Best Practices

for the Implementation

of

Call Authentication Frameworks

NANC Call Authentication Trust Anchor Working Group

Table of Contents

Best Practices for the Implementation of Call Authentication Frameworks

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 recent 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] As part of the TRACED Act, Congress directed the Commission to "issue best practices that providers of voice service may use as part of the implementation of effective call authentication frameworks…to take steps to ensure the calling party is accurately identified."[2]

The FCC's Wireline Competition Bureau (WCB) has called upon the North American Numbering Council (NANC), via its Call Authentication Trust Anchor (CATA) Working Group (WG), to recommend best practices that would, in the NANC's view, satisfy Congress's directive above if adopted by the Commission.[3] These recommendations should address at least the following questions:

1. Which aspects of a subscriber's identity should, or must a provider collect to enable it to accurately verify the identity of a caller?
2. What guidelines or standards should providers use when assigning the three attestation levels— A (or "full" attestation), B ("partial"), and C ("gateway")—of the SHAKEN/STIR[4] framework?
3. How should best practices vary depending on the type of subscriber, such as between large enterprises, individuals, and small businesses?
4. When should providers consider using third-party vetting services, and how should they make the best use of them?

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

[2] TRACED Act § 4(b)(7).

[3] FCC Wireline Competition Bureau Letter to NANC CATA WG (Feb. 27, 2020) (available at: https://docs.fcc.gov/public/attachments/DOC-362809A1.pdf)

[4] Signature-based Handed of Asserted Information Using toKENs (Shaken) and Secure Telephone Identity Revisited (STIR) standards.

5. Should there be unique industry-wide best practices for knowing the identity of subscribers located abroad? If so, what best practices could the WG recommend regarding identification of such subscribers?
6. Are there any other best practices voice providers can implement "to take steps to ensure the calling party is accurately identified"?

The best practices recommended in this report were developed based on industry expertise and experience, to assist in the overall objective of mitigating robocalling when implementing call authentication frameworks. These best practices:

1. Are considered voluntary and do not imply mandatory implementation, nor should they be mandated, to ensure carriers have the flexibility and speed to respond to evolving issues.
2. Were developed through rigorous deliberation and industry consensus by a broad set of stakeholders.
3. Have been proven through actual implementation and are more than just a "good idea".
4. Address classes of problems, rather than one-time issues.
5. Do not endorse specific commercial products or services.
6. Should not be assumed to apply in all situations or to all industry types.

Communications organizations should evaluate and implement the best practices they deem appropriate. The recommendations in this report can help inform a specific organization's best practices. Additionally, organizations should institutionalize the review of these best practices as part of their operational processes and assess, on a periodic basis, how implementing selected best practices might assist in the overall mitigation of robocalls.

2 Executive Summary

The best practices below summarize the recommendations of the CATA WG for implementing effective call authentication strategies. Best practices must be tailored to specific calling scenarios and functional relationships among service providers and their discrete Customer classes. Moreover, as the industry's technical working groups advance new robocall mitigation techniques, and if bad actors find ways to subvert current mitigation techniques, best practices must continue to evolve. To these ends, the CATA WG recommends the WCB consider the following best practices to further implement the TRACED Act:

1. **Subscriber Vetting.** Service Providers should vet the identity of retail and wholesale subscribers, in conjunction with approving an application for service, provisioning of network connectivity, entering into a contract agreement, or granting the right-to-use telephone number resources.

2. **TN Validation.** Originating Services Providers should confirm the End-User or Customer's right-to-use a Telephone Number.

3. **A-Level Attestation.** Originating Service Providers should authenticate calls with attestation level A only when they can confidently attest that the End-User initiating the call is authorized to use the TN-based caller identity associated directly with the calling line or account of the End-User.

4. **B- and C-Level Attestation.** Originating Service Providers should only authenticate calls with attestation levels B or C for calls where TN Validation has not been performed on the originating telephone number.

5. **Third-Party Validation Services (referred to by the FCC as third-party vetting services in the charge letter).** Originating Service Providers should use a third-party validation service when they cannot or choose not to independently perform TN Validation. Third-party vetting services may be particularly useful in the case of enterprise customers that acquire telephone numbers from multiple telephone number service providers.

6. **International**. Service providers that sell services to international call originators using North American Numbering Plan (NANP) numbers should develop processes to validate that the calling party is authorized to use the telephone number or caller identity. Further, domestic gateway providers may wish to explore voluntary commercial arrangements with international providers that include terms and conditions that would give the domestic gateway provider the tools, information, and confidence to trust the validity of the calling identity.

7. **Ongoing Robocall Mitigation.** Service providers, whether IP- or non-IP-based should have ongoing robocall mitigation programs in addition to implementing call authentication protocols. The elements of such programs may vary depending on the nature of the service provider’s business but may include ongoing monitoring of subscriber traffic patterns to identify behaviors that are consistent with illegal robocalling. Service providers may, after further investigation, take appropriate action to address such behaviors.

The subsections of section 3 below roughly correspond to the order of the questions in the WCB letter, but the subject matter addressed in the subsections may exceed the specific inquiries. The group also defined material terms when responding to the WCB questions as necessary, which are contained in the Glossary.

3 Best Practice Recommendations

The following sections provide context for the specific best practices recommended by the CATA WG to implement effective call authentication frameworks. The report defines many of the concepts regarding the parties that have a role in the telephone number caller identity trust ecosystem. The best practices should provide both a technical and business relationship framework for how telephone number identities can be trusted as calls are delivered from origination to termination. The trust framework is governed by participation in the SHAKEN ecosystem, whereby responsible parties abide by FCC rules, industry standards, or the Secure Telephone Identity Governance Authority (STI-GA) policies. Likewise, subscribers to a voice service are bound by terms of service that require the correct use of telephone number caller identities when initiating calls.

3.1 Vetting caller identity

Accurately defining the terms "subscriber" and "caller identity" will establish the proper context for relationships between the two terms and use-cases that will inform the best practices. The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. The phone number may or may not be associated with the subscriber's account with the responsible party. The definition of caller identity is precisely defined in ATIS-1000088, A Framework for SHAKEN Attestation and Origination Identifier:

> *Telephone Number (TN)-based caller identity* - the originating phone number included in call signaling used to identify the caller for call screening purposes. In some cases, this may be the Calling Line Identification or Public User Identity. In other cases, this may be set to an identity other than the caller's Calling Line Identification or Public User Identity.

In other words, the TN-based caller identity represents the telephone number used in a telephone call that is uniquely associated with a subscriber.

3.1.1 Overview of a subscriber

The subscriber is an entity that has a business relationship with a service provider who transits, originates and/or terminates calls on behalf of the subscriber. ATIS-1000088 defines two concepts of subscriber including *Customer* and *End-User*:

> *Customer* - Typically a service provider's subscriber, which may or may not be the ultimate End-User of the telephone service. A Customer, for example, may be a person, enterprise, reseller, or value-added service provider.
>
> *End-User* - The entity ultimately consuming the VoIP-based telephone service. For the purposes of this report, an End-User may be the direct customer of a Voice Service Provider (VSP) (the interconnected provider that originates the call to the telephone network) or may indirectly use the VoIP-based telephone service through another entity such as a reseller or value-added service provider.

