

Deployment of STIR/SHAKEN

by

Small Voice Service Providers

NANC Call Authentication Trust Anchor Working Group

Table of Contents

1. Introduction	3
2. Report	4
2.1. Barriers preventing implementation of STIR/SHAKEN	4
2.2. Technical solutions	6
2.2.1. Hosted SHAKEN	7
2.2.2. Carrier SHAKEN	7
2.2.3. SHAKEN Software	8
2.2.4. SHAKEN for TDM interconnected service providers	9
2.3. Methods to encourage and promote technical solutions	10
2.3.1. Short-term solutions for call authentication	10
2.3.2. Overcoming challenges to VoIP connectivity	11
2.3.3. Overcoming challenges to VoIP destination routing	13
2.4. Next Steps	14
3. Conclusion	16
4. Glossary.....	17

Deployment of STIR/SHAKEN by Small Voice Service Providers

1. Introduction

Fighting illegal robocalls is a top consumer protection priority for the Federal Communications Commission (FCC), and call authentication is an important part of solving this critical challenge. With the passage of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, Congress expressed its support for a robust call authentication system.¹

The FCC's Wireline Competition Bureau has called upon the North American Numbering Council's (NANC) Call Authentication Trust Anchor (CATA) Working Group (WG), to report on several topics surrounding the deployment of STIR/SHAKEN by small voice service providers. These topics include:

1. Identify barriers that prevent small voice service providers from implementing the STIR/SHAKEN framework.
2. Identify technological solutions available to small voice service providers that will promote their deployment of STIR/SHAKEN.
3. Identify methods to encourage and promote technical solutions to the challenges of STIR/SHAKEN deployment by small voice service providers.
4. Recommend steps that the Secure Telephone Identity Governance Authority (STI-GA) or the rest of the industry (including major voice service providers, vendors, and equipment manufacturers) can take to advance STIR/SHAKEN deployment by small voice service providers.
5. Recommend steps that the Commission can take to encourage deployment of STIR/SHAKEN by small voice providers.

While implementing STIR/SHAKEN may cause justifiable challenges for certain service providers, it is clear that non-ubiquitous deployment of STIR/SHAKEN negatively impacts the broader service provider ecosystem. Customers of both large and small service providers exchange traffic with each other on the PSTN. However, calls from small originating service providers that have not implemented STIR/SHAKEN will not display calls as "verified" on the terminating end irrespective of the size of the terminating provider (even where the terminating provider has implemented STIR/SHAKEN). Likewise, calls originating from large providers who have implemented STIR/SHAKEN will not display as "verified" on the terminating end of a call to a small service provider if that provider has not implemented STIR/SHAKEN. Analytics that use call authentication as an input to their algorithms may

¹ Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, S. 151, 116th Cong., § 4(b)(l) (2019) (TRACED Act).

also be hampered. As a result, service providers of all sizes have a vested interest in resolving the issues raised in the CATA WG charge.

2. Report

In general, there are no significant barriers which prevent universal STIR/SHAKEN implementation for interconnected and non-interconnected VoIP providers (regardless of size). That is not the case for certain small competitive local exchange carriers (CLECs) and incumbent local exchange carriers (ILECs), where IP tandem SIP interconnects and SHAKEN solutions universally available to VoIP providers are not economically feasible. While the industry is currently developing non-IP call authentication solutions which may provide effective alternatives for these small CLECs and ILECs, as it now stands the TRACED Act provides limited protection for subscribers of these providers. Rural rate-of-return regulated incumbent local exchange carriers (RLECs) encounter similar difficulties—current solutions can be uneconomic, require distant interconnection points beyond the RLEC service territory, and raise service quality concerns. These issues are discussed in Section 2.1.

There are various technical solutions available, both in-network or from third-party commercially hosted call signing service solutions, for promoting STIR/SHAKEN deployment. Because there are robust SHAKEN solutions for VoIP-connected networks, this report provides several categories of solutions, including hosted, carrier, and software-based SHAKEN solutions. There are more limited options for time-division multiplexing (TDM) interconnected service providers. ATIS has recently published two standards which provide network designers with more flexibility to deploy system-specific solutions, and ATIS is currently improving these standards which should provide additional opportunities for TDM interconnected service providers. These solutions are provided in Section 2.2.

Beyond these technical solutions, Section 2.3 provides methods to encourage and promote their deployment and includes further discussion on two obstacles (VoIP connectivity and VoIP destination routing) which need to be addressed.

Section 2.4 provides several next steps, including developing an STI-CPS governance structure and an aspirational recommendation for the industry to address end-to-end SIP interconnection to enable ubiquitous STIR/SHAKEN adoption, subject to further Commission involvement if industry efforts do not materialize.

These issues are discussed below.

2.1. Barriers preventing implementation of STIR/SHAKEN

The second order implementing the TRACED Act broadly expands the term service provider² to apply SHAKEN call authentication requirements to interconnected VoIP providers and non-interconnected

² *In re Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, ¶ 19 (Oct. 1, 2020) (“voice service” is defined as a service “that is interconnected with the public switched telephone network and that furnishes voice communications to an end user”).

VoIP providers.³ The barriers to implementing SHAKEN and the availability of solutions for interconnected and non-interconnected VoIP providers, small and large alike, are generally different from the barriers and solutions for certain small CLECs and ILECs. Where these small providers serve rural footprints, the barriers can be exacerbated. For this reason, the issues for these two distinct groups of small service providers will be considered separately.

