Valid Signed Call (see Section 3.1.1.2.1).

##### 3.1.2.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the INVITE message includes a URI that cannot be dereferenced (i.e., the "info" parameter or "x5u" claim in the SIP Identity header)
3. For testing purposes only, confirm a call failure action and that the destination test environment returns either the response with SIP status code 436 "Bad Identity-Info"

or response with SIP status code 200 OK and Reason header field with a value of 436 "Bad Identity-Info"

#### 3.1.2.3 *Observable Results*

##### 3.1.2.3.1 Message Flows

The associated message flow for this test will be a modification to Figure 3 and added to this section. This assumes that the optional use of the Reference Plane is not involved.

##### 3.1.2.3.2 Pass/Fail Criteria

The pass/fail criteria for this test is provided in Section 3.1.2.2.2 above.

#### 3.1.2.4 *Trace Capture*

The SIP trace capture should be enabled to document test and diagnose any errors.

#### 3.1.2.5 *Known Issues*

None at this time.

### *3.1.3 Invalid Signed Call (Can't validate certificate)*

#### 3.1.3.1 *Purpose*

The purpose of this test is to validate that a SIP 437 response code is returned if the referenced certificate can't be validated.

#### 3.1.3.2 *Test Setup*

Same as for a Valid Signed Call (see Section 3.1.1.2).

##### 3.1.3.2.1 Test Pre-conditions

Same as for a Valid Signed Call (see Section 3.1.1.2.1).

##### 3.1.3.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the INVITE message includes a URI where its referenced public certificate has any one of the following errors:
    - It is self-signed or untrusted
    - Signed by untrusted or unknown CA

- Expired
- Revoked

3. For testing purposes only, confirm a call failure action and that the destination test environment returns the SIP response code 437 “Unsupported Certificate”

#### 3.1.3.3 *Observable Results*

##### 3.1.3.3.1 Message Flows

The associated message flow for this test will be a modification to Figure 3 and will be added to this section. This assumes that the optional use of the Reference Plane is not involved.

##### 3.1.3.3.2 Pass/Fail Criteria

The pass/fail criteria for this test is provided in Section 3.1.3.2.2 above.

#### 3.1.3.4 *Trace Capture*

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.1.3.5 *Known Issues*

None at this time.

### *3.1.4 Invalid Signed Call (Valid certificate but for wrong TN)*

#### 3.1.4.1 *Purpose*

The purpose of this test is to validate that a SIP 438 response code is returned if there is a valid Identity header but certificate is for different TN.

#### 3.1.4.2 *Test Setup*

Same as for a Valid Signed Call (see Section 3.1.1.2).

##### 3.1.4.2.1 Test Pre-conditions

Same as for a Valid Signed Call (see Section 3.1.1.2.1).

#### 3.1.4.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the INVITE message includes a validly constructed Identity header but the signature value is invalid for destination TN, which in turn leads to a signature verification failure
3. For testing purposes only, confirm a call failure action and that the destination test environment returns either the response with SIP status code 438 "Invalid Identity Header" or response with SIP status code 200 OK and Reason header field with a value of 438 "Invalid Identity Header"

### 3.1.4.3 *Observable Results*

#### 3.1.4.3.1 Message Flows

The associated message flow for this test will be a modification to Figure 3 and added to this section. This assumes that the optional use of the Reference Plane is not involved.

#### 3.1.4.3.2 Pass/Fail Criteria

The pass/fail criteria for this test is provided in Section 3.1.4.2.2 above.

### 3.1.4.4 *Trace Capture*

The SIP trace capture should be enabled to document this test and diagnose any errors.

### 3.1.4.5 *Known Issues*

None at this time.

## *3.1.5 Unsigned Call (no Identity header)*

### 3.1.5.1 *Purpose*

The purpose of this test is to validate that the appropriate response code is returned if there is no Identity header in the SIP INVITE message when one is locally expected.

### 3.1.5.2 *Test Setup*

Same as for a Valid Signed Call (see Section 3.1.1.2).

#### 3.1.5.2.1 Test Pre-conditions

Same as for a Valid Signed Call (see Section 3.1.1.2.1).