End-Users are typically the *retail* consumer or commercial entity that has purchased the right-to-use a telephone number (or numbers) as part of a service to which the End-User has subscribed. Customers, on the other hand, may be *wholesale or retail* Customers of a VSP. In the latter case, they are also End-Users of the VSP's service. Conversely, resellers or value-added service providers may be Customers but are not End-Users. Instead, End-Users of their service may not have an authenticated relationship with the VSP that is the originating network of the call and is responsible for attestation of the call.

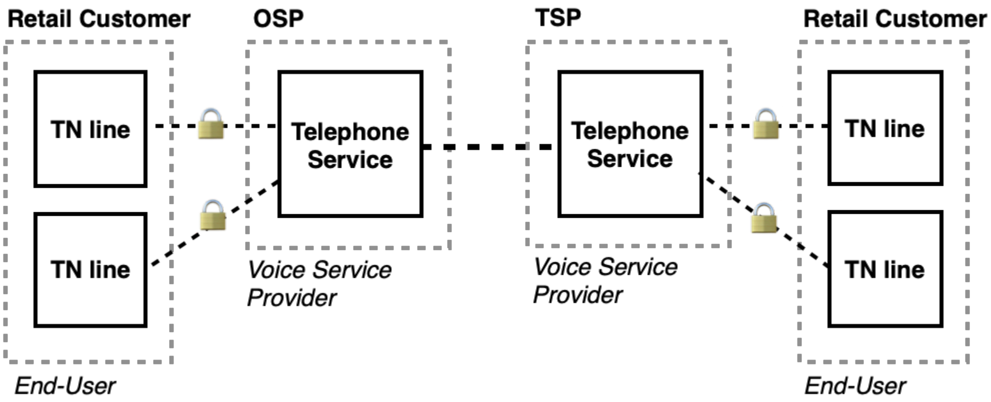


Figure 1: Example of End-User as a direct retail customer of a voice service provider acting as the OSP for a call. The Terminating Service Provider (TSP) receives the call and delivers it to their End-User subscriber.

Generally, a subscriber that is both an End-User and a Customer of a VSP can be classified as a "direct" subscriber type. Ideally, the service should always be provided over an authenticated network channel using up-to-date and robust authentication procedures, so the service provider knows with confidence who is sending the calls into its network. ATIS-1000088 provides two example use-cases of this subscriber type: the direct individual assignment case A.1.1; and the pre-paid account case A.1.2. The figure above shows an example of a retail Customer that is the End-User represented by the TN-based caller identity. Note the authenticated relationship (denoted by the lock icon) between the OSP and the End-User.

There are, however, many common call use-cases beyond direct subscriber cases. These *indirect* use-cases can take many forms. ATIS-1000088 provides three illustrative use-cases including Enterprise A.1.3, Communications Reseller A.1.4, and Value-Added Service Provider (VASP) A.1.5. For A.1.3, the Enterprise is the End-User and has a direct subscriber relationship with the VSP, although the Enterprise may be using indirectly acquired TNs (from the perspective of the VSP) that were assigned by a Telephone Number Service Provider (TNSP) and/or Responsible Organization (Resp Org) in the case of Toll-Free telephone numbers. In the A.1.4 and A.1.5 indirect subscriber calling cases, the reseller or VASP is a Customer of the VSP, i.e., the VASP/reseller has an authenticated relationship with the VSP as described by the above use-cases. However, in A.1.4 and A.1.5, the End-User ultimately has an indirect indeterminant relationship to the VSP. In order to properly validate the authority of an indirect End-User to be represented by a particular telephone number (telephone number-based caller identity) there needs to be new and additional mechanisms in place so the VSP can be sufficiently confident the caller identity or telephone number used for the call merits full attestation (i.e., A-level attestation).

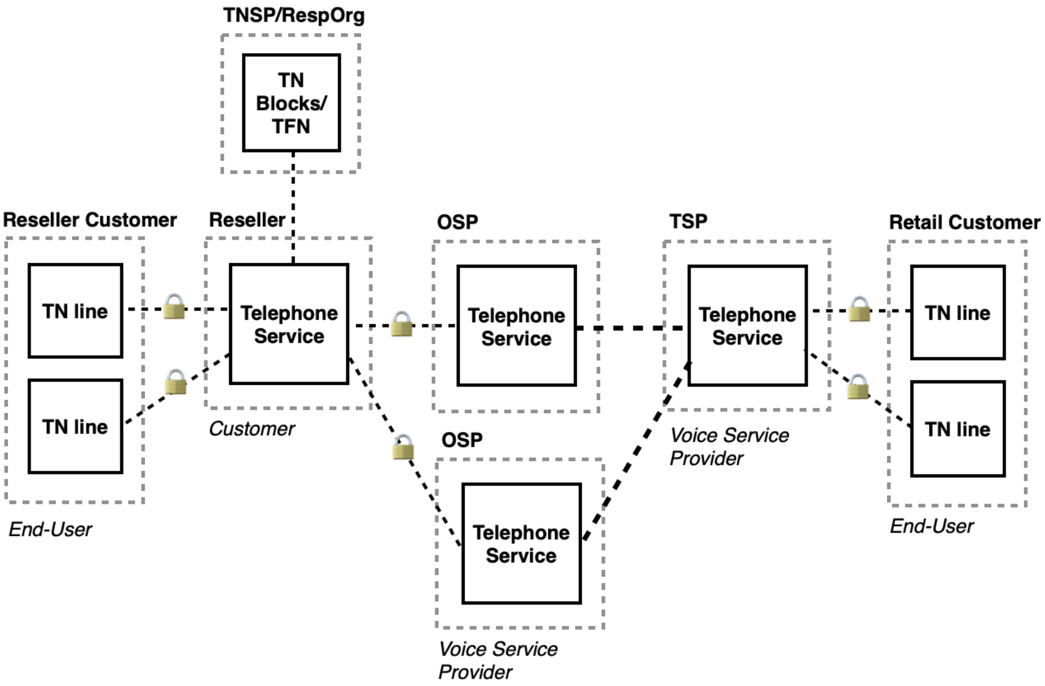


Figure 2: Example of a reseller as customer of multiple TSPs and End-User as a reseller customer

