Adoption

of

Caller ID Authentication Technology and Other Techniques

to

Combat Robocalls
by Policymakers and Providers

in

Countries outside the United States

NANC Call Authentication Trust Anchor Working Group

Table of Contents

Adoption of Caller ID Authentication Technology and Other Techniques to Combat Robocalls by Policymakers and Providers in Countries outside the United States

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 recommend steps to encourage adoption of caller ID authentication technology and other techniques to combat robocalls by policymakers and providers in countries outside of the United States (U.S.), especially when that adoption would benefit U.S. consumers. Specifically, they directed the NANC to address the following:

1. Provide observations on progress made towards combatting robocalls in other countries, and the effect this progress, or lack thereof, has on U.S. consumers.
2. Identify whether foreign voice service providers and/or other countries have adopted caller ID authentication technologies, whether under the STIR/SHAKEN framework or under different frameworks.
   - Provide observations about the level of deployment of caller ID authentication technology in other countries, and how such deployment affects the ability of U.S. providers to combat robocalls terminating to U.S. consumers from overseas.
   - Provide available detail about the successes or difficulties experienced with the various technologies deployed.
   - Where relevant, identify whether there are barriers to the exchange of caller ID authentication information between different systems.
   - If there are such barriers, recommend how these barriers can be overcome.

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

3. Recommend specifics on how the STIR/SHAKEN framework can be used by U.S. voice service providers and intermediate providers to combat illegal robocalls originating outside the United States and received by U.S. consumers.
4. Recommend steps the Secure Telephone Identity Governance Authority and other members of the industry can take to encourage the adoption of caller ID authentication technology—including the STIR/SHAKEN framework—in other countries.
5. Recommend whether Commission engagement with other countries could be helpful to encourage the adoption of caller ID authentication technology—including the STIR/SHAKEN framework.
    - If such engagement is recommended, identify priority countries for engagement and suggest specific steps and/or technical capacities that would promote successful implementation.

2. Report

The Wireline Competition Bureau's (WCB) third charge to the NANC CATA WG in its June 15, 2021, letter – to address adoption of caller ID authentication in countries outside the United States (US) – is apt because the majority of suspected illegal robocallers are located outside the U.S. There are multiple categories of calls that originate outside of the U.S., including calls with a U.S. number in the caller ID, and calls with non-U.S. numbers in the caller ID. In addition, a subset of calls with a U.S. number in the caller ID are from U.S. mobile customers roaming internationally. The recommendations in this report apply to all three categories because the full benefits of caller authentication are only realized if all calls are authenticated by the originating service provider. Robocalls are not just a U.S. problem anymore. They are a growing international problem and other countries are more likely to cooperate if solutions address calls that terminate internationally as well. This report recommends actions to accelerate the widescale deployment of robocall mitigation tools.

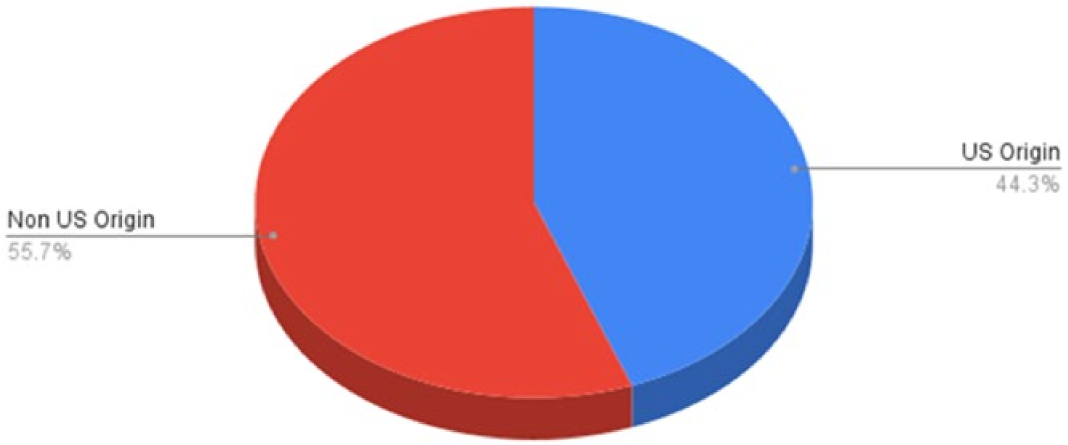
Many illegal robocalls targeting U.S. customers originate from overseas using U.S. caller IDs, typically through spoofing. Based on data compiled by the USTelecom-led Industry Traceback Group (ITG) between October 2021 and February 2022, almost 56% of suspected illegal robocalls traced back by the ITG were made by callers abroad. [2] During the same period, almost 60% of tracebacks of suspected

[2] ITG traceback results are driven by the campaigns that the ITG prioritizes, as well as the accuracy of the information provided by the voice service providers in response to traceback requests. In the ITG's experience, fraudulent robocalls, such as impersonations of government agencies and technical support scams, more often originate from other countries than from the U.S. Extreme high-volume lead generation robocall campaigns that violate U.S. telemarketing laws, most often by transmitting prerecorded messages without consent, commonly originate in the U.S. The ITG traces back both types of call campaigns, but typically prioritizes fraud campaigns. Note that the pie charts in Figures 1 and 2 reflect calls using U.S. North American Numbering Plan (NANP) numbers only.

illegal robocalls traced back by the ITG identified U.S.-based providers originating the calls (see Figure 1 below).[3] At times, callers physically located outside the U.S. use VoIP-based service providers located in the U.S. (or that are purportedly located in the U.S.) to initiate illegal robocalls through the Internet. There also are times that U.S.-based callers rely on VoIP-based service providers located outside of the U.S. to initiate illegal robocalls in the same manner (see Figure 2 below).

Figure 1

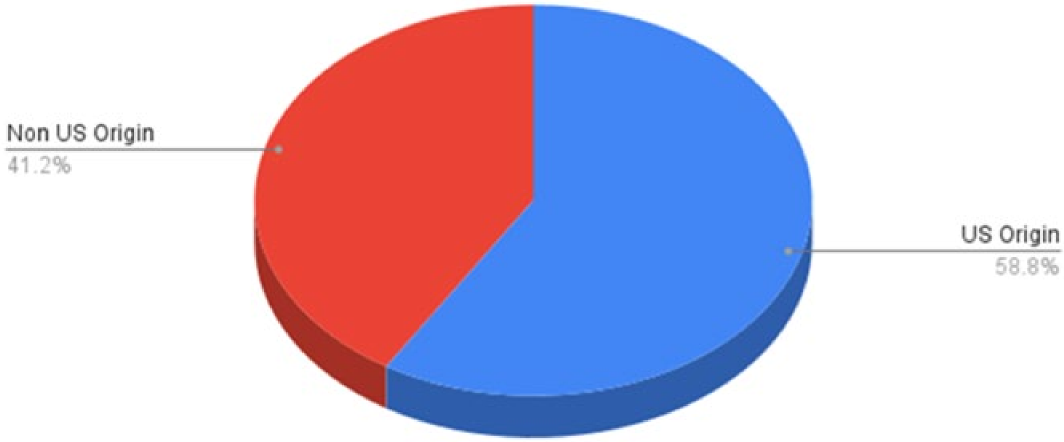
Robocall Traceback Origination by Caller Location
(October 2021 to February 2022)



[3] The ITG relies on the Commission's Robocall Mitigation Database, in addition to information submitted by a given provider and its downstream carrier, to designate the provider as U.S.-based or foreign. In the ITG's experience, at times providers identified in tracebacks have limited or no U.S. physical presence, operations, or principals, but nevertheless purport to be U.S.-based and sometimes establish U.S.-based corporate entities.