Interconnected and non-interconnected VoIP providers, or VoIP providers generally, are SIP connected networks. These service providers should have no significant barriers preventing the implementation of SHAKEN, irrespective of size. The market for SHAKEN solutions is robust and competitive and Section 2.2 discusses the general options available for any providers in this category. Even if VoIP providers implement SHAKEN/STIR within their network, VoIP providers that opt to obtain their own numbering resources for the purpose of provisioning voice service are required to access the public switched telephone network (PSTN) using a 3rd party carrier partner or interconnect through a commercial arrangement or tariffed offering.⁴ Although some of these interconnections are SIP, interconnections between the 3rd party provider and local LECs could be TDM, which could result in authentication headers being lost in transit to the terminating carrier.

In contrast, the barriers to implementing SHAKEN can be quite different, and the available solutions limited, for small CLECs and ILECs (particularly in rural areas). Some rural service providers operate networks that largely rely on legacy TDM tandems to generally receive inbound and send outbound intercarrier calls. These rural service providers also typically provide some portion of the transport to access these legacy TDM tandems. Although alternatives may exist, in some cases TDM interfaces may be the only available option for these service providers to interconnect with legacy TDM tandems. IP tandem SIP interconnects and the SHAKEN solutions available to small interconnected, and non-interconnected, VoIP providers may not be an economic option for some small rural CLECs and rural ILECs. Without economic access to SIP interconnection, the subscribers of such providers may have limited benefit from the TRACED Act. However, new standards for non-IP call authentication offer techniques that may provide alternatives for small CLECs and ILECs to join the SHAKEN trust network using their existing TDM interconnects.

Rural rate-of-return RLECs have similar concerns, that a barrier to effective implementation of STIR/SHAKEN is that IP interconnection is either not available or is not an economically viable option.⁵ According to NTCA-The Rural Broadband Association, a trade association representing approximately 850 RLECs with 4,500 voice telephony subscribers on average,⁶ a 2019 member survey indicated that 93% of respondents operate IP switching facilities (meaning they have the ability to generate call

³ 47 U.S.C. § 153(36) (“non-interconnected VoIP service” is defined as services that “enables real-time voice communications that originate from or terminate to the user’s location using Internet protocol or any successor protocol; and requires internet protocol compatible customer premises equipment; and does not include any service that is an interconnected VoIP service.”).

⁴ *In re Numbering Policies for Modern Communications*, WC Docket No. 13-97, Report and Order, 30 FCC Rcd 6839, at 6856, ¶ 37 (Jun. 18, 2015).

⁵ *In re Call Authentication Trust Anchor*, WC Docket No. 17-97, Comments of NTCA – The Rural Broadband Association (fil. May 15, 2020).

⁶ NTCA-The Rural Broadband Association, Broadband/Internet Availability Survey Report (Dec. 2020), p. 3 (available at: <https://www.ntca.org/sites/default/files/documents/2020-12/2020BroadbandSurveyReport.pdf>).

authentication data in their own networks).⁷ However, many RLECs' voice traffic is often routed over TDM tandems operated by other carriers. As a result, with the use of existing facilities, STIR/SHAKEN call authentication to or from these voice providers will not be passed for the vast majority of voice calls without obtaining IP interconnection with an IP capable network. Therefore, their implementation of the STIR/SHAKEN standard would be ineffective in protecting consumers.⁸

Additionally, IP capable network interconnection may often be located at distant points outside of the rural ILECs' service territory. With respect to the concern that IP interconnection alternatives are not economically viable, rural and other small service providers are concerned that they could end up bearing additional costs of interconnecting at distant points from their service area, with the assumption of transport costs that they do not bear today. Additional alternatives may rely upon the use of Over-the-Top (OTT) (i.e., "public Internet") routing of voice calls, and these options create the additional concern of service quality for voice service. From the larger service provider perspective interconnecting in IP and TDM are vastly different, and it would be inefficient to replicate TDM interconnection methods in IP. For example, unlike TDM interconnection, traffic exchanged over IP interconnection arrangements are not limited by geographic boundaries and do not necessarily require multiple providers to reach the interconnecting network's customers who may be located anywhere.

2.2. Technical solutions

A technical option available to small service providers to authenticate their SIP traffic using the STIR/SHAKEN standard is to leverage the number of vendor solutions offering both in-network or commercially hosted call signing service solutions.

Beyond typical in-network solutions, an increasingly popular approach are platform-as-a-service (PaaS) cloud solutions, where service providers can avoid complicated and costly STIR/SHAKEN implementations on their networks by sending their traffic to a vendor that provides access to a STIR/SHAKEN solution on the vendor's network, or through cloud computing services. These third-party hosted solutions provide simplified policy management which supports complex and customizable call handling policies.

The following sections provide a general classification of these available SHAKEN solutions for service providers with VoIP connected networks, and can be divided into three groups, 1) Hosted SHAKEN, 2) Carrier SHAKEN, and 3) SHAKEN Software. Beyond that, for TDM connected providers there are a number of recently standardized solutions that are described. Additionally, other services that are similarly available that add to the effectiveness of STIR/SHAKEN and robocall mitigation are described.

⁷ NTCA-The Rural Broadband Association, Broadband/Internet Availability Survey Report (Dec. 2019), p. 9 (available at: <https://www.ntca.org/sites/default/files/documents/2019-12/2019%20Broadband%20Survey%20Report.pdf>).