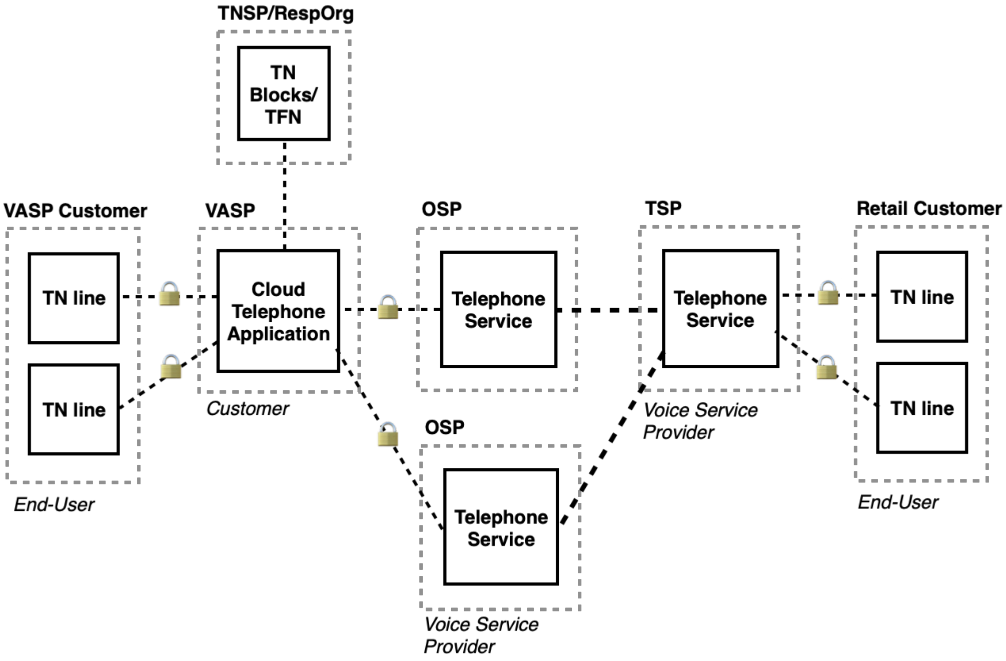


Figure 3: Example of a Value-Added Service Provider as a customer of multiple TSPs with an End-User as the VASP Customer

A further complication in many indirect cases is that the Communications Reseller or VASP may source telephone number resources from multiple TNSPs, or in the case of toll-free numbers from multiple Resp Orgs. In these cases, because of least cost routing or calling path diversity, the TNSPs or Resp Orgs may not be the OSP for a particular call. As a result, validation by the OSP of the authority for right-to-use of the telephone number can also be indirect. The topic of indirect use-cases and the best practices associated with these scenarios will be covered in the validation section (3.4) of the report.

3.1.2 Vetting of the End-User or Customer entity and identity

Whether a subscriber is an End-User or other Customer type, a provider should vet the identity of the subscriber as part of an application for service or contract process. The best practice applies whether the service provider is a VSP, VASP, Reseller, TNSP, Resp Org or other telephone application provider. The type of information collected to vet a subscriber is explicitly different from the information required or used to confirm the right-to-use a telephone number and used to authenticate the use of a TN-based caller identity for a call for STIR/SHAKEN. Moreover, vetting may involve collecting different information for different types of subscribers. For example, it may be appropriate to collect distinct sets of information to vet the identity of residential End-Users, commercial End-Users, wholesale Customers, and other Resellers. In all of these cases, the subscriber vetting process is intended to help determine the legitimacy of a Customer for the purposes of establishing a business relationship. Additionally, such information may be useful and important to law enforcement (e.g., the ability to find and prosecute the Customer in the event they are involved in illegal robocalling or other illegal activities despite being vetted). Such Customer vetting should be part of any robocall mitigation program and should precede TN Validation when establishing new service. The TN Validation process is a separate best practice recommended later in this document.

3.1.3 Best practices for vetting retail Customers

Residential and small business retail End-Users (i.e., mass market Customers) present a low risk for perpetrating illegal robocalls. VSPs collect End-User address contact information for general provisioning and billing of service. Retail End-User service is generally provisioned to a fixed location, is easily identifiable, and is unlikely to generate illegal robocalls.

Commercial retail End-Users, comprised of larger businesses with more complex service configurations, may present a somewhat higher risk of perpetrating illegal robocalls. As a result, a different intensity of vetting may be appropriate for such subscribers.

The general concept of subscriber vetting is embodied in the State Attorneys General/Service Provider Anti-Robocalling Principles endorsed by more than a dozen/certain VSPs.[5] Specifically, Principle #5 reads: "Confirm the Identity of Commercial Customers. Providers will confirm the identity of new commercial VoIP customers by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business." This recommendation from the State Attorneys General/Service Provider Anti-Robocalling Principles provides example customer information to gather during subscriber vetting, however, it may not apply to all VSP use cases or business models.

[5] *State Attorneys General Anti-Robocall Principles for Voice Service Providers* (Aug. 22, 2019) (appended below).

Principle #5, in conjunction with Principles #3 and #4 (described in Section 3.6), are elements of a broader robocall mitigation program for VSPs and are consistent with other industry practices such as the CA Browser Forum defined extended validation procedures for certificates (reference CA-Browser-Forum-EV-Guidelines Section 11). Vetting the identity of a new subscriber should occur whether calls are originated on IP or non-IP networks. In addition, monitoring Customers' network traffic, investigating suspicious calling patterns, and taking action when illegal robocalling campaigns are identified should be included as best practices for all VSPs, whether they originate calls on IP or non-IP networks.

Ultimately, VSPs should have the discretion to develop their own subscriber vetting program, which may include some combination of the practices summarized in this section, based on the types of subscribers they serve. Subscriber vetting should parallel the way VSPs enforce their acceptable use polices and terms of service. VSPs should, however, reevaluate their vetting processes if the VSP's network is found to be used for illegal robocalling.

3.1.4 Best practices for vetting wholesale subscribers

Illegal robocall mitigation for wholesale subscribers can take multiple forms. Resale is one form of wholesale relationship, where the Reseller serves retail End-Users using the facilities-based platform of a wholesale VSP (e.g., Mobile Virtual Network Operator (MVNO) or full-service resale). Transit or transport is another form of wholesale service, where the wholesale VSP provides intermediate transport services or termination services to its wholesale subscriber. Wholesale providers also may give retail providers, such as Resellers, a right-to-use TNs. While calls typically do not originate on a wholesale transit or transport service provider network, it is also important to adequately vet wholesale Customers. If appropriate, wholesale providers may vet identity information for their wholesale Customers by confirming whether the Customer is an FCC Form 499-A filer in the FCC Form 499 Filer Database[6] or intermediate provider registration.[7] If an applicant for a wholesale service such as full service resale or an MVNO is not an FCC Form 499-A filer, the wholesale service provider should understand the nature of the Customer's business that exempts them from being a Form 499-A filer.

As indicated in Section 3.1.3 above, VSPs should have the discretion to develop their own wholesale subscriber vetting program, which may include some combination of the practices summarized in this section as well as Section 3.1.3, based on the types of wholesale subscribers they serve. Wholesale subscriber vetting should parallel the way VSPs enforce their acceptable use polices and terms of service. VSPs who provide wholesale services should also reevaluate their vetting processes if their network is found to be used for illegal robocalling.