Figure 2

Robocall Traceback Origination by Originating Service Provider Location
(October 2021 to February 2022)



While greater ubiquity of STIR/SHAKEN adoption in the U.S. will have beneficial network effects, illegal robocalls are a global issue that can only be addressed through greater international engagement. The following sections of the report address the specific questions posed by the WCB based on input from CATA WG members and third-party presenters.

2.1. Progress made towards combatting robocalls in other countries, and the effect this progress, or lack thereof, has on U.S. consumers

Illegal robocalls are a growing problem internationally – not just in the US. Several foreign countries have adopted regulations or published guidelines related to Calling Line Identification (CLI) for calls with a caller ID associated with their country code, primarily aimed at domestic traffic. As a result, the actions taken in other countries to date do not measurably benefit U.S. consumers, either with respect to foreign-originated traffic terminating in the U.S. or U.S.-originated traffic terminating in foreign countries.

STIR/SHAKEN has been broadly deployed in Canada for VoIP traffic and discussions between the STI-GA in the U.S. and the Canadian Secure Token Governance Authority (CST-GA) in Canada have started to formally address cross-border STIR/SHAKEN. This would represent the first instance of official support for country cross-border call authentication.

Technical issues will need to be overcome and could be different with each country. End-to-end testing among service providers will be critical. When considering global STIR/SHAKEN expansion, broader testing[4] confirms that there is a strong likelihood that call authentication PASSporTs may be dropped in transit between countries, at least during initial deployments and where calls traverse multiple intermediate (or transit) service providers. There was a similar initial deployment problem in the U.S. until network equipment was correctly configured to not block SIP Identity headers at interconnection and peering points between networks. As a result, it is expected that this will also improve over time for cross-border traffic. More broadly, while different countries may ultimately adopt different call authentication solutions, it is understood that solutions must be interoperable and properly enabled in service provider networks to be effective. This is discussed in more detail in section 2.2.3.

Finally, it is worth noting that many countries that are in the process of considering or implementing STIR/SHAKEN, like the U.S. and Canada, do not have ubiquitous VoIP networks.

2.1.1. Status of efforts in different countries

In general, countries tackling caller ID authentication focus on addressing calls within their national borders and calls coming into their national networks to protect their consumers. There is a recognition that fully addressing the problem in the long term will include outgoing as well as incoming calls to and from other countries, but this is rarely the initial focus.

Australia:

The Australian Communications and Media Authority (ACMA) notes phone scams as among its compliance priorities for 2021-22. ACMA notes that its focus will include rules requiring telcos to "identify, trace and block scam calls" and to "use enhanced ID checks, such as multi-factor identification, when transferring mobile numbers from other providers." It is also noted that new ACMA rules require telcos to publish information for reporting scam calls, and to share information with other telcos and authorities.[5]

Belgium:

On December 4, 2020, the Belgian Institute for Postal Services and Telecommunications (BIPT) published CLI guidelines with four principles:

- Each call must be associated with a network number
- The network number must identify the caller in a unique manner
- The presentation number must be dialable
- The network and presentation numbers must be valid

[4] The ATIS Robocalling Testbed, hosted by Neustar, a TransUnion company, has conducted some testing of international connections and found configuration problems similar to those initially encountered in the U.S.

[5] https://www.acma.gov.au/publications/2021-09/report/action-telco-consumer-protections-april-june-2021 (last visited April 3, 2022).

The regulator is also proposing a "list of geographical numbers susceptible to fraud" and that these numbers would not be allowed to originate outside the country. (This would be similar to a Do Not Originate (DNO) Registry but applied at the gateway into the country.)

Canada:

Beginning in January 2018, the CRTC issued a number of decisions related to STIR/SHAKEN, culminating in CRTC 2021-123, issued April 6, 2021, confirming that all telecommunications service providers must implement STIR/SHAKEN in their IP-based networks as a condition of providing service. The mandated implementation deadline for STIR/SHAKEN in IP-based voice networks was set at November 30, 2021. In support of this mandate, the CRTC earlier issued CRTC 2019-403 on December 8, 2019, which approved the establishment of the CST-GA as the governance authority. The CST-GA developed criteria for SHAKEN participation to "ensure the integrity of the STIR/SHAKEN framework" and published this in a consensus industry report, as directed by the CRTC, on September 29, 2021. Subsequent to the implementation deadline, the Commission deferred STIR/SHAKEN for all 911 calls from end-users to Public Safety Access Points (PSAPs) and for call-backs from PSAPs to end-users, pending further analysis. For more details on the status of STIR/SHAKEN in Canada, refer to Appendix A.

France:

A French law aimed at tackling fraudulent calls, enacted on July 24, 2020, requires all carriers to implement technologies to authenticate CLI information to prevent call spoofing, within 36 months. ARCEP, the French regulator, established and chaired the MAN (Mechanisms for the Authentication of Numbers) Working Group of APNF (Fixed Number Portability Association) to develop a plan and published a report of their findings on December 16, 2021.

- MAN Working Group decision: The MAN Working Group completed a detailed analysis of options and concluded that they needed a mechanism that is commercially available now (to meet the tight timeframe) and standards-based (to ensure interoperability between service providers), leading them to select STIR/SHAKEN.
- Governance: The APNF (Fixed Number Portability Association) is tentatively planning to fill the governance authority role, but they insist that it is essential that "Public Authorities" (i.e., legislative, regulatory, and enforcement/legal) be involved in governance to make it effective.
- Cross-border: The report recognizes that spoofing and fraud are global problems that require global approaches. This implicitly acknowledges the need for cross-border call authentication, but the report does not take this idea any further. Their immediate concern is complying with the French law.

For more details on the status of call authentication in France, refer to Appendix B.

Germany:

The German Telecommunications Modernization Act (TKG) provided some approaches to combat CLI spoofing but did not provide the power to investigate and thus identify the person responsible.

A revised TKG came into effect on December 1, 2021, in which the German legislator – among other things to improve the situation regarding caller ID spoofing – chose a new approach for regulating duties and obligations relating to the transmission of numbers.

- If an incoming international call has a German number, the number must not be displayed. (There is an exception for mobile numbers.)
- There are new obligations for disconnecting calls for which "forbidden" numbers are displayed as the CLI, including premium numbers and emergency services numbers.
- The Bundesnetzagentur now has the power to prosecute.

Ireland:

Ireland's telecoms regulator, the Commission for Communications Regulation (ComReg) announced the formation of the Nuisance Communications Industry Taskforce (NCIT) in information notice ComReg 21/129 issued December 17, 2021. It defined "nuisance communications" as "unwanted, unsolicited communications … often having the intent to mislead the receiver, so that they unknowingly provide sensitive information … which can enable the criminal to perpetrate fraud". The notice identified two related problems: 1) consumers are being defrauded, and 2) business calls are not being answered because consumers are losing trust in electronic communications services. Problem calls are happening with increasing frequency – a poll conducted for *The Journal* found that 75% of Irish adults had received a scam call from an Irish number in the previous month. As result, the taskforce could look at ways to block numbers which "clone" Irish numbers from abroad.

The NCIT will bring together representatives of organizations operating under a General Authorization to carry voice calls and/or text messages in Ireland and will meet monthly. The NCIT will produce two progress reports, one after six months and the second after 12 months. The first meeting was held in late January 2022.

The NCIT terms of reference include the following objectives:

- Identify and recommend practical interventions that can be taken in a short, medium, and long-term timeframe to combat nuisance communications.
- Develop an intervention implementation roadmap to ensure that the interventions are implemented by the appropriate network and/or service providers as quickly as possible.
- Develop an effective means for industry to collaborate and share information over the long term should nuisance communications evolve.