⁸ This does not reflect recent work to develop Non-IP Call Authentication alternatives. These Non-IP Call Authentication alternatives are discussed later in this document.

2.2.1. Hosted SHAKEN

Hosted SHAKEN describes a turn-key SHAKEN authentication and verification solution offered in a public or private cloud that includes all the required SHAKEN components for offering a comprehensive standards-compliant solution, i.e., STI-AS, STI-KMS, SKS, STI-CA, STI-CR, STI-VS. These services can conveniently offer other value-added features beyond the core STIR/SHAKEN specified requirements such as call analytics, call treatment, call blocking or diversion along with other consumer enabling features. An OSP has flexible options to integrate their voice infrastructure with a host SHAKEN service using either HTTP or SIP protocols. Hosted SHAKEN services, as defined in this document, do not provide SIP origination or termination services.

The following call-flow diagram illustrates a basic example of how an OSP might integrate with a hosted SHAKEN service using SIP.⁹ The small service provider, acting as the OSP, performs the Telephone Number (TN) Validation by confirming the End-User's right-to-use the telephone number, which determines the proper "A," "B," or "C" level attestation. The OSP then sends a SIP INVITE to the hosted SHAKEN service. The hosted SHAKEN service signs the call using the certificate of the OSP and returns a SIP 302 response that includes the SHAKEN Identity header. The OSP copies the SHAKEN Identity header from the SIP 302 message into the outbound SIP INVITE sent to the call destination. A similar STIR/SHAKEN verification occurs with the TSP. These types of third-party hosted STIR/SHAKEN services are compliant with the latest STIR/SHAKEN standards.