[6] Available at: https://apps.fcc.gov/cgb/form499/499a.cfm.

[7] Available at: https://opendata.fcc.gov/dataset/Intermediate-Provider-Registry/a6ec-cry4.

3.1.5 Industry communication and implementation

The industry is in the best position to collaboratively develop a process to educate and encourage service providers to adopt applicable best practices outlined in this document. Associations which participate in the STI-GA governance process represent a broad range of service providers and can disseminate this information to their members and as appropriate may hold informational sessions on this topic.

These practices could be implemented through various mechanisms:

- *Voluntarily* – The best practices for service providers may require updating as industry practices and technologies evolve. This could most effectively be accomplished through collaborative industry working groups. For example, the industry could work to develop both network traffic monitoring, investigation, and policy enforcement best practices to minimize third-party illegal robocalling campaigns.
- *Contractually* – For example, wholesale providers could require clauses in their transit contracts, among others to require customers to adopt robocall mitigation best practices including confirming the identities of their End-User subscribers either directly from the End-Users or by providers or third parties that act on behalf of the End-User.
- *Regulatorily* – Because illegal call mitigation is evolving and the associated regulatory environment for robocall mitigation is still developing, it would be premature to mandate any specific practices or standards in the near-term.

3.2 Guidelines for different SHAKEN attestation levels

The common goal for SHAKEN and the industry is to provide the ability to authenticate calls with attestation "A" level or full attestation, when the End-User initiating the call is authorized to use the TN-based caller identity.

"B" is a higher level of attestation than "C" and can provide some additional information to the terminating provider, but best practice seems to have converged that both "B" and "C" are more useful for identifying originating networks.

An analysis of attestation assignments factoring in connectivity, business association, confirmation of real-world identity, and authorization of the End User to legitimately place calls using the calling number is found in Appendix A.

3.3 Best practices for achieving full attestation for different subscriber types and use-cases

As discussed in Section 3.1.1, there are two subscriber types of End-User and Customer. Depending on whether a subscriber is an End-User or a Customer or both, there are two high-level subscriber relationship cases in the telephone network today. The first is the "direct" relationship where the VSP provides the telephone number as an integrated product within a telephone service to an End-User subscriber (e.g., residential End-User or a commercial entity (small business or complex commercial enterprise)) that may have several End-Users for whom it controls access to telephone service. The second is the "indirect" relationship involving End-Users that are not getting service from a VSP directly. Rather they obtain telephone service through entities such as those mentioned in Section 3.1: enterprise, resellers, VASPs, or cloud telephone application providers. For indirect relationships, the industry is working on various mechanisms that, in the future, can be used to obtain full attestation. This includes, but is not limited to Delegate Certificates, Letters of Authorization, and Central Database methods.

Subscriber Type	Relationship to Originating Service Provider	Description
End-User and Customer	Direct	Subscriber is managed by an Originating VSP with telephone number(s) and telephone service as part of a single product that is authorized for both telephone number usage and telephone service from a directly authenticated device. (e.g., a subscriber that obtains access to the public telephone network via a phone or SIP-PBX that has a direct relationship with the VSP).
End-User Only	Indirect	Subscriber is given the right-to-use a telephone number, block or sets of each with the intent of using those numbers to originate calls via a call initiation functional service. (e.g., an enterprise subscriber that obtains access to the public telephone network via a reseller or VASP).
Customer Only	Indirect	Subscriber is provided an application service, a trunk or a wholesale service that allows them to facilitate the origination of calls from their customers authorized TN-based caller identity for outbound calling services that may support human- or machine-based calling to and from the Public Switched Telephone Network (PSTN) (e.g., a Service Provider (SP) subscriber that is a reseller or VASP).

Table 1: Subscriber types and relationship to OSP descriptions

For best practices regarding individuals and small businesses (i.e., mass-market Customers), as opposed to large enterprises, there may be a generalization made that mass-market Customers typically fall in the direct relationship category, where larger businesses often have multiple telephone services encompassed by a combination of different direct and/or indirect business relationships.

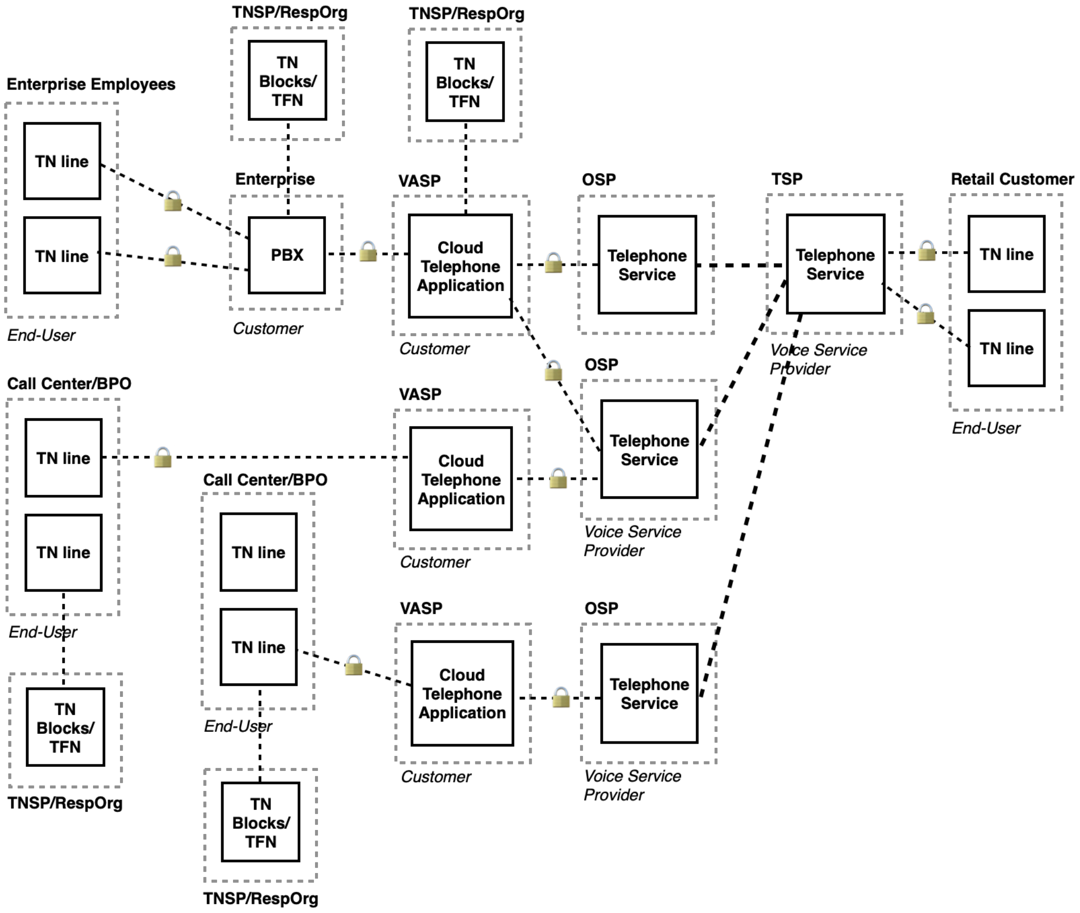


Figure 4: An illustrative enterprise use-case involving both corporate communications as well as outbound customer contact center use-cases

The next section will detail further the best practices associated with the process of validating the authorized use of a telephone number in the context of both direct and indirect subscribers.