The final report will recommend whether the taskforce should continue beyond the initial 12 months.

Latvia:

Latvia has used formal regulation to oblige operators to block calls where the A-number (calling number) has been manipulated, including cases when the end-user does not have the right to use the A-number or where the A-number is not routable.

CLI spoofing, including partial or full replacement of an A-number, is considered a numbering misuse and fraud in Latvia. Latvia's National Regulatory Authority (NRA) has developed a procedure regarding the elimination of fraud using numbering.

Norway:

In Norway, a formal regulation has been in place since 2013 obliging the operators to block, if technically possible and economically feasible, calls where the end-user does not have the right to use the A-number or where the A-number is not routable.

United Kingdom (UK):

Ofcom indicates that "using technology to fight fraud in the future" would involve authenticating caller ID information for calls originating in the United Kingdom and indicates that "this should be achievable once the UK's transition to digital landlines is complete."[6] Ofcom further indicates that BT and other service providers have made the decision to retire the Public Switched Telephone Network (PSTN) by 2025.[7] This suggests that we may not see regulatory directives for caller ID authentication in the UK for several years.

2.1.2. International call authentication frameworks and standards work

Sections 2.1.2.1 through 2.1.2.4 describe several potential frameworks for international call authentication expansion and summarize some key considerations. Call authentication frameworks include the cross-border exchange of PASSporTs, as well as the governance structure.

2.1.2.1. Jurisdictional STIR/SHAKEN framework

The STIR/SHAKEN call authentication framework could continue to expand globally using the established jurisdictional approach as followed by the U.S. and Canada. In this approach, each participating country or group of countries/coalition would establish the equivalent of an STI-GA and STI-PA, along with one or more approved STI-CAs to administer the allocation of STI certificates for signing PASSporTs. The governance authority would also have a partnership with the regulator(s). Authorized voice service providers would then sign and verify PASSporTs in compliance with

[6] https://www.ofcom.org.uk/news-centre/2022/crackdown-on-fake-number-fraud (last visited April 9, 2022).

[7] https://www.ofcom.org.uk/news-centre/2021/upgrading-landlines-to-digital-technology (last visited April 9, 2022).

published IETF and ATIS standards, thereby enabling interoperability between service providers. As noted above, this approach can allow multiple countries to potentially share a common governance and policy administration framework. Note also that establishing STIR/SHAKEN within a given jurisdiction does not automatically result in cross-border calls being authenticated in other jurisdictions. The respective governance authorities should first agree to expand their zone-of-trust to include the other jurisdiction, as discussed in section 2.3.

2.1.2.2. Jurisdictional STIR framework

Some participating countries may not embrace all aspects of the call authentication framework as recommended or standardized by SHAKEN. Such approaches may differ in how the national governance and policy management framework is established and/or to what level the ATIS SHAKEN standards for PASSporT signing and verifying are adopted. The differences between these STIR-based approaches and the jurisdictional approach followed by the U.S. and Canada for STIR/SHAKEN may create interoperability challenges.

2.1.2.3. Non-jurisdictional STIR/SHAKEN framework

A non-jurisdictional (global) STIR/SHAKEN call authentication framework is another approach that could support international expansion. Such a framework would follow the same ATIS standards as STIR/SHAKEN in the U.S. and Canada, but the governance and policy management would not be linked to a single country (or jurisdiction). The governance and policy management would be consistent with STIR/SHAKEN recommendations and standards and all service providers would be rigorously vetted to ensure compliance with the STIR/SHAKEN foundational principles of "inclusiveness, security, and accountability." Authorized service providers would sign and verify PASSporTs in compliance with published IETF and ATIS standards. Compliance with IETF and ATIS standards would simplify PASSporT interoperability between service providers. Non-jurisdictional call authentication frameworks may not be able to rely on the regulatory/legal enforcement generally available to a jurisdictional STIR/SHAKEN framework, and therefore will need to implement other mechanisms that have the same effect. These mechanisms could include policies, processes, and/or monitoring tools, but they must be well-defined, transparent, and effective to protect the security and accountability of the STIR/SHAKEN ecosystem. Non-jurisdictional STIR/SHAKEN call authentication frameworks will also need to be open and transparent about their processes to allow jurisdictional STIR/SHAKEN frameworks to conduct an accurate assessment before agreeing to trust them. For example, non-jurisdictional call authentication frameworks could include 3rd party audits, a neutral review/appeal board or a requirement to register with the FCC or other national regulators to increase confidence in their reliability.

2.1.2.4. Non-jurisdictional "STIR/MIXER" (Mobile IntereXchange Encompassing Roaming) framework

One non-jurisdictional approach for extending the global call authentication framework is to build on ongoing work in the Validating INtegrity of End-to-end Signaling (VINES) Working Group under the GSMA Fraud and Security Group (FASG). VINES is looking at a series of security threats confronting mobile operators today. The GSMA Diameter End-to-end Signaling Security (DESS) Working Group, also in FASG, is chartered to explore how cryptographic keys can be shared between operators to facilitate 5G roaming. This includes bilateral connections between operators for Diameter signaling, for example, which requires digital certificates.

Mobile operators today share roaming information with each other through an IR.21 document.[8] To publish an IR.21, GSMA verifies an operator's spectrum and "vets" you as a legitimate operator. Assigned Telephone Number (TN) ranges and Mobile Country Code/Mobile Network Codes (MCC/MNCs) are then built into IR.21s, along with other data. Mobile operators could just share a digital certificate in their respective IR.21. DESS has its own requirements for certificate revocation and key lifecycle management.

Given this ongoing work in FASG, it is feasible to look at this as a potential international mobile operator approach for STIR cryptographic keys. With this approach, one would need to specify a way for STIR to refer to cryptographic keying material published in the IR.21. One would then sign PASSporTs with these self-signed digital certificates bilaterally between agreeing operators. This would likely impose minimal cost since it would be re-using a keying system already being implemented for roaming.

GSMA could ultimately "bless" one or more CAs to issue digital certificates for the public keys of operators who publish their DESS keys through the IR.21. CAs would conform to a Certificate Policy (CP) effectively set by the GSMA (like an STI-PA). CA practices would rely heavily on the existing full membership enrollment in GSMA (a prerequisite for using IR.21). The premise is that if the enrollment is good enough to secure roaming, then it should be good enough to secure PASSporT signing.

For more details on the "STIR/MIXER" approach, refer to Appendix C.

2.1.2.5. Call authentication framework considerations

Based on available information to date, it is unlikely (and impractical) that all countries will adopt the same jurisdictional call authentication approach adopted by the U.S. and Canada for STIR/SHAKEN.

[8] The IR.21 document specifies a common and simple overview of the most important data related to International Roaming. The Roaming Agreement Exchange (RAEX) is a real-time system that gives access to the data of a partner's IR.21, including updates. See also "GSMA Roaming Database, Structure and Updating Procedures."

Thus, interoperability between the frameworks adopted will require a number of administrative and technical areas of alignment. All approaches must ensure accountability by implementing a well-defined mechanism to identify bad actors, revoke their credentials, and a defined process to coordinate with the appropriate enforcement agencies to take action. There are multiple key areas of alignment that are likely to be relevant across all the discussed frameworks.

First, the STIR/SHAKEN call authentication framework assumes that service providers have some sort of assigned Service Provider Code (SPC) that is a unique identifier. In the North American context, this is an Operating Company Number (OCN). Outside North America, other sorts of identifiers are either used or would need to be identified for the required TN Authorization List extension in a STI certificate. These could include an established Public Land Mobile Network (PLMN) code for mobile carriers (the MCC/MNC), already established country-specific service provider identifiers, global identifiers such as through the Global Legal Entity Identifier Foundation (GLEIF) organization, or even greenfield identifiers established specifically for STIR/SHAKEN. To foster international interoperability, these identifiers should be consistent (within the country) and publicly recognizable codes, rather than opaque, proprietary identifiers.