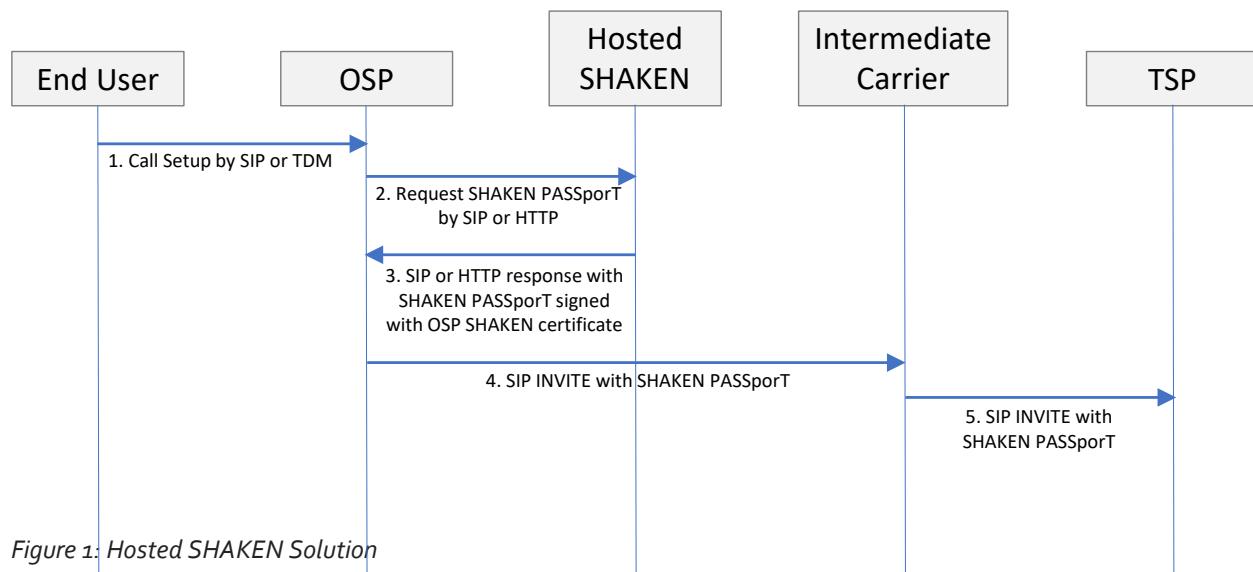


Figure 1: Hosted SHAKEN Solution

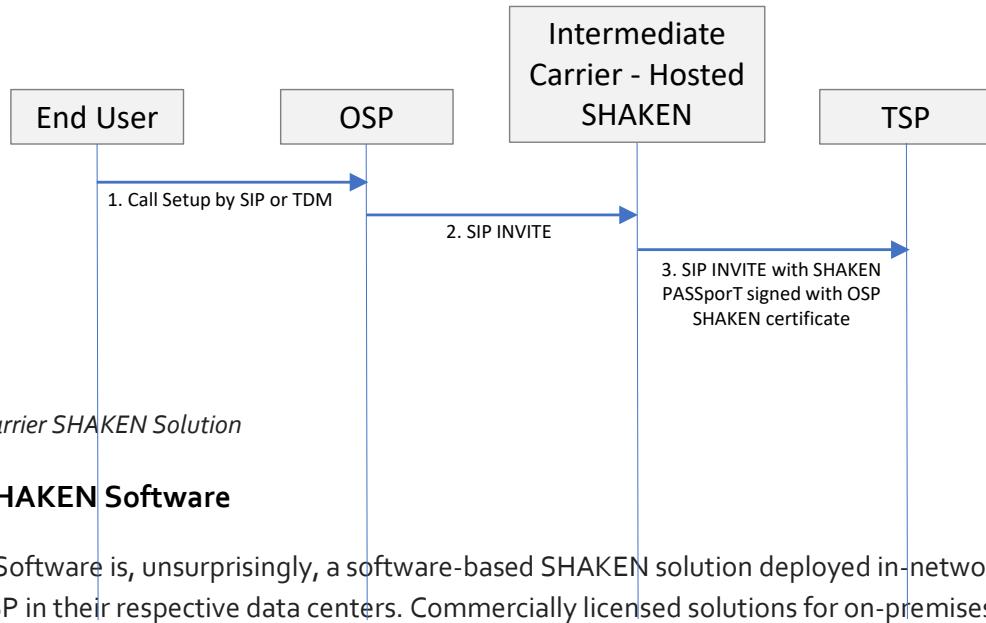
2.2.2. Carrier SHAKEN

Carrier SHAKEN describes another category of turn-key SHAKEN services offered by a growing number of Direct Inward Dialing (DID) or wholesale providers that also provide SIP termination to the PSTN.

⁹ Note, a similar interaction occurs at the TSP for STIR/SHAKEN verification.

This service combines SHAKEN authentication service with SIP termination to the PSTN (transit service).

The following diagram illustrates carrier hosted SHAKEN services.¹⁰ The call is signed by the intermediate provider using the certificate of the OSP. In this use case, the attestation level for each calling number is determined by the OSP. This implementation requires additional effort by the OSP whom must obtain a Service Provider Code (SPC) token from the STI-PA. However, this implementation benefits the real time robocall detection of TSPs who can identify the OSP from the SHAKEN certificate.



2.2.3. SHAKEN Software

SHAKEN Software is, unsurprisingly, a software-based SHAKEN solution deployed in-network by the OSP or TSP in their respective data centers. Commercially licensed solutions for on-premises software are available in the market, however these solutions have generally become less popular than vendors simply offering hosted and directly supported SHAKEN services, or through carrier SHAKEN solutions. However, opensource SHAKEN solutions are growing more important. Two notable examples of SIP proxy projects that support SHAKEN are OpenSIPS, which first published its SHAKEN module in 2019, and Kamailio, which released its SHAKEN module in 2021. Both open source SHAKEN solutions are being used widely in production and lower the cost of entry for the growing number of service providers that utilize open source solutions.

The table below provides a list of several available SHAKEN solution options.

SHAKEN Solution	Hosted SHAKEN	Carrier SHAKEN	SHAKEN Software
1callconnect.com/products/stir-shaken/		X	
bulkvs.com/stir-shaken-service	X		
connexcs.com	X		

¹⁰ Note, a similar interaction occurs at the TSP for STIR/SHAKEN verification.

SHAKEN Solution	Hosted SHAKEN	Carrier SHAKEN	SHAKEN Software
gbsdtech.com/wpweb/	X		X
home.neustar/trusted-call-solutions/certified-caller	X		
inteliquent.com/services/voice/stir-shaken		X	
kamailio.org/w/2021/03/new-module-stirshaken/			X
netnumber.com/services/guaranteed-caller/	X		
opensips.org/html/docs/modules-devel/stir_shaken.html			X
prescott-martini.com/stir-shaken		X	
ribboncommunications.com/solutions/service-provider-solutions/stirshaken	X		
sansay.com/solutions/stir-shaken/	X		
tnsi.com/product/call-guardian-authentication-hub	X	X	
transnexus.com/shaken/	X		X
www.peeringhub.io/stir-shanken.html	X		X

Figure 3: Software-based SHAKEN solutions

2.2.4. SHAKEN for TDM interconnected service providers

In May 2020, a new ATIS task force was formed to define call authentication solutions for non-IP networks. The Non-IP Call Authentication (NIPCA) Task Force was formed as a sub-working group of the Packet Technologies and System Committee. The NIPCA Task Force developed two different standards for call authentication by non-IP networks, ATIS standard 1000095¹¹ and 1000096.¹² These two standards provide network designers the flexibility to select the best technique for specific use cases, are not mutually exclusive, and may be used together in a single network. Neither standard impacts service providers with IP-only interconnects.

ATIS-1000095, Extending STIR/SHAKEN over TDM, defines how the SHAKEN attestation level can be transmitted over TDM signaling. The ISUP screening indicator parameter can be used to pass the

¹¹ ATIS-1000095 – Extending STIR/SHAKEN over TDM (available at: https://access.atis.org/apps/group_public/download.php/60331/ATIS-1000095.pdf).

¹² ATIS-1000096 – Signature-based Handling of Asserted information using toKENs (SHAKEN): Out-of-Band PASSport Transmission Involving TDM Networks (available at: https://access.atis.org/apps/group_public/download.php/60535/ATIS-1000096.pdf).

ATIS-1000097 Technical Report on Alternatives for Call Authentication for Non-IP Traffic was published concurrently with ATIS-1000095 and ATIS-1000096, which evaluates these approaches including scope, network impact, security considerations and dependencies (available at: https://access.atis.org/apps/group_public/download.php/60536/ATIS-1000097.pdf).

SHAKEN attestation level over TDM signaling or, alternatively, separate TDM trunk groups can be used for each SHAKEN attestation level. Before a call is converted from SIP to TDM, the ISUP screening indicator parameter is set based on the SHAKEN attestation level. When a call is converted from TDM back to SIP, a SHAKEN PASSporT is constructed with the SHAKEN attestation level received in the ISUP screening indicator parameter. Work on version 2 of this standard is in progress.