#### 3.1.5.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant without an Identity header
2. For testing purposes only, confirm a call failure action and that the destination test environment returns either the response with SIP status code 428 "Use Identity Header" or response with SIP status code 200 OK and Reason header field with a value of 428 "Use Identity Header"

### 3.1.5.3 *Observable Results*

#### 3.1.5.3.1 Message Flows

The associated message flow for this test will be a modification to Figure 3 and added to this section. This assumes that the optional use of the Reference Plane is not involved.

#### 3.1.5.3.2 Pass/Fail Criteria

The pass/fail criteria for this test is provided in Section 3.1.5.2.2 above.

### 3.1.5.4 *Trace Capture*

The SIP trace capture should be enabled to document this test and diagnose any errors.

### 3.1.5.5 *Known Issues*

None at this time.

## *3.1.6 Date Freshness Test*

### 3.1.6.1 *Purpose*

Verify that if the date freshness test fails, a SIP error code of 403 is returned

#### 3.1.6.2 *Test Setup*

##### 3.1.6.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

##### 3.1.6.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the full form of PASSporT token exists in the Identity header field
4. Test to make sure that the 'iat' value falls within 60 seconds (configurable) from the current time
5. Verify that a 403 SIP error code is returned if the 'iat' value is older than 60 seconds from the current time

#### 3.1.6.3 *Observable Results*

3.1.6.3.1 Message Flows

3.1.6.3.2 Pass/Fail Criteria

This test passes if Steps 3, 4 and 5 of the Procedure are all verified.

#### 3.1.6.4 *Trace Capture*

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.1.6.5 *Known Issues*

None at this time.

## 3.2 Detailed Protocol Testing

### *3.2.1 Certificate Testing*

### *3.2.2 Identity Header Testing*

#### 3.2.2.1 *Valid PASSporT Token*

3.2.2.1.1 Purpose

Verify that a valid PASSporT token exists in the Identity header field

#### 3.2.2.1.2 Test Setup

Same as for a Valid Signed Call (see Section 3.1.1.2).

##### 3.2.2.1.2.1 Test Pre-conditions

Same as for a Valid Signed Call (see Section 3.1.1.2.1).

##### 3.2.2.1.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header included in the INVITE message includes the full form of the PASSporT token

#### 3.2.2.1.3 Observable Results

##### 3.2.2.1.3.1 Message Flows

##### 3.2.2.1.3.2 Pass/Fail Criteria

Pass criteria is to observe a valid PASSporT token in the Identity header field.

#### 3.2.2.1.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.2.2.1.5 Known Issues

None at this time.

### 3.2.2.2 *"ppt" Parameter*

#### 3.2.2.2.1 Purpose

Test to see if the SHAKEN "ppt" parameter exists in the Identity header.

#### 3.2.2.2.2 Test Setup

##### 3.2.2.2.2.1 Pre-conditions

Same as for a Valid Signed Call (see Section 3.1.1.2).

##### 3.2.2.2.2.2 Procedure

#### 3.2.2.2.3 Observable Results

##### 3.2.2.2.3.1 Message Flows

##### 3.2.2.2.3.2 Pass/Fail Criteria

The test passes if the "ppt=shaken" exists in the Identity header field.

#### 3.2.2.2.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.2.2.2.5 Known Issues

None at this time.

### 3.2.2.3 *"info" Parameter*

#### 3.2.2.3.1 Purpose

Verify that "info" parameter exists in the Identity Header field and its value is a valid URI

#### 3.2.2.3.2 Test Setup

##### 3.2.2.3.2.1 Test Pre-conditions

Same as for a Valid Signed Call (see Section 3.1.1.2).

##### 3.2.2.3.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header included in the INVITE message includes the 'info' parameter field

#### 3.2.2.3.3 Observable Results

##### 3.2.2.3.3.1 Message Flows

##### 3.2.2.3.3.2 Pass/Fail Criteria

1. 'info' parameter is present
2. The value of the 'info' parameter is a valid URI
3. The value of the 'info' parameter matches the 'x5u' attribute value in the PASSporT token

#### 3.2.2.3.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.2.2.3.5 Known Issues

None at this time.