Second, at the core of most interoperability models is the notion that every participating ecosystem will maintain a list of approved CAs (if more than one) that can issue STI certificates for signing PASSporTs, and that those lists would then be mutually exchanged and trusted between ecosystems. The key to establishing this trust is the satisfactory establishment of Certification Policies which address the circumstances under which STI certificates will be issued (and potentially revoked) in these ecosystems. To foster international interoperability, it is recommended that ecosystems seeking to interoperate with the U.S. have, at a minimum, the following:

- A clear vetting policy for service providers and, if applicable, non-service provider entities that can participate in their call authentication ecosystem and be issued STI certificates;
- A documented and exercisable traceback process for suspect and/or illegitimate calls; and
- Well-defined mechanism(s) to identify and resolve misuse of call authentication (e.g., illegitimate calls receiving full attestation) and to cooperate with enforcement in the case of fraud or other illegal activity.

Third, a more technical aspect of necessary alignment among call authentication frameworks is agreement on how to handle variations in the way that calling party information may be conveyed in SIP headers across various jurisdictions and environments. For example, in some countries, the SIP P-Asserted-IDentity (PAID) header is not used to convey the calling party TN that should be rendered to the called party (i.e., the “presentation” number). Instead, the PAID header contains a “network” number that must not be rendered to a called party. In order for a PASSporT to be meaningful across national boundaries, originating and terminating service providers must agree on what parts of SIP signaling are mirrored as the calling party TN (i.e., the “orig” claim in a PASSporT). There are also various categories of presentation numbers that, in some jurisdictions, will not map cleanly into the levels of SHAKEN attestation. While there are potential workarounds for some of these variations, reaching technical alignment will be necessary across SIP ecosystems to achieve genuine interoperability.

Finally, interoperability must accommodate multiple jurisdictional and non-jurisdictional call authentication framework approaches. Although the initial deployment of STIR/SHAKEN in both the U.S. and Canada is supported by national regulatory mandates, non-jurisdictional framework approaches may need incentives for service providers to participate in the absence of country-specific regulatory mandates. For example, an international service provider that is not eligible to directly participate in the established U.S. STIR/SHAKEN ecosystem and originates a significant volume of legitimate calls terminating in the U.S., may benefit by proactively adopting a non-jurisdictional call authentication framework approach. Non-jurisdictional frameworks enhance "inclusiveness," but they may not be able to count on the regulatory/legal backstops available to jurisdictional frameworks and will therefore require well-defined mechanisms to ensure the "security" and "accountability" of the SHAKEN ecosystem.

2.2. Status of foreign voice service providers and/or other countries adoption of caller ID authentication technologies, whether under the STIR/SHAKEN framework or under different frameworks

Canada:

Per CRTC mandate, the CST-GA was established to govern the deployment of STIR/SHAKEN in Canada. Subsequently, the CST-GA selected an STI-PA, an initial STI-CA vendor, and a policy and certificate management solution was successfully deployed by the required September 30, 2020, date. The deadline for mandated deployment of STIR/SHAKEN by all telecommunications service providers was November 30, 2021, and a growing number of IP-based calls are being authenticated using STIR/SHAKEN.

France:

French law enacted on July 24, 2020, requires all carriers to implement technologies to authenticate CLI information, preventing call spoofing, within 36 months. Relying on this legal framework, ARCEP formed the MAN working group to discuss the best way to comply with the law. The MAN working group completed a detailed analysis of options and selected STIR/SHAKEN. The report provides a detailed project plan to support the required in-service date of July 24, 2023. The APNF is tentatively planning to fill the governance authority role, at least initially.

Ireland:

In January 2022 Ireland's telecoms regulator, ComReg, launched a NCIT taskforce to recommend practical actions that can be taken to combat nuisance communications. The NCIT will provide an interim report to ComReg mid-year and a final report early in 2023. Although the taskforce terms of reference do not identify a specific technology, there is a recognition that many nuisance calls with Irish numbers in the caller ID originate outside of the country. This aligns with the assessment in this report and suggests that there may be value in collaborative discussions to develop complementary approaches to combatting nuisance communications.

2.2.1. Level of deployment of caller ID authentication technology in other countries, and how such deployment affects the ability of U.S. providers to combat robocalls terminating to U.S. consumers from overseas

STIR/SHAKEN has already been deployed in Canada and is planned for deployment in France by July 2023. Currently, each country has its own independent “zone-of-trust,” meaning, in general, that calls authenticated in one country cannot be verified in the other. See section 2.3.1 for a discussion of near-term technical approaches that can facilitate cross-border call authentication. Discussions between the STI-GA in the U.S. and the CST-GA in Canada have started and are expected to expand the “zone-of-trust” to allow all signed cross-border calls between the U.S. and Canada to be successfully verified. A similar approach could be taken with France, once a French governance authority is established, to allow caller ID authentication among the three countries. This approach can then be extended to other national deployments of SHAKEN as they occur.

In addition, non-jurisdictional approaches discussed in section 2.1.2 could be used to further expand the zone-of-trust if they were judged to be consistent with the foundational principles discussed in section 2.5.

2.2.2. Successes or difficulties experienced with the various technologies deployed

Various call authentication mechanisms have been proposed, studied, and in some cases implemented. To date, the only approach to achieve widespread, multi-vendor deployment in live networks is STIR/SHAKEN.

The results of the French MAN WG study (see section 2.1.1 of this report) are instructive. A number of possible caller ID authentication mechanisms were evaluated but, in the end, the MAN WG concluded that STIR/SHAKEN was the only viable approach because it is:

- **Standards-based**: ensures that independent implementation by various service providers will interoperate, and not be limited to a single vendor; and
- **Commercially available**: the tight implementation timeline required by the French legislation led them to prioritize approaches that were proven in live networks and available from multiple vendors.

2.2.3. Barriers to the exchange of caller ID authentication information between different systems, and where they exist, how they can be overcome

Caller ID authentication is inherently end-to-end. As such, the information flow must be end-to-end. An originating service provider has the most detailed information about the caller and their right to use the caller ID (i.e., the TN), and is therefore in the best position to vouch for the caller ID. This caller ID information is then made available to the terminating service provider to help the called party assess the credibility of the caller. While end-to-end information flow is easiest when both the originating and terminating service providers use the same standards-based mechanism (i.e., no translation is required), it is still possible to have an end-to-end information flow when different mechanisms are used at the origination and termination of a call. The jurisdictional approaches discussed earlier in this section define where a translational boundary might occur, not unlike the role of international gateways for calls that transition from one country-specific jurisdiction or regulatory domain to another. The industry would need to define similar points where one call authentication approach can transition to another.

The most effective way to "overcome barriers to the exchange of caller ID information" is to encourage use of a consistent standards-based approach, such as STIR/SHAKEN to avoid complexities at the jurisdictional boundaries. Although some translation is likely unavoidable, having common characteristics and similarities to STIR/SHAKEN, such as use of trusted root certificates and easily translatable frameworks, is highly recommended.

2.3. Recommendation on how the STIR/SHAKEN framework can be used by U.S. voice service providers and intermediate providers to combat illegal robocalls originating outside the United States and received by U.S. consumers.