ATIS-1000096, Out-of-Band PASSporT Transmission Involving TDM Networks, defines how SHAKEN PASSporTs can be transmitted out-of-band for the portions of the call using TDM signaling. A Secure Telephone Identity Call Placement Service (STI-CPS) temporarily stores PASSporTs for the TDM portions of a call so that the PASSporTs are not lost due to the use of TDM signaling. Before a call is converted from SIP to TDM, the SHAKEN PASSporT is published to an STI-CPS. When a call is converted from TDM back to SIP, the SHAKEN PASSporT is retrieved from an STI-CPS.

Out-of-Band PASSporT Transmission Involving TDM Networks is currently being used in production for both inbound and outbound calls by multiple RLECs with TDM interconnects. Out-of-Band PASSporT Transmission Involving TDM Networks can be a more cost-effective solution for some than replacing existing TDM interconnects with IP interconnects.¹³

2.3. Methods to encourage and promote technical solutions

The following sections describe the current technical landscape for solving call authentication in both the short and long term. The first discusses the choices providers have available to achieve STIR/SHAKEN deployment and call authentication. The second and third sections describe the two main areas of challenge and potential solutions for moving toward all-IP and a more ubiquitous end-to-end IP based STIR/SHAKEN eco-system.

2.3.1. Short-term solutions for call authentication

Small providers should first and foremost deploy STIR/SHAKEN for calls that currently leave or enter their network using IP interconnects. As described in Section 2.2, STIR/SHAKEN can be deployed by small service providers for calls that leave or enter their network using IP interconnects. For calls that currently leave or enter small service provider's networks using TDM interconnects, listed below are three solutions that the small service provider can consider:

1. Implement IP network capability (if not already implemented), acquire IP interconnection, deploy SHAKEN in band within SIP signaling, and transition all calls to use IP interconnection as expeditiously as possible;

¹³ See *In re Call Authentication Trust Anchor*, WC Docket No. 17-97, Wabash Ex Parte Letter, at 2–3 (Aug. 17, 2021) (“It did not require changes either to our network or interconnection with other networks. It operates reliably at a substantially less capital investment and recurring expense than the cost of carrying our calls to a distant IP interconnection.”) (available at: <https://ecfsapi.fcc.gov/file/10817447614778/8.17.21%20Wabash%20OOB%20Exparte%208-17-21.pdf>).

2. Deploy SHAKEN functional components and publish or retrieve SHAKEN PASSporTs to an STI-CPS as described in Out-of-Band PASSporT Transmission Involving TDM Networks, ATIS-1000096; and,
3. Set or interpret the ISUP screening indicator parameter indicating each call's SHAKEN attestation level as described in Extending STIR/SHAKEN over TDM, ATIS-1000095.

Option #1 requires obtaining IP interconnects. However, this may not always be practical as described in Section 2.1. Implementation requirements such as scalability and costs need to be identified and evaluated by the service provider.

Option #2 requires the intermediate service provider who converts the call to SIP, or the TSP if terminated TDM, to retrieve the SHAKEN PASSporT from the STI-CPS. This also requires the intermediate service provider who converts the call to TDM, or the OSP if originated TDM, to publish the SHAKEN PASSporT to the STI-CPS. Implementation requirements such as scalability, dependency resolution,¹⁴ and costs need to be identified and evaluated for the service provider.

Option #3 requires the intermediate service provider who converts the call to SIP to construct a new SHAKEN PASSporT with the SHAKEN attestation level received in the ISUP screening indicator or requires the TSP to interpret the ISUP screening indicator parameter if terminated. This also requires the intermediate service provider who converts the call to TDM to verify the SHAKEN PASSporT and set the ISUP screening indicator parameter based on the attestation level received or requires the OSP to set the ISUP screening indicator parameter if originated TDM. Implementation requirements such as scalability, dependency resolution,¹⁵ and costs need to be identified and evaluated for the service provider.

2.3.2. Overcoming challenges to VoIP connectivity

One of the challenges to achieve an all-SIP, all-IP telephone network and allowing for end-to-end STIR/SHAKEN with SIP has been the challenge of direct, IP-based network-to-network interconnection between all service providers.

The traditional method of direct interconnection requires at least two or more service providers meeting physically at locations, often referred to as “carrier hotels” or “meet points,” where these providers exchange traffic and physically link their networks. These direct interconnection practices have evolved for many years for the purposes of Internet connectivity but can also be relevant to VoIP interconnection and the exchange of SIP traffic over this physically connected network-to-network interface (NNI). This physical interconnection has a number of properties that are desirable for voice and real-time data. In particular, for large amounts of traffic and when bandwidth utilization is large and symmetrical, the cost and density of a physical “wired” connection going through a carrier grade router can be beneficial to the efficient transmission of voice call signaling and media traffic. VoIP

¹⁴ See ATIS-1000097 Technical Report on Alternatives for Call Authentication for Non-IP Traffic for dependencies (available at: https://access.atis.org/apps/group_public/download.php/60536/ATIS-1000097.pdf).

¹⁵ *Id.*

traffic generally should, to the extent possible, be delivered with high quality of service (QoS) that facilitates good voice quality by ensuring lower occurrence of packet loss or retransmission. Physical interconnection can provide a balance of cost-effectiveness, bandwidth efficiency and the ability to achieve high levels of QoS per physical connection.