3.4 TN Validation

Telephone Number (TN) Validation refers to the confirmation of the End-User's right-to-use the telephone number. TN Validation is necessary and appropriate when an End-User's right-to-use the telephone number is unknown to the OSP responsible for performing SHAKEN attestation for the call. TN Validation is the inherent result of an OSP's assignment of a telephone number to its End-User. Thus, TN Validation may not be necessary as an explicit process in this regard.

TN Validation is intended to support elevation of attestation for a call originating from an End-User with a telephone number, where the telephone number is not assigned by the OSP. Third parties may be used for TN Validation or providers may offer TN Validation for End-Users. Multiple TNSPs may provide telephone numbers to End-Users, such as enterprises or small business, or to providers that offer services to End-Users, such as resellers, VASPs, or cloud telephone application providers in larger blocks or ranges, which those providers then may assign to their End-User as part of the telephone service.

It is also intended to support cases of legitimate spoofing of telephone numbers where an End-User that is authorized to use a telephone number through a particular TNSP relationship may want to also use that telephone resource(s) with another communications service.[8] One example of legitimate spoofing is where a school district has a telephone number associated with its main switchboard supported by one service provider, which it also wants to use as the TN-based caller identity with the snow-day robocalling application service supported by another service provider.

3.4.1 TN Validation for Toll-Free Resp Orgs

Where the Resp Org, or in some cases the reseller SP who obtained the Toll-Free Number (TFN) for the End-User, is not the Service Provider for the End-User, on a call(s) the relationship between the OSP and the End-User for the TFN is indirect. A TN Validation process (see 3.4 above) may be used in advance of call placement. For TFNs, the Resp Org or, in some cases, the reseller SP who obtained the TFN for the End-User is the entity with the knowledge of which End-User has been assigned the TFN.

The End-User, which has the right-to-use a TFN, may authorize a third party to use the TFN for the calling party number. In this case, another mechanism would be needed to provide proof the third party is allowed to use the TFN —e.g., one of the mechanisms mentioned in section 3.3 being worked on by the industry. For more information regarding Resp Org requirements, see Appendix B.

3.5 Identification of international subscribers

For internationally originated calls, there is a desire for other countries to adopt corresponding STIR/SHAKEN, STI-GA and STI-PA ecosystems that provide authorized digital signatures, endorsed by local regulatory agencies and coordinated through cross-border efforts being discussed in the Joint ATIS/SIP Forum IP-NNI Task Force and other forums. This is similar to what is happening between the US and Canada, where there is coordination of providing authorized root certificates specific to a country or region.

In the United States, it is a long-standing problem that international gateway traffic is a significant source of fraudulent traffic. However, both how and where that traffic is coming from is not well defined. Traditionally, an "international gateway" is defined as a network element that specifically translates international call signaling from country specific standards to US provider compatible protocols. As VoIP services have evolved, the use of the term "international gateway" has unfortunately become less well defined. VoIP does not have as many geographic restrictions as non-IP services, which has enabled international entities to send VoIP traffic easily around the world including traffic that may terminate into a US-based provider's network. Today, it is understood that most of the fraudulent internationally-sourced traffic is coming through domestic telephone application providers and VSPs. Often, this occurs through underground or backdoor types of operations that mainly cater to malicious entities (either international or domestic) that want to terminate traffic with illegally spoofed NANP

[8] *See also* ATIS-1000089, Study of Full Attestation Alternatives for Enterprise and Business Entities with Multi-Homing and Other Arrangements, or other processes, including processes in development but not yet published.

telephone numbers or illegitimate or invalid numbers. While fraudulent traffic does happen with international calling party telephone numbers coming from the legitimate country of origin, currently the portion of this traffic to the overall fraudulent call volume is relatively small. Based on SP experience, it appears the primary source of the problem may not be "international gateways," rather, it is VoIP applications, trunks, and wholesale providers that cater to subscribers sourcing traffic from international entities with fraudulent intent.

Fraudulent internationally sourced or originated traffic can be separated into the following broad categories:

- Internationally-based companies or individuals sending fraudulent traffic using US-based application, trunking, or wholesale services with spoofed domestic numbers;
- Internationally-based companies or individuals sending fraudulent traffic using US-based application, trunking, or wholesale services with spoofed international numbers;
- Internationally-based companies or individuals sending fraudulent traffic using internationally based application, trunking, or wholesale services with spoofed domestic numbers; or
- Internationally-based companies or individuals sending fraudulent traffic using internationally based application, trunking, or wholesale services with spoofed international numbers.
- Best practices for these use cases could utilize these broad categories to inform specific future practices.

3.5.1 Alternative mechanisms to assist with interoperability in the absence of STIR/SHAKEN technologies

Best practices for internationally-originated calls using NANP numbers are still evolving, including how to acquire sufficient information to accomplish TN Validation for elevation to "A" attestation. Industry consensus has not yet coalesced on call authentication with less than "A" (full) attestation in some call scenarios. This could include the best practices, as appropriate, endorsed by this working group and explained in this document, including the vetting of customers and the validation of telephone numbers used for the services offered.

For example, international VSPs have proposed technical and contractual solutions that may enable them to work with domestic carrier partners to apply the full range of SHAKEN attestations to calls originating overseas. This "enhanced international attestation" approach may offer international providers the means to deliver more information and value to domestic carriers and consumers than if all calls originating outside the U.S. are assigned a "C"-level attestation, or are not authenticated. International providers may enter into voluntary commercial agreements with domestic carriers or intermediate providers capable of assigning the relevant SHAKEN attestation level based on information the international provider has collected from its Customers (as well as its vetting, ordering, and TN validation procedures). Industry stakeholders should be permitted to develop the specific mechanisms or techniques by which they achieve higher levels of fidelity to SHAKEN attestation for international traffic.

In one example of this arrangement, international voice traffic could be segmented into separate streams via a multi-trunk approach that correlates to the three attestation levels of SHAKEN—"A" for calls that originated on a provider's network from numbers assigned to the originating subscriber, "B" for calls that originated on a provider's network from numbers that were not assigned to the originating subscriber, and "C" for calls that neither originated on a provider's network nor from numbers assigned to the originating subscriber. Domestic carriers could then rely on information proffered by the international provider to assign the appropriate attestation level and send the traffic either to another downstream provider or to its termination point.[9]

It should be noted that while this approach would be voluntary for domestic carriers (permitting these providers to choose international partners that display high levels of trustworthiness), the inclusion of robust commercial and contractual remedies, if an international provider fails to appropriately identify its traffic, could obviate domestic carriers' concerns about exposure to reputational or enforcement risk as well as regulators' anxieties that such a mechanism could be used as a backdoor for illegal robocalls or spoofing.