Because of the end-to-end nature of the STIR/SHAKEN framework, combatting illegal robocalls originating outside the U.S. will require deployment of an interoperable framework by international carriers. Until international carriers implement a caller ID authentication technology, either by themselves or through a third party, there will not be an end-to-end approach for call authentication for calls that originates/terminates outside the U.S. Once STIR/SHAKEN, or another compatible call authentication mechanism, is deployed internationally, the STI-GA can begin the process of working with international peers on mutually accepted policies for authenticating international calls. This will require consideration of the following:

- **Protocol interoperability**: *(Largely defined)* The basic elements of STIR/SHAKEN interoperability are defined, though it will be necessary to select a suitable Service Provider Code identifier to use instead of the Operating Company Number (OCN).
- **Trust Anchor**: *(Largely defined)* [ATIS-1000087] defines a mechanism to add other country STI-CAs to the list of trusted CAs, but only after approval by the governance authorities. An

update to [ATIS-1000087] is required to address merging of Certificate Revocation Lists (CRLs).

- **Authorization**: *(Partially defined)* The U.S. STI-GA is responsible for maintaining the integrity of the SHAKEN ecosystem in the United States, and therefore must authorize merging another trust anchor into the ecosystem. The authorization process is not yet defined, but discussions between the STI-GA in the U.S. and the CST-GA in Canada have started and may provide a template for future additions.
- **Trust criteria**: *(Purposely Undefined)* The criteria for one governance authority to trust another governance authority in the SHAKEN framework is intentionally not defined by the standards as it is a policy matter. It is the responsibility of each governance authority to maintain the integrity of the SHAKEN ecosystem within their respective domain and to determine how they will support the foundational principles of inclusiveness, security, and accountability. While this has not been defined by the standards it needs to be defined by each governance authority as part of governance policies.

2.3.1. Example of cross-border SHAKEN (U.S./Canada)

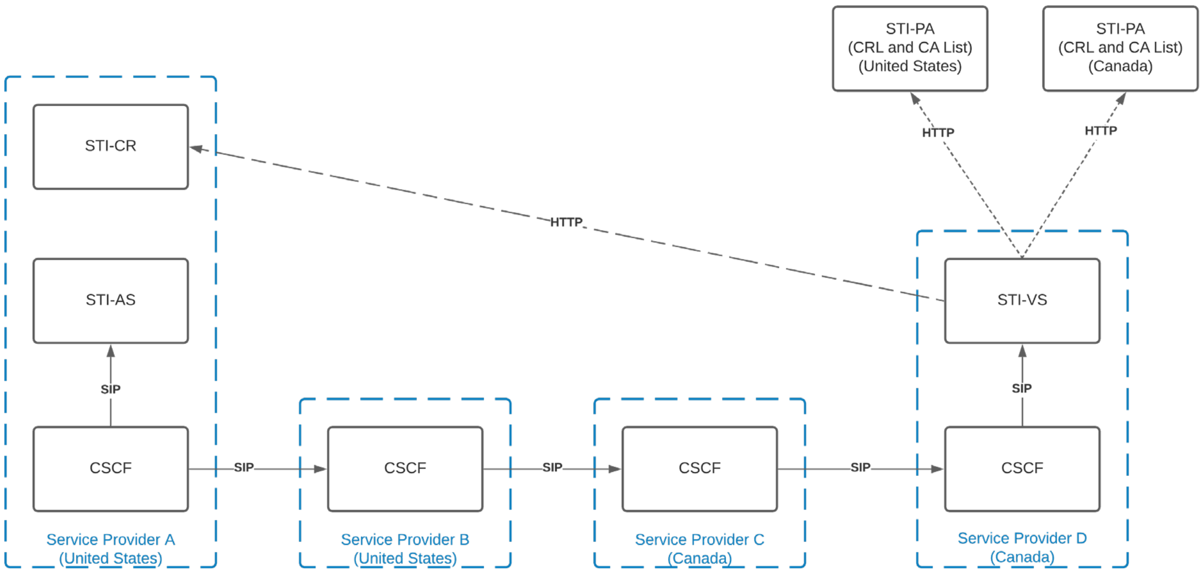
Cross-Border SHAKEN

[ATIS-1000087] and [ATIS-1000091], respectively, present short- and longer-term frameworks for supporting both international (+1 country code), as well as other international country codes or regulatory domains. These proposed frameworks assume STI-GA collaboration, policy agreements and modest STI-PA platform developments to recognize and jointly enable SHAKEN across national borders.

However, as of October 22, 2021, STI-PAs in the U.S. and Canada made their approved SHAKEN Certificate Authority (CA) Lists and indirect Certificate Revocation Lists (CRLs) available to the public, consistent with [ATIS-1000080] and [ATIS-1000084]. This allowed vendors to implement technical solutions to support SHAKEN between the two countries in advance of formal agreement from the respective STI-GA/STI-PAs. Figure 3 illustrates a solution architecture for SHAKEN calls originating in the U.S. and terminating in Canada. Note that a similar architecture applies for the reverse call direction.

Figure 3

Cross-Border SHAKEN (U.S. and Canada)



Several vendors have deployed solutions for their service provider customers consistent with the above architecture, and with acknowledgment by the U.S. and Canadian governance authorities. Note that this technical approach is not intended to be a replacement for [ATIS-1000087] but a description of what is currently possible and being used to authenticate such calls today. For some calls, the above architecture has also been adapted and deployed for non-IP SHAKEN cross-border calls.

Before enabling cross-border SHAKEN, service providers, and other vested entities, should take the following actions:

1. Ensure that current governance authority policies support the signing of calls destined for the other country (e.g., can a Service Provider Code Token and associated STI Certificate issued in one country be used to sign calls destined for the other country?)
2. Service providers (and/or their vendors) should decide if they will accept PASSporTs from the other country before the governance authority has formally decided to accept PASSporTs from the other country (this could lead to non-uniform deployments where Service Provider A accepts PASSporTs from the U.S. (or Canada) while Service Provider B does not)
3. Service providers (and/or their vendors) need to properly integrate with the U.S. and Canada STI-PA APIs for the public CA List and indirect CRL (note that the Canadian APIs are currently publicly accessible for these, while the U.S. APIs still require IP whitelisting –

however, since October 22, 2021, the U.S. STI-PA now provides public access to these through a web portal)

2.4. Steps the Secure Telephone Identity-Governance Authority (STI-GA) and other members of the industry can take to encourage the adoption of caller ID authentication technology—including the STIR/SHAKEN framework—in other countries.

The U.S. STI-GA makes its policies, procedures, and webinars publicly available on the ATIS website: https://sti-ga.atis.org/. The U.S. STI-GA worked closely with Canada as they were setting up their own governance and policy management process. The U.S. STI-GA had open communications with Canada during the process and communications continue as cross-border exchange processes are being developed. The U.S. STI-GA welcomes the opportunity to work with other countries adopting caller ID authentication.

As noted in this report, only a few countries are starting to take steps to develop their own caller ID authentication processes. While it may not be necessary for every country to develop the STIR/SHAKEN framework, it will be necessary to develop the appropriate interfaces to exchange information and ensure trust by developing appropriate traceback and enforcement processes.

It is recommended that either by itself or with the CST-GA, the U.S. STI-GA develop a webinar and/or report on resources available, document Canadian/U.S. coordination, and define key considerations for implementation (e.g., interoperability and enforcement handoffs). It is important that the purpose of policies and processes be explained so that each country can easily review key considerations, if applicable. For example, criteria to determine which entities can perform the call authentication process in each country, as well as the SPC Token access policy, must be well understood. In the U.S., the purpose of the SPC Token access policy is to be as inclusive as possible while protecting the security of the ecosystem. The criteria requires that the service provider have a registered OCN which could be revoked by the issuer, is a current Form 499-A filer (for calculating an annual fee) and has certified in the FCC's Robocall Mitigation Data Base. Other countries are likely to have different criteria that govern which entities are eligible to access an SPC Token.