For smaller providers the calculus of bandwidth, capacity, and the economics of network connectivity can be quite different than for larger providers. Often for many smaller providers with limited subscriber lines, the peak bandwidth and capacity requirements do not justify, for example, an entire dedicated physical connection or set of physical connections to other IP peers. Geographic proximity concerns can present very real technical and economic challenges for both parties that may want to establish direct connectivity. Fortunately, SIP/VoIP is an IP-based technology using the same physical network requirements as internet connectivity and has more recently become widely utilized. Internet connectivity may be established via business or commercial connectivity arrangements that provide more granular dedicated bandwidth services with much wider geographic availability and is currently readily available to small service providers or established for other business purposes. Solutions such as Metro Ethernet and SD-WAN are options which typically do not have many of the costs, restrictions, and burdens associated with physical direct interconnection points. This gives flexibility for both parties where establishing SIP connectivity over a public internet network connection can provide the reliability and Service Level Agreement (SLA) of dedicated networks but at capacities that are a fraction of what would otherwise be required for physical dedicated connections.

Concerns of using public internet or what is considered “non-carrier grade” solutions can include issues of security, reliability, and the ability to provide QoS. If multiple Internet Service Providers (ISPs) are in the IP packet transport path of OTT SIP from small service providers, VoIP traffic may be more susceptible to issues of packet loss, delay, and variable delay (aka “jitter”). There can also be regulatory concerns such as potential implications for Intercarrier Compensation and/or physical network costs such as transport.

The network related QoS concerns are items that are being addressed in the work of the ATIS/SIP Forum IP-NNI Joint Task Force related to defining standardized use of generally available public IP networks. There are also positive advantages to these new SIP connectivity approaches compared to network interconnection. Among the challenges of traditional facilities-based interconnection, or even IPSec or other network tunnelling techniques, are that these techniques literally connect two networks at the physical IP layer. This requires careful and critical management of security, network exposure, and policy rules that need to be worked out with comprehensive technical and legal agreements. The advantages of these new approaches are that they utilize techniques that are common in trunking and other SIP applications where the security is limited to application layer compared to the physical network layer, where exposing physical networks to potential competitors or peers, in particular in large numbers, may be avoided.

The availability of solutions that provide reliable internet connectivity with QoS has grown tremendously in recent years. Even consumer internet connectivity, bandwidth, and reliability has grown tremendously as shown by the recent global pandemic and heavy use of not only voice, but video-based conferencing and calling services. However, within VoIP standards, specifically with Real-

Time Protocol (RTP), there are several tools commonly available to most deployed SIP devices and software stacks that can help provide more reliability, redundancy and error-correction while being utilized in a best-effort public IP network. Additionally, there are many advanced Compression/DECompression (codecs) algorithms that could be utilized beyond the common G.711 μ-Law codec that dominates the US PSTN and provide excellent adaptivity and quality over potentially lossy networks. The recent Real-Time Communications rtcweb working group in IETF has defined common profiles with tools including more advanced audio codecs that are now in wide use with SIP clients, web browsers and device OS software stacks and are supported by many VoIP products today.¹⁶

Many of the techniques discussed above have been addressed in existing specifications focused on SIP trunks and other similar SIP connectivity product focused profiles. SIP Connect 2.0 from the SIP Forum is one which specifically has a profile meant for provider level connectivity as compared to PBX registration. There is a growing list of interested companies where implementation and products could soon follow. Although there is informal usage of these techniques by many providers, the use of these techniques is reportedly not consistent with security best practices. A larger industry endorsement of a proper security-validated standard that can be more widely implemented in vendor and open-source products may allow quick and economical adoption by most providers.

OTT SIP generally implies the use of commercially available public internet access to maximize availability of IP interconnection while minimizing the cost of IP transport. OTT SIP is likely to be the fastest, cheapest way that small IP-based TDM-connected service providers will be able to transition to VoIP Network-to-Network Interconnection (NNI) and support STIR/SHAKEN call authentication technology. However, small TDM based providers would need to transition to IP to realize this benefit.

2.3.3. Overcoming challenges to VoIP destination routing

The current telephone network routing paradigm is based on the fundamental premise of associating terminating NPA-NXX telephone numbers with routing and a destination switch location with the LERG™ Routing Guide. VoIP has adopted a similar paradigm but relies mainly on peering/interconnection agreements to determine the terminating destination location of SIP traffic. This has worked by closely managing these interconnection agreements and where a TDM endpoint is involved, may also rely upon competitive IP to TDM/TDM to IP tandem services that bridge the gap between these worlds as well.

One of the issues with current VoIP routing and interconnection paradigm is the need for destination routing associated with TDM switches and a similar solution for all-IP providers. Exclusive use of direct interconnection for routing calls to all providers including VoIP destinations may not be practical in the long term. There may always be a role for intermediate carriers that help aggregate the ability to reach different destinations as the industry transitions from TDM to IP.

¹⁶ While advanced codecs are more resilient and often save bandwidth required, they can come at a cost. Newer adaptive codecs if not supported end-to-end can require transcoding hardware or software to transcode from G.711 that is ubiquitously deployed across the PSTN to some other codec that is more resilient to packet loss, delay, and jitter.