Additionally, the Global System for Mobile Communications Association (GSMA) has recently undertaken an activity by establishing the Validating INtegrity of End-to-End Signaling (VINES) Working Group to develop a set of recommendations to prevent internetwork signaling fraud, which includes illegal robocalls, illegal spoofing, illegal toll bypass and consumer fraud. One of its objectives is to propose a mechanism to interwork with STIR/SHAKEN.

3.6 Additional best practices for accurate identification of calling party

There are several additional best practices discussed by the working group for achieving full attestation for indirect relationships, and for more robust robocall mitigation practices, as discussed below.

3.6.1 Achieving full attestation for indirect relationships

There are many use-cases, subscriber types, and subscriber relationships guiding implementation of best practices regarding accurate use of a TN-based caller identity as part of a call and the application of SHAKEN attestation of a call. The base SHAKEN framework has good coverage for direct subscriber relationships. For indirect subscriber relationships, there has been much discussion about solutions to provide end-to-end authentication. Best practices in general should include TN Validation to confirm the authority for an End-User's right-to-use a TN-based caller identity, including a robust mechanism to authenticate the call and allow the OSP to confidently elevate to full attestation "A." The ATIS/SIP Forum IP-NNI Joint Task Force has two study documents that discuss solutions for handling these indirect use-cases: ATIS-1000088, A Framework for SHAKEN Attestation and Origination Identifier; and ATIS-1000089, Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements.

[9] *See generally* Letter of Sheba Chacko, Chief Regulatory Counsel, BT Americas Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket Nos. 17-97, 20-67 (filed Apr. 21, 2020).

3.6.2 Robust robocall mitigation practices

In addition to the vetting best practices described above, robust robocall mitigation programs should include network monitoring for suspicious calling patterns. If, after appropriate investigation, it is determined that illegal robocalls are likely originating or transiting their networks, SPs should take appropriate action to stem the flow of the calls by taking actions permitted by FCC rules and orders, or contractual provisions. Along with Principle #5, as set forth in section 3.1.3 above, it is recommended that SPs implement the following two best practices delineated in the State Attorneys General/Service Provider Anti-Robocalling Principles:

Principle 3 – Analyze and Monitor Network Traffic; and

Principle 4 – Investigate Suspicious Calls and Calling Patterns.

The WG recommends these principles, as helpful best practices and recommend that the FCC encourage SPs, as applicable, to adopt applicable best practices as well as the other State Attorneys General/Service Provider Anti-Robocalling Principles. These principles are included in Appendix C for reference.

4 Conclusion

This report recommends best practices that VSPs may use to implement effective call authentication frameworks. In addressing the six specific questions presented to the WG by the WCB, the group considered the various types of providers operating in the voice ecosystem and the different services they provide. The WG sought to avoid best practice recommendations that were overly prescriptive because narrowly tailored recommendations could be inapt for certain types of services. While recognizing that STIR/SHAKEN is relevant only for IP networks, the group also recommended best practices for a broader robocall mitigation program that apply equally to IP and non-IP networks and services.

These best practices must evolve and respond to the dynamic nature of mitigating illegal robocalling. This iterative process should be industry driven to ensure providers have the flexibility and speed to respond to bad actors. Regulatory solutions—for example giving service providers more tools (e.g., blocking tools) and taking additional actions that target bad actors effectively complements industry efforts. Further solutions in this same vein (i.e., actions aimed at thwarting bad actors) may be necessary in the future.

5 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.

Caller Identity - The originating phone number included in call signaling used to identify the caller for call screening purposes. In some cases, this may be the Calling Line Identification or Public User Identity. [ATIS-1000082]

Certificate Validation – An act or process by which a certificate user established that the assertions made by a certificate can be trusted. [ATIS-1000084.v002]

Communication Resellers – Non-facilities-based VSPs that are wholesale Customers of and resell the voice services of facilities-based VSPs, whereby the facilities-based VSPs are also the OSPs for the reseller's End-User subscribers.

Customer – Typically a service provider's subscriber, which may or not be the ultimate End-User of the telecommunications service.

End-User – The entity ultimately consuming the VoIP-based telecommunications service and may include the End-User's device used for placing the call.

Enterprise – A business, non-governmental organization, or government entity that is a user of voice services. An enterprise may have direct relationships with any type of service provider, or service or TN reseller described in this document, and may have indirect relationships with any of these entities. An enterprise may initiate calls directly on its own behalf or may contract with other entities (e.g., call centers or hosted service providers) to initiate calls on its behalf. [ATIS-1000089]

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

Form 499-A – An FCC multi-purpose form used for annual reporting revenues which are used as the basis for federal Fund assessments, funding of some administrative functions, sharing costs for some telephone service administration, and calculating regulatory fees; and one-time (with obligation to revise if information changes) designation of an agent for service of process, and fulfillment of obligations to register with the FCC by law.

Identity – Unless otherwise qualified, an identifier that unambiguously distinguishes an entity for authentication and other security and policy application purposes.

Identity owner – This is the user, subscribed to the controlling operator, who is currently assigned a specific E.164 phone number for call routing purposes. This E.164 number may be presented to a called party as the user's calling party identity. The identity owner can authorize other users or subscribers of controlling or non-controlling operators to also use the E.164 number as caller identity in phone calls made on the identity owner's behalf. [ATIS-1000072]

Identity service provider – An entity that verifies, maintains, manages, and may create and assign identity information of other entities. [ATIS-1000044]

Individual – An entity with a characteristic of being human.

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)

Large Enterprise – See 'Enterprise'.

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]

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.

Subscriber's Identity – This is the name, title, and authority of the subscriber agreement signatory.

Telephone Identity – An identifier associated with the originator or a telephone call. In the context of the SHAKEN framework, this is a SIP identity (e.g., a SIP URI or a TEL URI) from which a telephone number can be derived. [ATIS-1000080]

Telephone Number Caller Identity – represents the telephone number used in a telephone call that is uniquely associated with a subscriber.

Telephone Number Service Provider (TNSP) – SP that has been formally assigned TNs by the national numbering authority (e.g., NANPA). A TNSP may assign a subset of its TNs to a business entity (i.e., TN Assignee), to be used as Caller Identification (ID) for calls originated by the business entity. TNSPs can also serve in the role as OSP or TSP. [ATIS-1000089]

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

Third-Party Vetting Service – A service provided to a VSP by a third party for the purpose of vetting potential and current subscribers.

Third-Party TN Validation Service – A service provided to a VSP by a third party for the purpose of confirm the right-to-use of TNs for potential and current subscribers.

TN-based Caller Identity – The originating phone number included in call signaling used to identify the caller for call screening purposes. In some cases, this may be the Calling Line Identification or Public User Identity. In other cases, this may be a TN-based caller identity that is not associated directly with the calling line or account of the subscriber. [ATIS-1000088]

TN Reseller – The party who holds the right-to-use a TN and offers for resale the right-to-use that TN.