### *3.2.3 PASSporT Object Testing*

#### 3.2.3.1 *"typ" attribute*

##### 3.2.3.1.1 Purpose

Verify that the "typ" attribute is set in the header section of the PASSporT object and it is set to the value "passport"

##### 3.2.3.1.2 Test Setup

###### 3.2.3.1.2.1 Test Pre-conditions

Same as for a Valid Signed Call (see Section 3.1.1.2)

###### 3.2.3.1.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the header section of the PASSporT object includes the "typ" attribute and that its value is set to "passport"

##### 3.2.3.1.3 Observable Results

###### 3.2.3.1.3.1 Message Flows

###### 3.2.3.1.3.2 Pass/Fail Criteria

This test passes if the value of the "typ" attribute is set to "passport".

##### 3.2.3.1.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

##### 3.2.3.1.5 Known Issues

None at this time.

#### 3.2.3.2 *"alg" attribute*

##### 3.2.3.2.1 Purpose

Verify that the "alg" attribute is set in the header section of the PASSporT object and that its value is set to "ES256"

##### 3.2.3.2.2 Test Setup

###### 3.2.3.2.2.1 Test Pre-conditions

Same as for a Valid Signed Call (see Section 3.1.1.2)

###### 3.2.3.2.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the header section of the PASSporT object includes the "alg" attribute and that its value is set to "ES256" or another acceptable value.

##### 3.2.3.2.3 Observable Results

###### 3.2.3.2.3.1 Message Flows

###### 3.2.3.2.3.2 Pass/Fail Criteria

This test passes,

1. If the value of the "alg" attribute is set to "ES256".
2. If "alg" is set to a valid value other than "ES256" (such as, "RS256"), an "alg" parameter MUST also be set in the Identity header field to match the "alg" attribute in the PASSporT object.

##### 3.2.3.2.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

##### 3.2.3.2.5 Known Issues

None at this time.

#### 3.2.3.3 *"x5u" attribute*

##### 3.2.3.3.1 Purpose

Verify that the "x5u" attribute exists in the header section of the PASSporT object and that it is set to a valid URI

##### 3.2.3.3.2 Test Setup

###### 3.2.3.3.2.1 Test Pre-conditions

Same as for a Valid Signed Call (see Section 3.1.1.2)

###### 3.2.3.3.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the header section of the PASSporT object includes the "x5u" attribute and that its value is set to a valid URI.

##### 3.2.3.3.3 Observable Results

###### 3.2.3.3.3.1 Message Flows

###### 3.2.3.3.3.2 Pass/Fail Criteria

This test passes,

1. If the value of the "x5u" attribute is set to a valid URI.
2. If the value of the "x5u" matches that of the "info" parameter of the Identity header field
3. Also, when the URI is resolved, it should point to a valid X.509 certificate

##### 3.2.3.3.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

##### 3.2.3.3.5 Known Issues

None at this time.

#### 3.2.3.4 *"iat" Attribute*

##### 3.2.3.4.1 Purpose

Verify that "iat" attribute exists in the claim section of the PASSporT object

##### 3.2.3.4.2 Test Setup

###### 3.2.3.4.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

###### 3.2.3.4.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the claim section of the PASSporT object includes the "iat" attribute and that its value is set to the current Unix epoch time.
4. Also, verify that the value type of "iat" is Numeric

##### 3.2.3.4.3 Observable Results

###### 3.2.3.4.3.1 Message Flows

###### 3.2.3.4.3.2 Pass/Fail Criteria

This test passes,

1. If the value of the "iat" attribute is set to a valid Unix epoch time.
2. If the value type of "iat" is Numeric

##### 3.2.3.4.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

##### 3.2.3.4.5 Known Issues

None at this time.

#### 3.2.3.5 *"orig" Attribute*

##### 3.2.3.5.1 Purpose

Verify that "orig" attribute exists in the claim section of the PASSporT object and that it contains a TN.

##### 3.2.3.5.2 Test Setup

###### 3.2.3.5.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

###### 3.2.3.5.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the INVITE message includes the Identity header
3. Verify that the Identity header field contains the full form of the PASSporT token
4. Verify that the claim section of the PASSporT object includes the "orig" attribute and that it contains the "tn" attribute.
5. Verify that the value of the "tn" should agree with section 8 of RFC 4474bis.

##### 3.2.3.5.3 Observable Results

###### 3.2.3.5.3.1 Message Flows

###### 3.2.3.5.3.2 Pass/Fail Criteria

This test passes if Steps 3, 4 and 5 of the Procedure are all verified.

##### 3.2.3.5.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

##### 3.2.3.5.5 Known Issues

None at this time.