Today, there are two general categories of available solutions for how to receive calls via VoIP. These solutions are focused on how providers manage allocated NANP telephone number resources.

The first allows the VoIP provider direct access to NANP telephone numbers pursuant to FCC 15-90 and allows the VoIP provider the ability to administer telephone numbers allocated directly to it for providing voice service. The second allows the VoIP provider to obtain numbering resources from the carrier partner's allocated NANP numbering resources where the carrier partner administers the numbers.

The following diagram shows a view of the potential interconnection arrangements. On the right is the traditional set of providers that are either fully TDM or both TDM and VoIP. The left side shows the proposed set of VoIP providers that are either direct IP interconnected, fully over internet-based services or a hybrid of both. The dashed lines represent the paths with use of the public Internet as the transport, which while is in some use today, is not represented with standards or industry endorsed best practices as discussed in Section 2.1. However, it is included to show what the transitional picture could look like if the goals of Section 2.1 for internet-based transport would be widely adopted.

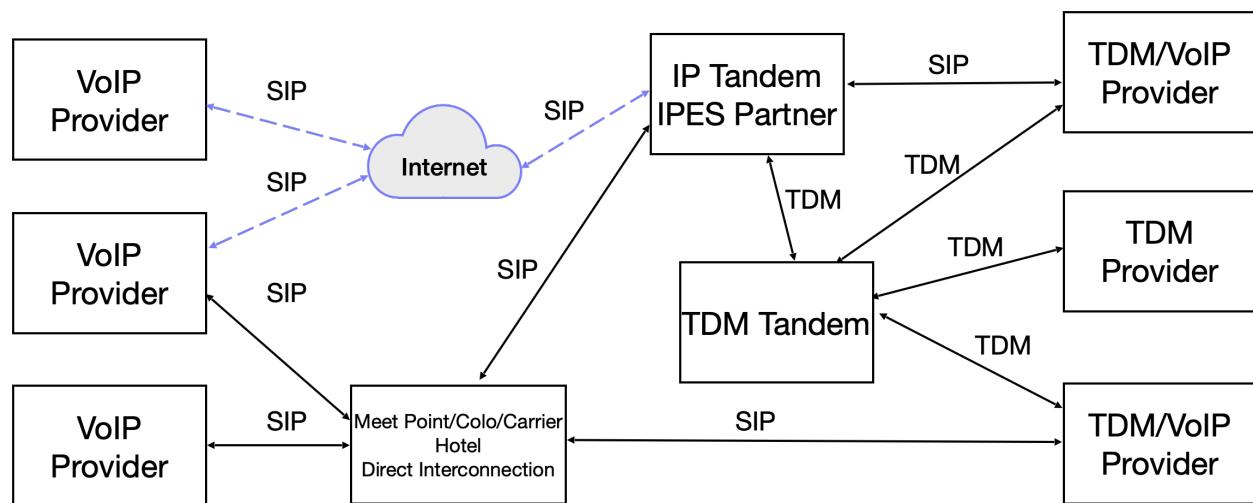


Figure 4: Landscape of potential interconnected provider connectivity and transport options

Both routing options may have different cost structures than the routing currently used by small service providers with TDM interconnects. The cost structures need to be identified and evaluated for the service provider.

For the IP transition to be complete, the providers on the right would transition toward becoming all-IP providers shown on left and the TDM portion of the PSTN traffic would support less and less traffic until fully transitioned.

2.4. Next Steps

The CATA WG Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR, which established the Governance structure, was approved by the NANC in May 2018. The STI-GA was

structured to encourage broad industry representation and small service providers are well represented on the STI-GA Board. Because of this, the interests and concerns of small and rural service providers are considered when establishing policies, as well as developing outreach opportunities. The now well-established STI-GA processes can reasonably continue to address the needs of small and rural service providers, including continuing to advance STIR/SHAKEN deployment.

The STI-GA should create a webinar to help small voice service providers understand how each STIR/SHAKEN technical solution discussed above fits into the STI-GA ecosystem. Major voice service providers are encouraged to volunteer to engage in lab testing with small service providers, including testing of alternate solutions (e.g., over-the-top interconnection solutions). Standards bodies should work on technical standards needed for potential solutions discussed in the report.

Furthermore, the WG provides two additional recommendations below.

As described in ATIS-1000096, Out-of-Band PASSporT Transmission Involving TDM Networks, an STI-CPS is used to temporarily store PASSporTs for the TDM portions of a call so that the PASSporTs are not lost due to the use of TDM signaling. Each STI-CPS shares every PASSporT received with all other STI-CPSs in the SHAKEN ecosystem so that the service provider publishing the SHAKEN PASSporT can use a different STI-CPS than the service provider retrieving the SHAKEN PASSporT. In order to ensure that all STI-CPSs are aware of each STI-CPS in the SHAKEN ecosystem, a centrally managed list of STI-CPSs is necessary. Without a centrally managed list of STI-CPSs, islands of non-interconnected STI-CPSs may be formed which could decrease the likelihood of the SHAKEN PASSporTs being received by the TSP. The industry should determine the entity, if appropriate, that will be responsible for managing the list of STI-CPSs. To that end, the CATA WG recommends that the Commission ask the CATA WG to expeditiously study alternatives and recommend a governance structure as well as any action the FCC needs to take.

The CATA WG also concludes that, in addition to the specific measures recommended in this report, important technological, economic, and regulatory challenges interfere with end-to-end adoption of STIR/SHAKEN methods for small voice service providers—Principally, ubiquitous SIP interconnection.