It is recommended that the U.S. STI-GA develop criteria under which international trust anchors implement cross-border STIR/SHAKEN (e.g., criteria for sharing CRLs and trusted CA root certificates).

2.5. Recommendation for Commission engagement with other countries to encourage the adoption of caller ID authentication technology—including the STIR/SHAKEN framework – and sharing of best practices and enforcement strategies.

As noted above, industry representatives have discussed STIR/SHAKEN implementation with international peers and participated in international forums addressing caller ID authentication. Further, certain international regulators are already imposing some level of caller ID authentication requirements domestically. Caller ID authentication, however, can only be effective if implementation is interoperable and enforceable across international boundaries.

It is recommended that the FCC reach out to its international counterparts to collaborate on solutions and, where appropriate, encourage adoption of principles for caller ID authentication and other robocall mitigation tools that will facilitate expanding the "zone-of-trust" without compromising the integrity of the ecosystem. This includes:

1. Encouraging adoption of caller ID authentication that is interoperable with the STIR/SHAKEN standards implemented in the U.S. and Canada;
2. Encouraging establishment of a governance structure (e.g., similar to the U.S. and Canada based on [ATIS-1000080] and [ATIS-1000084] standards) and adoption of criteria that are consistent with the underlying caller ID authentication principles of inclusiveness, security, and accountability;
3. Encouraging cooperation among national authorities and global service providers and identifying impediments that may limit cooperation and ability to collaborate on enforcement;
4. Entering into MOUs to share best practices and enforcement strategies as appropriate; and
5. Educating foreign regulators on STIR/SHAKEN implementation and other robocall mitigation tools including guiding foreign counterparts to willing U.S. experts for their input on lessons learned and approaches taken to date.
6. Encouraging foreign regulators to mandate cooperation in traceback.
7. Encouraging foreign regulators to identify regulatory roadblocks that limit service providers' willingness to implement robocall mitigation practices such as providing safe harbors for inadvertently blocking an occasional legal call.

2.5.1. Priority countries for engagement and technical capacities for successful implementation

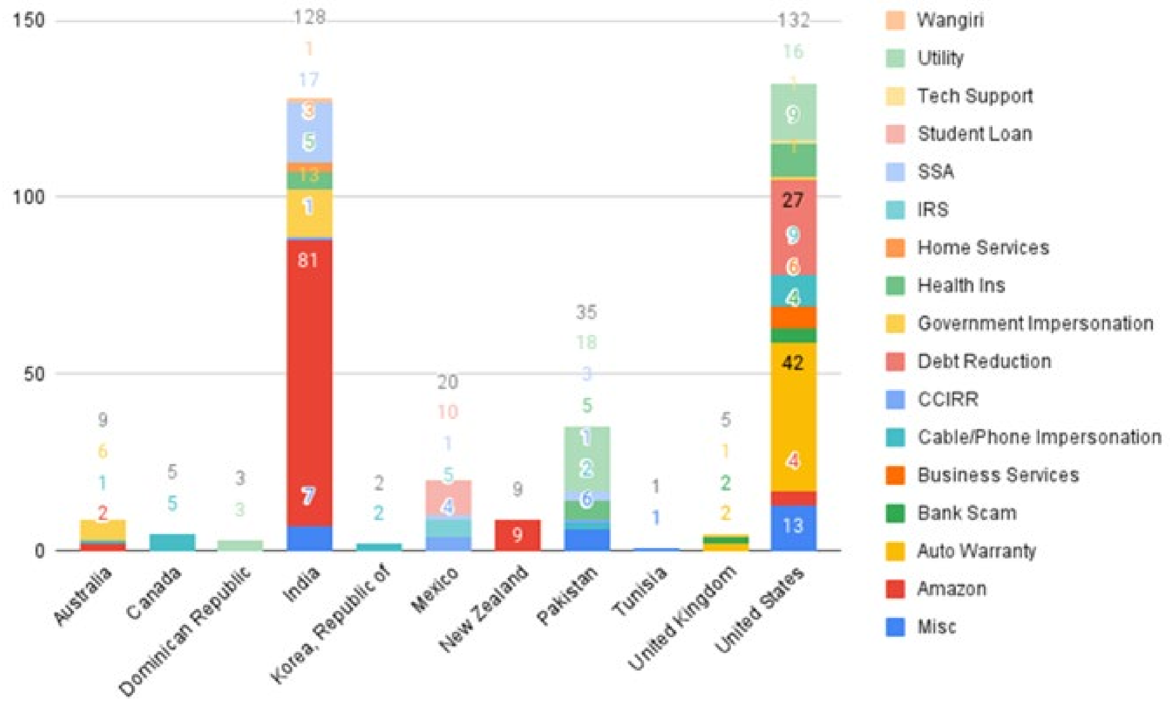
As noted throughout this report, there are two general problems to be addressed. One is ensuring there is a common or compatible framework that allows for the trust of call authentication information between domains (i.e., call authentication of jurisdictional traffic originating from a particular regulatory domain or industry ecosystem and terminating in another).

The second problem is the origination of international call traffic that has a U.S. caller ID, which, as noted earlier in this report, is a large source of suspected illegal robocalling traffic domestically. This is of great concern today and may be a growing problem due to the success of domestic call authentication and enforcement efforts to date. Interaction with foreign regulators and industry ecosystems for the purpose of encouraging implementation of call authentication requirements (and collaboration on enforcement) could help with both problems. Implementation of call authentication requirements by a threshold number of participants in the telephony ecosystem globally can encourage further implementation and expose when entities are not properly using call authentication. Such broader implementation can then aid in the consistent enforcement of the proper use of call authentication on all types of traffic.

The ITG tracks origination points of robocallers by campaign (see Figure 4 below). The caller origination point data for the period October 26, 2021, through January 3, 2022, shows that the vast majority of foreign-originated campaigns tracked by the ITG originated from callers in India. The next highest volume of calls originated in Pakistan. Engaging with regulators, as well as law enforcement in these countries, is important but should not be the sole focus of engagement by regulators or the industry in general. It is important for the FCC and other government agencies targeting illegal robocalls to take a broad approach to robocall mitigation because each country that adopts call authentication methods that are interoperable with STIR/SHAKEN creates momentum for further adoption of compatible standards.

Figure 4

Traceback Origination Points of Caller Country by Campaign (10/26/21-1/3/22)



Engagement with other countries should be prioritized based on the following:

- **Sources of fraudulent robocalls**: ITG traceback results can be used to identify the main sources of fraudulent robocalls and used to prioritize FCC and other U.S. government agency outreach. The latest results, as discussed in section 2 of this report, shows that most fraudulent robocalls originate outside the U.S., with the majority currently originating in India. In coordination with other federal partners, the FCC should continue to use ITG traceback results to identify countries for priority outreach in the future.
- **Existing relationships**: The FCC should continue to leverage existing relationships to share experiences and highlight the benefits of STIR/SHAKEN as opportunities arise. It will be beneficial to coordinate with countries that have already deployed SHAKEN (e.g., Canada), countries that are in the process of deploying SHAKEN (e.g., France) and countries that are actively evaluating mechanisms to combat nuisance calls (e.g., Ireland) to cooperate in developing compatible caller ID authentication approaches. The FCC should continue to monitor international activities to evaluate or deploy caller ID authentication and engage with these countries to coordinate robocall mitigation action.

3. 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] defines this claim and permitted values.

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 caller ID, used in a call.

Caller Identity (Caller ID) - 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.

Certificate Revocation Lists (CRL) – A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire. [RFC4949]

Certificate Policy (CP) - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. [RFC3647].