#### 3.2.3.6 *"dest" Attribute*

##### 3.2.3.6.1 Purpose

Verify that "dest" attribute exists in the claim section of the PASSporT object and that it contains a TN

#### 3.2.3.6.2 Test Setup

##### 3.2.3.6.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

##### 3.2.3.6.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the INVITE message includes the Identity header
3. Verify that the Identity header field contains the full form of the PASSporT token
4. Verify that the claim section of the PASSporT object includes the "dest" attribute and that it contains at least one "tn" attribute.
5. Verify that the value of the "tn" agrees with section 8 of RFC 4474bis.

#### 3.2.3.6.3 Observable Results

##### 3.2.3.6.3.1 Message Flows

##### 3.2.3.6.3.2 Pass/Fail Criteria

This test passes if Steps 3, 4 and 5 of the Procedure are all verified

#### 3.2.3.6.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.2.3.6.5 Known Issues

None at this time.

### 3.2.3.7 *"attest" Attribute*

#### 3.2.3.7.1 Purpose

Verify that "attest" attribute exists in the claim section of the PASSporT object

#### 3.2.3.7.2 Test Setup

##### 3.2.3.7.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

##### 3.2.3.7.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the Identity header includes the full form of the PASSporT token
4. Verify that the claim section of the PASSporT object includes the "attest" attribute and that its value is set to one of the following values: "A", "B", or "C"

3.2.3.7.3 Observable Results

3.2.3.7.3.1 Message Flows

3.2.3.7.3.2 Pass/Fail Criteria

This test passes if Steps 3 and 4 of the Procedure are all verified.

3.2.3.7.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

3.2.3.7.5 Known Issues

None at this time.

### 3.2.3.8 *"origid" Attribute*

3.2.3.8.1 Purpose

Verify that "origid" attribute exists in the claim section of the PASSporT object

3.2.3.8.2 Test Setup

3.2.3.8.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

3.2.3.8.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the Identity header field includes the full form of the PASSporT token

4. Verify that the claim section of the PASSporT object includes the "origid" attribute and that its value is set to a valid UUID

#### 3.2.3.8.3 Observable Results

##### 3.2.3.8.3.1 Message Flows

##### 3.2.3.8.3.2 Pass/Fail Criteria

This test passes if Steps 3 and 4 of the Procedure are all verified.

#### 3.2.3.8.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.2.3.8.5 Known Issues

None at this time.

## 3.3 STI Authentication Service Testing

### *3.3.1 AS Functional Testing*

#### 3.3.1.1 *PAI as Secure Telephone Identity*

##### 3.3.1.1.1 Purpose

Verify that PAI header with a TN user part is given precedence over the From header

##### 3.3.1.1.2 Test Setup

###### 3.3.1.1.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

###### 3.3.1.1.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the INVITE message also contains the PAI header
4. Verify that the user part of the URI in the PAI is a TN
5. Verify that the "tn" attribute within the "orig" attribute in the claim section of the Identity header reflects the TN in the PAI header

#### 3.3.1.1.3 Observable Results

##### 3.3.1.1.3.1 Message Flows

##### 3.3.1.1.3.2 Pass/Fail Criteria

This test passes if Steps 3, 4 and 5 of the Procedure are all verified.

#### 3.3.1.1.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.3.1.1.5 Known Issues

None at this time.

### 3.3.1.2 *TN in the SIP URI*

#### 3.3.1.2.1 Purpose

Verify that E.164 TN in the From header SIP URI is used as STI when PAI is absent

#### 3.3.1.2.2 Test Setup

##### 3.3.1.2.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

##### 3.3.1.2.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is included in the INVITE message
3. Verify that the “tn” attribute within the “orig” attribute in the claim section of the Identity header reflects the TN from the SIP URI of the From header

#### 3.3.1.2.3 Observable Results

##### 3.3.1.2.3.1 Message Flows

##### 3.3.1.2.3.2 Pass/Fail Criteria

This test passes if Step 3 of the Procedure is verified.

#### 3.3.1.2.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.3.1.2.5 Known Issues

None at this time.