TN Right-to-Use/Authorization – When a party is appropriately assigned a TN, this is the right-to-use that TN; the assignment confers the right to the use of the numbering resource.

TN Validation – A process by which an indirect End-User's authorization to use a telephone number or set of telephone numbers is established and the process of providing that information to the VSP originating the call onto the telephone network through the use of existing and upcoming standardized secure mechanisms. TN Validation can be performed at the time the right-to-use of telephone numbers is established or throughout the life of the contract.

Value-added Service Provider (VASP) – Generally, a third-party provider supporting value-added services, for example including applications beyond the core voice calling services offered by a traditional VSP. In this document, it is used as a general term for VoIP and VoIP application providers that offer voice services without having direct interconnection with other VSPs utilizing wholesale providers for call origination and termination.

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.

Vetting – A process by which a customer's identity and operational legitimacy is confirmed by their service provider. Confirmation can be performed at the time service is established (initial confirmation of identity) or throughout the life of the service subscription or contract (ongoing confirmation such as evaluation of roboscores or traffic patterns indicative of abusive robocalling). TNs are not part of the vetting process; TNs are covered by the TN Validation process.

Vetted – The successfully verified result of a vetting activity.

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.

Appendix A – Attestation Level Guideline Details

ATIS-1000074, Section 5.2.3 Attestation Indicator ("attest") Note 1 under A. Full Attestation states:

> The signing provider is asserting that their customer can "legitimately" use the number that appears as the calling party (i.e., the Caller ID).

Two essential qualifications of the A-level attestation listed in ATIS-1000074 are that the signing service provider:[10]

- Can identify the End-User.
- Has established a verified association of the End-User with the telephone number used for the call.

Two other aspects not listed in ATIS-1000074 but which can have a bearing on the application of the local policy used by a service provider to assign attestation during call authentication are:

- Connectivity of the signing service provider to the End-User.
- Business relationship of the signing service provider with the End-User.

These additional aspects can be used by the signing service provider to better identify the End-User and to qualify if the call is coming from an individual or enterprise, or another service provider.

If the service provider is directly connected to the End-User, origin and screening information may be available and able to be used to assess if the calling number can be legitimately asserted by the End-User.

Conversely, if the service provider is not directly connected to the End-User and is instead receiving the call from another service provider, the indirect connection between the signing service provider and the calling entity obfuscates origin and screening information inhibiting the signing service provider's ability to assess if the calling number can be legitimately asserted by the End-User.

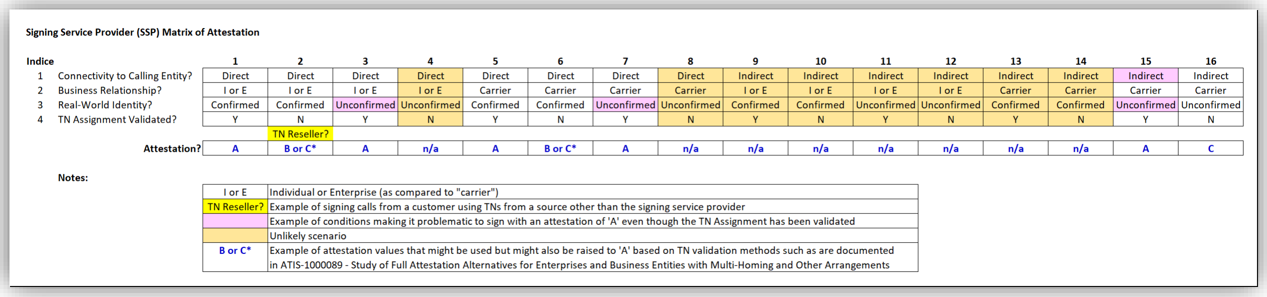
If the End-User is an individual or business customer the signing service provider is very likely directly connected to them and the key aspects highlighted in ATIS-1000074 regarding confirmed real-world identity of the End-User, and a verified association with the calling number are then cardinal in assessing assignment of attestation. And, if the calling entity is connected to and is a customer of another service provider, then there probably is not be a direct business relationship with the calling entity.

Each of the qualifications outlined can be analyzed using two possible values per qualification. i.e., real-world identity is confirmed (or not), caller association with calling number is verified (or not), signing service provider is directly connected to the caller (or not), the calling entity is a customer (or not).

[10] Note: For alignment with terminology used in this document, some of the terms in this appendix have been modified from the original ATIS-1000074 text.

Taken together, the four qualifying factors with two possible values each, yields sixteen possible combinations which can be assessed to estimate the appropriate attestation level of A (full), B (partial), or C (gateway) when authenticating (i.e., signing) a call.

The table below outlines all 16 possible scenarios using the 4 qualifying factors:



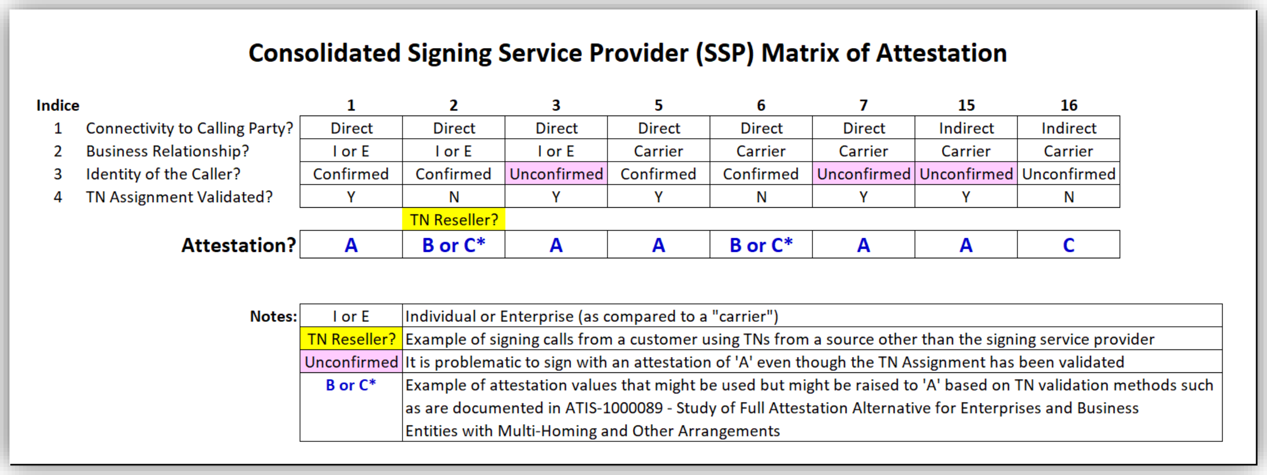
Signing Service Provider (SSP) Matrix of Attestation