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

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 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.

Intermediate Service Provider (or Intermediate Provider) – The term Intermediate Service 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)

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]

SIP – Session Initiation Protocol is the foundational signaling protocol for creating, modifying, and terminating voice calls on internet protocol (IP) networks. [RFC3261]

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]

Terminating Service Provider (TSP) – The voice service provider of the called party. The TSP performs the STIR/SHAKEN verification function.

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

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 sharing that information to the service provider 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 and/or throughout the life of a contract.

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) and/or throughout the life of a service subscription or contract (i.e., the ongoing evaluation of traffic patterns indicative of abusive robocalling). TNs are not part of the vetting process and are covered by the TN Validation process.

Vetted – The successfully verified result of a vetting activity.

Voice Service Provider (VSP) – A 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 the STIR/SHAKEN Authentication function when acting as the OSP and the STIR/SHAKEN Verification functions when acting as the TSP. [ATIS-1000089]

Appendix A – Supplemental information about Canada

In January 2018 the CRTC issued CRTC 2019-32 which stated that STIR/SHAKEN "should be implemented" for all IP calls and that the CRTC "expects, by 31 March 2019, that (service providers) will implement measures to authenticate and verify caller ID for all IP-based voice calls". This decision also stated that the CRTC expects the "telecommunications industry will establish a Canadian certificate administrator."

CRTC 2019-402, issued December 9, 2019, established an implementation deadline of September 30, 2020, for implementation of STIR/SHAKEN for IP-based voice calls. The decision also required service providers to submit action plans and implementation reports tracking deployment progress.

In 2018 and 2019, the Canadian Local Number Portability Consortium (CLNPC) developed a proposal to establish a Canadian STIR/SHAKEN Governance Authority (GA) consistent with the governance model established in [ATIS-1000080], with the same shareholders as the CLNPC. CRTC 2019-403, issued on December 9, 2019, approved the establishment of the Canadian Secure Token Governance Authority (CST-GA) as a GA to support the implementation of the STIR/SHAKEN framework in Canada. The CRTC requested that the CST-GA select a PA and one or more CAs. In July 2020 the CST-GA selected Neustar, a TransUnion company, as the STI-PA, and also to provide STI-CA services. The STI-PA and STI-CA functions were operational by September 30, 2020.

CRTC 2019-402-2, published September 15, 2020, considered industry input requesting that the required STIR/SHAKEN mandate be postponed, and the CRTC approved an extension of the deadline for the implementation of STIR/SHAKEN (for IP-based voice calls) by nine months to June 30, 2021.

CRTC 2021-123, issued April 6, 2021, confirmed that all service providers must implement STIR/SHAKEN in their IP-based networks as a condition of providing service, concluding that the burden of upgrading the IP portion of their networks to support STIR/SHAKEN, even for smaller service providers, is outweighed by "the important and ever more urgent objective of ensuring an effective caller ID authentication system in order to reduce the harm caused by nuisance calls." However, in light of some technical and policy issues that had yet to be resolved, the CRTC pushed back the now mandated implementation deadline for STIR/SHAKEN in IP-based voice networks to November 30, 2021.

CRTC 2021-267, issued August 5, 2021, recognized that restricting STI certificates to service providers with direct access to numbering resources could result in constraints for non-eligible service providers complying with the CRTC's requirement for all service providers to implement STIR/SHAKEN. The CRTC further noted that "a policy that precludes an entire category of (service providers) from direct access to STI certificates, based solely on the type of (service provider), could result in a competitive (dis)advantage for those (service providers) that do not have such access". The CRTC therefore directed the CST-GA to initiate a collaboration with all service providers ("eligible" and "non-eligible") to revise eligibility criteria for access to STI certificates. The CST-GA was given

60 days to develop revised eligibility requirements that "prevent access to STI certificates only to those (service providers) that cannot be trusted to maintain the integrity of the STIR/SHAKEN framework."

The CST-GA delivered a consensus industry report, as directed by the CRTC, on September 29, 2021, proposing criterial to allow previously "non-eligible" service providers to participate in the STIR/SHAKEN framework in Canada. This report noted that expanding eligibility was based on the following principle:

"The criteria for participation in the Canadian STIR/SHAKEN framework are intended to maximize participation while still ensuring the integrity of the STIR/SHAKEN system. This will depend on a robust system for monitoring and enforcing compliance with all CST-GA certificate use policies."

The unanimous industry consensus requirements developed in this collaboration required service providers to address the following:

- **Identity**: proving "you are who you say you are" and that you are eligible to provide voice services in Canada.
- **Reputation**: provide information to "assure the regulator, the industry, and the general public of its commitment to provide secure attestation of caller identity in telecommunications".
- **Technical**: provide information to establish a technical ability to comply with STIR/SHAKEN specifications and best practices.

Finally, on November 1, 2021, the CRTC noted that it had received an application for a deferral of STIR/SHAKEN specific to 9-1-1 calls, which resulted in CRTC 2021-426 on December 20, 2021. In this decision the CRTC concluded that:

1. In light of the above, the Commission finds that implementing STIR/SHAKEN on 9-1-1 calls at this time could result in emergency calls being misidentified as spoofed calls or being dropped. This situation results in a risk for the reliability of the NG9-1-1 service and therefore a risk for the safety of Canadians.
2. The Commission therefore agreed with the application and concluded that it is necessary and appropriate to suspend the application of the STIR/SHAKEN condition set out in Compliance and Enforcement and Telecom Decision 2021-123 to all 9-1-1 calls from end-users to PSAPs and to call-backs from PSAPs to end-users. In the case of NG9-1-1 calls, the suspension will remain in effect only until a new implementation date is set by the Commission, based on CISC's recommendation. A report is due from the CISC WG (CRTC Interconnection Steering Committee) to the CRTC in May 2022.

Appendix B – Supplemental information about France

Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) has made several decisions throughout the years to combat CLI spoofing.

- In 2012, rules were passed to prevent Wangiri from premium rate numbers, forbidding the use of premium rate numbers as the CLI.
- ARCEP modified the rules in 2018:
    - French operators are allowed to block incoming international calls with French CLI numbers.
    - Auto dialers cannot use mobile numbers as the CLI. This was extended in January 2021 to cover all French numbers other than a dedicated numbering range for automated systems.
    - The CLI must be from a valid, allocated, and assigned number (for French numbers).
- The French decision of 2019 also includes STIR/SHAKEN as a long-term solution. In order to test it, ARCEP has already introduced specific ranges (for geographic, mobile, and non-geographic numbers) which are dedicated to authenticated numbers. Furthermore, a French law aimed at tackling fraudulent calls has been enacted on July 24, 2020, as the outgrowth of an almost two-year effort. It requires operators to block calls and messages with a French CLI received through an interconnection with an operator that does not provide telecommunications services to end-users in Europe by October 24, 2020. Some exceptions apply for international roaming or a potentially specific range for toll-free numbers. The law also requires all carriers to implement technologies to authenticate CLI information, preventing call spoofing, within 36 months. Relying on this legal framework, ARCEP organized workshops with operators to discuss the opportunities and the best way to implement the requirement to authenticate CLI information. ARCEP chaired the MAN (Mechanisms for the Authentication of Numbers) working group of APNF (Fixed Number Portability Association) and published a report of their findings on December 16, 2021.
- MAN working group decision: The MAN working group completed a detailed analysis of options and concluded that they needed a mechanism that was commercially available (to meet the tight timeframe) and standards-based (to ensure interoperability between service providers). This led them to select STIR/SHAKEN, despite some initial reservations about the approach. The report provides a detailed project plan to support an in-service date of July 24, 2023. The working group concluded that it would be impossible to deal with all possible use cases in the limited time available, so instead they opted to address as many use cases as practical with the initial release and satisfy the spirit of the law. Additional enhancements, post 2023, will be defined to expand coverage.
- Governance: The APNF (Fixed Number Portability Association) is tentatively planning to fill the governance authority role, but they insist that it is essential that "Public Authorities" (i.e., legislative, regulatory, and enforcement/legal) be involved in governance to make it effective.