However, SIP interconnection between service providers is complex and cannot be resolved within the scope of the FCC's June 15, 2021, Charge Letter. To address this issue, the CATA WG recommends the Commission encourage the industry to develop and propose a solution to the SIP interconnection problem to the FCC within 6-12 months of the date of this report. Only if, after the 6-12-month window, the industry fails to develop a reasonable solution should the FCC consider more prescriptive action.

Specifically, we recommend that the industry group be comprised of representatives from the same associations that stood up the STI-GA structure. Within 30 days from the date the Commission accepts this CATA WG report and recommendation, these industry associations will develop the structure for the discussion. At the end of the period the industry group will submit a final report to the FCC with any agreed upon solutions, FCC rules that need changing, and recommendations for unresolved issues, if any, to be addressed in an NPRM. The industry group will give periodic updates to the FCC.

Additionally, new standards development can be done concurrently as the need for standards are identified.

3. Conclusion

While future efforts are necessary to achieve the full guarantees of the TRACED Act, and each of the sections above could be expanded and explored in greater detail, the CATA WG is confident that this report outlines the general landscape for deployment of STIR/SHAKEN solutions by small service providers.

4. Glossary

Attestation – In the context of SHAKEN, the attestation of a call is represented by an “attest” claim allowing the OSP that is populating an Identity header to clearly indicate the information it can vouch for regarding the origination of the call. [ATIS-1000074] This includes the known validity of the TN-based caller identity.

Authentication – A process based on the Authentication Service (STI-AS) function defined in [ATIS-1000074] which is the SIP application server that creates an identity header [RFC8224] using private keys to generate a PASSporT [RFC8225] including a digital signature that protects the integrity of the information, most importantly the TN-based caller identity, used in a call.

Carrier Grade – “carrier-grade” is not a clearly defined term and does not refer to an industry standard, but generally refers to a carrier network that is extremely reliable, engineered to meet or exceed 99.999% availability and employs automatic fault recovery mechanisms in core signaling and voice service transport. Additionally, Carrier Grade Voice Quality is an audio Quality of Experience (QoE) of users as measured using a subjective Mean Opinion Score (MOS) of 4 (or better), or some reasonable equivalent determined using applicable industry standards for automating audio monitoring and QoE measurement.

FCC – Federal Communications Commission. The FCC may also be referred to in this document as “the Commission.”

Intermediate Service Provider – The term Intermediate Provider means any entity that carries or processes traffic that traverses or will traverse the PSTN at any point insofar as that entity neither originates nor terminates that traffic. 47 C.F.R. §64.1600(i)

IPES – Internet Protocol Enabled Service is telephone service a VoIP provider can establish with telephone number access that uses a partner company (IXC or CLEC) at a minimum to manage traffic from other TDM providers.

IPsec – a secure network-to-network protocol suite for encrypting IP packets creating a network tunnel. IPsec is a layer 3 network security scheme independent of application versus session-based application layer encryption like TLS used in SIP or DTLS used for Secure RTP (Real-Time Protocol)

Originating Service Provider (OSP) – The service provider that handles the outgoing calls from a customer at the point at which they are entering the public network. The OSP performs the STIR/SHAKEN Authentication function. The OSP may also serve in the role as TNSP, Resp Org, TN reseller and other roles. [ATIS-1000089]

Resp Org – A Responsible Organization is an entity authorized by the FCC to assign tollfree numbers to Customers. A Resp Org may also be a service provider, a TN Reseller as well as act in other roles. [ATIS-1000089]

SD-WAN – Software-defined networking (SDN) in a wide area network (WAN). This is a generally available and popular network product that allows companies to build higher-performance WAN networks using lower-cost and commercially available Internet access, generally used to replace more

expensive private WAN connection technologies such as MPLS (Multiprotocol Label Switching) and other “carrier-grade” networking technologies.

Secure Telephone Identity Call Placement Service (STI-CPS) – temporarily stores PASSporTs for the TDM portions of a call so that the PASSporTs are not lost due to the use of TDM signaling. [ATIS-1000096]

Small Business – A business entity of less size or scale than a large enterprise, which may have direct and/or indirect subscriber relationships with one or more VSPs.

TDM – “Time Division Multiplex” is an inter-switch transmission protocol that relies upon channelized data transmission synchronized between two endpoints. As used in this document the reference to “TDM” may also refer to other “Non-IP” data transmission protocols.

Terminating Service Provider (TSP) – The VSP of the called party. The TSP performs the STIR/SHAKEN Verification function.

Verification – A process based on the Verification Service (STI-VS) function defined in [ATIS-1000074] which is the SIP application server that checks the validity of an identity header [RFC8224] using SHAKEN certificates to verify the digital signature contained in a PASSporT [RFC8225] and then the integrity of the information, most importantly the TN-based caller identity, used in a call.

Voice Service Provider (VSP) – The service provider whose network is interconnected to other service providers to both originate and terminate calls across the telephone network. The VSP is responsible for performing both STIR/SHAKEN Attestation functions when acting as the OSP and STIR/SHAKEN Verification functions when acting as the TSP [ATIS-1000089] aka Telephone Service Provider.

Wholesale Service Provider – A facilities-based VSP that acts as: an OSP for the End-User of a Reseller; an Intermediate Service Provider, or a gateway provider.