### 3.3.1.3 *TN in the TEL URI*

#### 3.3.1.3.1 Purpose

Verify that E.164 TN in the From header TEL URI is used as STI if PAI is absent

#### 3.3.1.3.2 Test Setup

##### 3.3.1.3.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

##### 3.3.1.3.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is included in the INVITE message
3. Verify that the "tn" attribute within the "orig" attribute in the claim section of the Identity header reflects the TN from the TEL URI in the From header

#### 3.3.1.3.3 Observable Results

##### 3.3.1.3.3.1 Message Flows

##### 3.3.1.3.3.2 Pass/Fail Criteria

This test passes if the Step 3 of the Procedure is verified.

#### 3.3.1.3.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.3.1.3.5 Known Issues

None at this time.

## 3.4 STI Verification Service Testing

### *3.4.1 VS Functional Testing*

#### 3.4.1.1 *Success with Valid Certificate*

##### 3.4.1.1.1 Purpose

Verify that PASSporT token validation succeeds with a valid certificate that is not expired and that is not in a CRL

##### 3.4.1.1.2 Test Setup

###### 3.4.1.1.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

###### 3.4.1.1.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the full form of PASSporT token exists in the Identity header field
4. Verify that "x5u" and "info" parameters refer to the same certificate
5. Verify that the certificate expiry date is in the future
6. Verify that the certificate CRL check passes
7. Verify that the PASSporT token signature is digitally verified

##### 3.4.1.1.3 Observable Results

###### 3.4.1.1.3.1 Message Flows

###### 3.4.1.1.3.2 Pass/Fail Criteria

This test passes if Steps 3 through 7 of the Procedure are all verified.

##### 3.4.1.1.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

##### 3.4.1.1.5 Known Issues

None at this time.

#### 3.4.1.2 *Failure with Expired Certificate*

##### 3.4.1.2.1 Purpose

Verify that PASSporT token validation results in a failure due to expired certificate

##### 3.4.1.2.2 Test Setup

###### 3.4.1.2.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

###### 3.4.1.2.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the full form of PASSporT token exists in the Identity header field
4. Verify that "x5u" and "info" parameters refer to the same certificate
5. Verify that the certificate expiry date is in the past, which results in validation failure

##### 3.4.1.2.3 Observable Results

###### 3.4.1.2.3.1 Message Flows

###### 3.4.1.2.3.2 Pass/Fail Criteria

This test passes if Steps 3, 4 and 5 of the Procedure are all verified.

##### 3.4.1.2.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

##### 3.4.1.2.5 Known Issues

None at this time.

#### 3.4.1.3 *Failure due to Certificate Revocation List Check*

##### 3.4.1.3.1 Purpose

Verify that PASSporT token validation fails due to the certificate being revoked

#### 3.4.1.3.2 Test Setup

##### 3.4.1.3.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

##### 3.4.1.3.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the full form of PASSporT token exists in the Identity header field
4. Verify that the certificate revocation list check is performed and that the result shows that the certificate has been revoked
5. Verify that an Identity header failure error has been returned

#### 3.4.1.3.3 Observable Results

##### 3.4.1.3.3.1 Message Flows

##### 3.4.1.3.3.2 Pass/Fail Criteria

This test passes if Steps 3, 4 and 5 of the Procedure are all verified.

#### 3.4.1.3.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.4.1.3.5 Known Issues

None at this time.

### 3.4.1.4 *Date Freshness Test*

#### 3.4.1.4.1 Purpose

Verify that if the date freshness test fails, a SIP error code of 403 is returned

#### 3.4.1.4.2 Test Setup

##### 3.4.1.4.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

#### 3.4.1.4.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the full form of PASSporT token exists in the Identity header field
4. Verify that the 'iat' value falls within 60 seconds (configurable) from the current time
5. Verify that a 403 SIP error code is returned if the 'iat' value is older than 60 seconds from the current time

### 3.4.1.4.3 Observable Results

#### 3.4.1.4.3.1 Message Flows

#### 3.4.1.4.3.2 Pass/Fail Criteria

This test passes if Steps 3, 4 and 5 of the Procedure are all verified.

### 3.4.1.4.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

### 3.4.1.4.5 Known Issues

None at this time.