- Cross-border: The report recognizes that spoofing and fraud are global problems that require global approaches. This implicitly acknowledges the need for cross-border call authentication, but the report does not take this idea any further. Their immediate concern is complying with the French law.

Appendix C – Supplemental information about STIR/MIXER framework

[RFC 8224] specified a protocol format for signing PASSporTs. The Secure Telephone Identity – Governance Authority (STI-GA) and STI Policy Administrator (STI-PA) were subsequently defined in ATIS to administer the allocation of certificates for signing PASSporTs.

However, what if it had been the other way around?

GSMA VINES

Validating INtegrity of End-to-end Signaling (VINES) is a working group under the GSMA Fraud and Security Group (FASG). VINES is looking at a series of security threats confronting mobile operators today. These include:

- CLI spoofing and thus nuisance calling;
- Re-routing (various forms of hacking, hijacking, and malicious redirection);
- Resizing (short-stopping, false ring); and
- Traffic pumping (routing calls through or to high-cost networks).

STIR/SHAKEN was proposed as a potential solution to the above. Other things discussed in VINES included AB Handshake and Solid project. There is a perception of growing consensus for STIR/SHAKEN internationally. There is a lot of interest in making sure calls sent to North America will not be marked as spam.

Perhaps, there is a shortcut to broader adoption due to existing GSMA security and governance?

A Collision: DESS Key Management

The GSMA Diameter End-to-end Signaling Security (DESS) working group, also in FASG, is chartered to explore how cryptographic keys can be shared between operators to facilitate 5G roaming. This includes bilateral connections between operators for Diameter, for example, which requires digital certificates.

Operators today share roaming information with each other through an “IR.21” document. To publish an IR.21, GSMA verifies an operator’s spectrum and “vets” you as a legitimate operator. Assigned Telephone Number (TN) ranges and Mobile Country Code/Mobile Network Codes (MCC/MNCs) are built into IR.21s, along with lots of other data. The Roaming Agreement Exchange (RAEX) is a real-time system that gives access to fields of a partner’s IR.21, including updates.

So, the thinking is that mobile operators could just share a digital certificate in their respective IR.21. DESS has its own requirements for certificate revocation and key lifecycle management. One caveat to this thinking is that not every operator uses the IR.21 (let alone RAEX) today but seems reasonable to assume if you want to participate in 5G roaming. Given this ongoing work in FASG, it makes sense to look at this as a potential international mobile operator approach for STIR cryptographic keys.

Specifically, use the IR.21 as its effective "root of trust" – that is, STIR/MIXER.

The STIR/MIXER Approach

With this approach, you specify a way for STIR to refer to cryptographic keying material published in the IR.21. Effectively, expose these IR.21 keys through a URI. There is some GSMA interest in both HTTP and the DNS (.3gpp domain) to expose keys. They are targeting PKCS #7 and ES256 which are the same keying requirements as STIR. One would sign PASSporTs with these self-signed digital certificates bilaterally between agreeing operators. This would likely impose minimal cost since re-using a keying system already being implemented for roaming.

One could probably bridge between these self-signed keys and an authorized Certification Authority (CA) with transitional strategies. Eventually, establish a CA (or small set of CAs) that issue digital certificates for the public keys of operators who publish their DESS keys through the IR.21. Finally, design services that distribute these digital certificates over HTTPS. This would be like an STI-Certificate Repository (CR).

Certification and STIR/SHAKEN Peering

GSMA could ultimately "bless" one or more CAs to issue digital certificates for DESS key management. CAs will conform to a Certificate Policy (CP) effectively set by the GSMA (like an STI-PA). CA practices will rely heavily on the existing full membership enrollment in GSMA (a prerequisite for using IR.21). The premise being that if the enrollment is good enough to secure roaming, then it should be good enough to secure PASSporT signing.

Regulatory constraints may require the use of certain CAs for certain geographies but the number of CAs will likely be much smaller than operators. Individual CAs could ultimately be responsible to national SHAKEN STI-GA/STI-PAs.

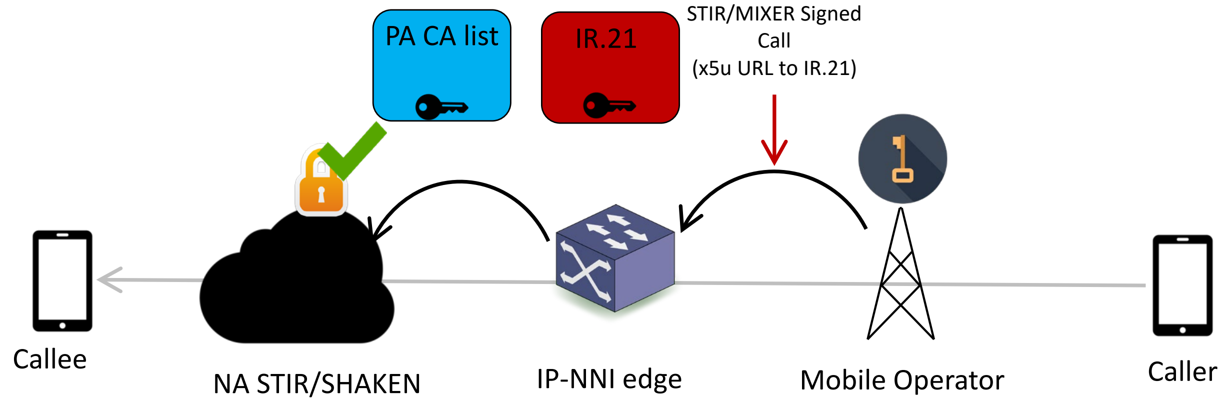
Note that STIR/MIXER is not intended to conflict with any future STI-GA/STI-PAs. The STIR/MIXER CAs could potentially peer with the STI-GA/STI-PA of North American SHAKEN instances. Perhaps jointly under the PA-like rubric of GSMA. However, this is obviously a decision for an STI-GA to accept these trust anchors or not.

SHAKEN Peering: From GSMA to North America STIR/SHAKEN

Figure 5 illustrates how an international call to North America (NA) can be authenticated using STIR/MIXER. Note that the "x5u" URL in this figure points to a publicly available STI-CR (reflecting the IR.21).

Figure 5

STIR/MIXER Call Authentication Example



Recap of DESS Key Management

DESS key management plans the integration of keys into IR.21 in phases. Once self-signed digital certificates are available in IR.21s, operators can begin leveraging them through bilateral agreement. Next, a RAEX capability for key rollover/revocation is needed. Potentially, also make keys available in the DNS in this phase.

This will take time, but for bilateral agreements, STIR/MIXER is easy to experiment with now.

Interesting Questions

The following are some questions to be addressed:

- What are the requirements of North America for peering with another trust anchor? For example, is there a requirement for a consolidated CRL?
- What kind of "vetting" of who is and isn't eligible to have a digital certificate is required? Would the GSMA full membership constraint (i.e., you own spectrum) be sufficient?
- Would MCC/MNC as a Service Provider Code (SPC) interwork with North American OCNs? Would other identifiers be better?
- VINES requirements would ultimately entail support for connected identity. Specifically, PASSporTs in the backwards direction which is still in development in the IETF. However, solving the VINES class of problems would bolster global adoption.