Indice		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	Connectivity to Calling Entity?	Direct	Direct	Direct	Direct	Direct	Direct	Direct	Direct	Indirect	Indirect	Indirect	Indirect	Indirect	Indirect	Indirect	Indirect
2	Business Relationship?	I or E	I or E	I or E	I or E	Carrier	Carrier	Carrier	Carrier	I or E	I or E	I or E	I or E	Carrier	Carrier	Carrier	Carrier
3	Real-World Identity?	Confirmed	Confirmed	Unconfirmed	Unconfirmed	Confirmed	Confirmed	Unconfirmed	Unconfirmed	Confirmed	Confirmed	Unconfirmed	Unconfirmed	Confirmed	Confirmed	Unconfirmed	Unconfirmed
4	TN Assignment Validated?	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N
			TN Reseller?														
	Attestation?	**A**	**B or C***	**A**	**n/a**	**A**	**B or C***	**A**	**n/a**	**n/a**	**n/a**	**n/a**	**n/a**	**n/a**	**n/a**	**A**	**C**

Notes:

I or E	Individual or Enterprise (as compared to "carrier")
TN Reseller?	Example of signing calls from a customer using TNs from a source other than the signing service provider
🟪	Example of conditions making it problematic to sign with an attestation of 'A' even though the TN Assignment has been validated
🟧	Unlikely scenario
B or C*	Example of attestation values that might be used but might also be raised to 'A' based on TN validation methods such as are documented in ATIS-1000089 - Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements

The full set of 16 possible combinations of qualifying factors contains several combinations which are unlikely, but which were shown for completeness. A more likely consolidated subset of eight (8) combinations from the table above is shown below:



Consolidated Signing Service Provider (SSP) Matrix of Attestation

Indice		1	2	3	5	6	7	15	16
1	Connectivity to Calling Party?	Direct	Direct	Direct	Direct	Direct	Direct	Indirect	Indirect
2	Business Relationship?	I or E	I or E	I or E	Carrier	Carrier	Carrier	Carrier	Carrier
3	Identity of the Caller?	Confirmed	Confirmed	Unconfirmed	Confirmed	Confirmed	Unconfirmed	Unconfirmed	Unconfirmed
4	TN Assignment Validated?	Y	N	Y	Y	N	Y	Y	N
			TN Reseller?						
	Attestation?	**A**	**B or C***	**A**	**A**	**B or C***	**A**	**A**	**C**

Notes:

I or E	Individual or Enterprise (as compared to a "carrier")
TN Reseller?	Example of signing calls from a customer using TNs from a source other than the signing service provider
Unconfirmed	It is problematic to sign with an attestation of 'A' even though the TN Assignment has been validated
B or C*	Example of attestation values that might be used but might be raised to 'A' based on TN validation methods such as are documented in ATIS-1000089 - Study of Full Attestation Alternative for Enterprises and Business Entities with Multi-Homing and Other Arrangements

Appendix B – Resp Org Establishment

For the general offering of telephone services to subscribers, a TNSP, Resp Org, or other telephone application provider should vet the identification of either the End-User or Customer entities to whom they offer telephone services. However, in the case of the Toll Free, there is an advanced step required before the Resp Org is able to access Toll-Free Numbers for assignment to their End-User.

For Toll-Free Numbers, the authoritative database is the Toll-Free Number Registry. Resp Orgs are the only parties who can assign Toll-Free Numbers, per FCC requirement. The following is the process used for a party to get approved as a Resp Org and then get access to Toll-Free Numbers that they can assign to their End Users.

The following are the Resp Org Establishment Steps:

Any person, company, or organization that can demonstrate the required skills and financial responsibility for managing Toll-Free Numbers can apply to become a Toll-Free Service Provider (Resp Org) in the SMS/800 Toll-Free Number Registry.

1) Complete a multi-page application that includes information on the business, contacts, billing, and certifications by the Resp Org. Resp Orgs are required to upload a copy of their IRS W-9 form at this time.

2) Attend a SMS/800 Toll-Free Number Registry week-long class or self-train with provided materials about Toll-Free.

3) Successfully complete an exam on Toll-Free Industry practices. Exam covers knowledge of customer records, number administration, and service provisioning.

4) Submit a deposit equal to the greater of two months Resp Org's anticipated bill from the Toll-Free Number Administrator, or $4,000. The deposit will be returned in 12 months (with interest) if the Resp Org has a record of paying its bill in full and on time.

After completing all steps, the applicant will be certified as a Toll-Free Service Provider (i.e., Resp Org), and a Resp Org ID will be assigned.

For reference, the ATIS SMS/800 Number Administration Committee (SNAC) developed and maintains–ATIS-0417001, Industry Guidelines for Toll-Free Number Administration.

Appendix C – State Attorneys General/Service Provider Anti-Robocall Principles

The Model Anti-Robocall Principles include the eight principles below:[11]

Principle #1 – Offer Free Call Blocking and Labeling. For smartphone mobile and VoIP residential customers, make available free, easy-to-use call blocking and labeling tools and regularly engage in easily understandable outreach efforts to notify them about these tools. For all types of customers, implement network-level call blocking at no charge. Use best efforts to ensure that all tools offered safeguard customers' personal, proprietary, and location information.

Principle #2 – Implement STIR/SHAKEN. Implement STIR/SHAKEN call authentication.

Principle #3 – Analyze and Monitor Network Traffic. Analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls.

Principle #4 – Investigate Suspicious Calls and Calling Patterns. If a provider detects a pattern consistent with illegal robocalls, or if a provider otherwise has reason to suspect illegal robocalling or spoofing is taking place over its network, seek to identify the party that is using its network to originate, route, or terminate these calls and take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating commercial customer owns or is authorized to use the Caller ID number, determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name, terminating the party's ability to originate, route, or terminate calls on its network, and notifying law enforcement authorities.

Principle #5 – Confirm the Identity of Commercial Customers. Confirm the identity of new commercial VoIP customers by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business.

Principle #6 – Require Traceback Cooperation in Contracts. For all new and renegotiated contracts governing the transport of voice calls, use best efforts to require cooperation in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered its network or by identifying its own customer if the call originated in its network.

Principle #7 – Cooperate in Traceback Investigations. To allow for timely and comprehensive law enforcement efforts against illegal robocallers, dedicate sufficient resources to provide prompt and complete responses to traceback requests from law enforcement and from USTelecom's Industry Traceback Group. Identify a single point of contact in charge of responding to these traceback requests and respond to traceback requests as soon as possible.

[11] The principles also include an introduction, definitions, a disclaimer, and signatories not included in this appendix. The full State Attorneys General Anti-Robocall Principles is available at: https://www.ustelecom.org/wp-content/uploads/2019/08/State-AGs-Providers-AntiRobocall-Principles-With-Signatories.pdf.

Principle #8 – Communicate with State Attorneys General. Communicate and cooperate with state Attorneys General about recognized scams and trends in illegal robocalling. Due to the ever-changing nature of technology, update the state Attorneys General about potential additional solutions for combatting illegal robocalls.