## 3.4.1.5 *Success on Missing Identity header*

### 3.4.1.5.1 Purpose

Verify that a 428 'Use Identity header' error is not returned if the Identity header is not present in the INVITE message

### 3.4.1.5.2 Test Setup

#### 3.4.1.5.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

#### 3.4.1.5.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant

2. Inspect the SIP trace to confirm that the Identity header is not present in the INVITE message
3. Per SHAKEN, verify that the call is established successfully and that SIP status code 428 is not raised

3.4.1.5.3 Observable Results

3.4.1.5.3.1 Message Flows

3.4.1.5.3.2 Pass/Fail Criteria

This test passes if Step 3 of the Procedure is verified.

3.4.1.5.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

3.4.1.5.5 Known Issues

None at this time.

3.4.1.6 *Success with Valid Certificate*

3.4.1.6.1 Purpose

Verify that PASSporT token validation succeeds with a valid certificate that is not expired and that is not on a CRL

3.4.1.6.2 Test Setup

3.4.1.6.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

3.4.1.6.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the full form of PASSporT token exists in the Identity header field
4. Verify that “x5u” and “info” parameters refer to the same certificate
5. Verify that the certificate expiry date is in the future
6. Verify that the CRL check is completed and passes

7. Verify that the PASSporT token signature is digitally verified

#### 3.4.1.6.3 Observable Results

##### 3.4.1.6.3.1 Message Flows

##### 3.4.1.6.3.2 Pass/Fail Criteria

This test passes if Steps 3 through 7 of the Procedure are all verified.

#### 3.4.1.6.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.4.1.6.5 Known Issues

None at this time.

### 3.4.1.7 *Failure on Certificate Fetch Error*

#### 3.4.1.7.1 Purpose

SIP error 437 'Unsupported Credential' should be returned if there is a failure in retrieving the certificate as referenced by the 'info' parameter

#### 3.4.1.7.2 Test Setup

##### 3.4.1.7.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

##### 3.4.1.7.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the full form of PASSporT token exists in the Identity header field
4. Verify that "x5u" and "info" parameters refer to the same URI
5. Verify that SIP error 437 is returned when the "info" URL doesn't yield a certificate

#### 3.4.1.7.3 Observable Results

##### 3.4.1.7.3.1 Message Flows

#### 3.4.1.7.3.2 Pass/Fail Criteria

This test passes if Steps 3, 4 and 5 of the Procedure are all verified.

#### 3.4.1.7.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.4.1.7.5 Known Issues

None at this time.

### 3.4.1.8 *Failure on Signature Verification Error*

#### 3.4.1.8.1 Purpose

SIP error 438 'Invalid Identity Header' should be returned if signature verification fails

#### 3.4.1.8.2 Test Setup

##### 3.4.1.8.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

##### 3.4.1.8.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the full form of PASSporT token exists in the Identity header field
4. Verify that SIP error 438 is returned in case of signature verification failure

#### 3.4.1.8.3 Observable Results

##### 3.4.1.8.3.1 Message Flows

##### 3.4.1.8.3.2 Pass/Fail Criteria

This test passes if Steps 3 and 4 of the Procedure are all verified.

#### 3.4.1.8.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.4.1.8.5 Known Issues

None at this time.

### 3.4.1.9 *Use of PAI as STI*

#### 3.4.1.9.1 Purpose

Verify that if PAI is present, it is given precedence as STI over the From header

#### 3.4.1.9.2 Test Setup

##### 3.4.1.9.2.1 Test Pre-condition

Same as for a Valid Signed Call (see Section 3.1.1.2)

##### 3.4.1.9.2.2 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header is present in the INVITE message
3. Verify that the full form of PASSporT token exists in the Identity header field
4. Verify that PAI header exists and that its user part qualifies as a TN
5. Verify that PAI header is used as STI for signature verification and the call is established successfully

#### 3.4.1.9.3 Observable Results

##### 3.4.1.9.3.1 Message Flows

##### 3.4.1.9.3.2 Pass/Fail Criteria

This test passes if Steps 3, 4 and 5 of the Procedure are all verified.

#### 3.4.1.9.4 Trace Capture

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.4.1.9.5 Known Issues

None at this time.

## 3.5 Interface Testing

### *3.5.1 Private Key Access*

Private Key access is performed by the STI Authentication Service (STI-AS) and thus will utilize the preferred key storage mechanism of the AS platform, which may be via the operating system of the call-processing component or a Hardware-Signing-Module if available on the platform.

Details will be worked out as platforms used for testing via the testbed are announced.

### *3.5.2 CSCF-CSCF Interworking*

(To be supplied)

### *3.5.3 Certificate Retrieval*

#### 3.5.3.1 *Purpose*

The purpose of these tests is to validate the interface to a Certificate Authority (or TN-CR). For these tests, the bearer protocol is http / https. This interface supports certificate retrieval and additional validation of certificates through Open Certificate Status Protocol (OCSP) and Certificate Revocation Lists (CRL). Optionally, an authoritative TN Reference Plane can be used to mitigate against "fake" CAs not being authoritative for TN certificates.

#### 3.5.3.2 *Test Setup*

1. The CA is reachable through http / https, preferably on the public Internet
2. A test computer runs scripts to handle certificate-retrieval, OCSP-responses, CRLs, and (optionally) Reference Plane queries. This can be a server with terminal access or any appropriate system with network access (e.g., a Unix machine with openssh and a web-server installed).
3. Test scripts are used to fetch and verify CA and Reference-Plane objects.
4. Root certificates of Test CA(s) in use will be installed and retrievable.

##### 3.5.3.2.1 Test Pre-conditions

The test machine is connected to the network and can reach the CA (and optionally Reference Plane) used in the tests.

Certificates used for testing include a set of domain-level certificates (e.g., company.com), a set of telephone number (TN) certificates, TN-CR intermediate certificates (if any), and CA-Root certificates. Certain certificates are constructed to be valid, invalid, or have valid or invalid signing certificates from CAs.

For TN certificates, below is a list of respective certificates with attributes for various tests. The TN-CR will be provisioned with a minimum set of test numbers, possibly of the form +1-NXX-555-01XX, and associated certificates with various properties. Private keys may be distributed between test participants.

1. TN-01: Phone number with valid certificate and chain
2. TN-02: Phone number with expired certificate
3. TN-03: Phone number with expired signing certificate
4. TN-04: Phone number with expired root certificate
5. TN-05: Phone number with revoked certificate
6. TN-06: Phone number with revoked signing certificate
7. TN-07: Phone number with revoked root certificate
8. TN-08: Phone number without entry in the TN-CR
9. TN-09: Phone number without entry in the Reference Plane ("fake" CA)

Note that these Test TNs and Test URIs may be used in setting up configurations for certain End-to End-Functional Tests as described in Section 3.1. The following table contains some ideas for using selected TNs and URIs to generate certain results.

| Test # | Test Title | Test Purpose | Comments/Suggestions |
|---|---|---|---|
| 3.1.1 | Valid Signed Call | Successful end-to-end signed call | TN-01 and URI-01 (link to valid certificate) |
| 3.1.2 | Invalid Signed Call (Response Code 436) | 'Bad Identity info' | TN-01 and URI-08 (link has no associated certificate) |
| 3.1.3 | Invalid Signed Call (Response Code 437) | 'Unsupported Credential' | TN-02 and URI-02 (link to expired certificate) |
| 3.1.4 | Invalid Signed Call (Response Code 438) | 'Invalid Identity Header' | Any valid TN other than TN-01 and URI-01 (“wrong” public key) |
| 3.1.5 | Unsigned Call (Response Code 428) | 'Use Identity Header' | TN-08 (no URI) |

3.5.3.2.2 Procedure *(note: these remaining sub-sections through 3.5.3.5 will be updated)*

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant
2. Inspect the SIP trace to confirm that the Identity header included in the INVITE message includes the full form of the PASSporT token
3. Confirm that the call is established and both the calling party and the called party can communicate with each other

3.5.3.2.3 Procedure

Test participants will repeat the following steps:

1. Initiate the call to the destination TN of the test participant without an Identity header
2. For testing purposes only, confirm a call failure action and that the destination test environment returns the SIP response code 428 “Use Identity Header”

#### 3.5.3.3 *Observable Results*

##### 3.5.3.3.1 Message Flows

The associated message flow for this test will be a modification to Figure 3 and added to this section. This assumes that the optional use of the Reference Plane is not involved.

##### 3.5.3.3.2 Pass/Fail Criteria

The pass/fail criteria for this test is provided in Section 3.5.3.2.2 above.

#### 3.5.3.4 *Trace Capture*

The SIP trace capture should be enabled to document this test and diagnose any errors.

#### 3.5.3.5 *Known Issues*

None at this time.