STIR/SHAKEN Protocol: Technical Overview & Industry Adoption

By ClearlyIP Published April 22, 2025 80 min read

STIR/SHAKEN Protocol: Comprehensive Technical and Industry Report

Introduction and Background

Unwanted **robocalls** and spoofed caller IDs have proliferated in recent years, eroding trust in telephone networks. Fraudsters often **spoof** caller ID information – making a call appear to come from a different number (often a local or known number) – to increase the chance that a victim will answer. By 2018–2019, billions of spam/scam robocalls were being placed annually in the U.S.,

prompting regulators and industry to seek solutions tnsi.com. The **STIR/SHAKEN** framework emerged as a leading solution to authenticate caller identity and combat illegal spoofing. STIR/SHAKEN is a suite of protocols and governance procedures that use **cryptographic signatures** in call signaling to verify that a calling number is legitimate and has not been spoofed docs.fcc.govdocs.fcc.gov. This report provides a comprehensive technical and industry overview of STIR/SHAKEN – from its development and inner workings to regulatory mandates, implementation challenges, industry adoption, and future outlook.

STIR stands for *Secure Telephone Identity Revisited*, an effort led by the Internet Engineering Task Force (IETF) to standardize a method of digitally signing caller ID information in Session Initiation Protocol (SIP) calls. **SHAKEN** stands for *Signature-based Handling of Asserted information using toKENs*, a framework developed by industry (ATIS/SIP Forum) that defines how STIR's digital certificates and signatures are deployed by service providers in real-world telephone networks ribboncommunications.com. Together, STIR/SHAKEN enables voice service providers to **attest** to the identity of callers and convey that attestation to the call recipient's provider, allowing verification of the calling number's authenticity. The ultimate goal is to restore trust in caller ID by ensuring that callers are who they claim to be – thereby helping consumers and carriers more reliably **identify and block** illegitimate robocalls and spoofed calls.

STIR/SHAKEN was motivated by the limitations of legacy caller ID frameworks. The traditional telephone network had no built-in way to validate the origin of a call's caller ID. As Voice-over-IP (VoIP) technology became widespread and interconnections between carriers increasingly used IP, bad actors found it easy to inject spoofed calls with fake caller IDs. By 2018, the IETF finalized new standards (revisiting earlier attempts) for authenticating caller identity in SIP, published as RFC 8224 in February 2018 10dlc.org. In parallel, the Alliance for Telecommunications Industry Solutions (ATIS) and the SIP Forum's IP-NNI Task Force developed the SHAKEN implementation framework (document ATIS-1000074) to apply those standards within carrier networks with a governance model and certificate infrastructure. Early trials of STIR/SHAKEN took place around 2018–2019, and regulators soon stepped in to accelerate adoption. In the U.S., the TRACED Act was signed into law in late 2019, directing the FCC to mandate STIR/SHAKEN for all voice providers en.wikipedia.org. In Canada, the CRTC likewise announced in 2019–2020 that all telephone service providers must implement caller ID authentication measures (STIR/SHAKEN) en.wikipedia.orgfasken.com. By mid-2021, STIR/SHAKEN went from concept to reality: most large U.S. carriers had deployed it by the FCC's June 30, 2021 deadline, and Canadian carriers by the CRTC's November 30, 2021 deadline fasken.comen.wikipedia.org. The following sections will delve into how STIR and SHAKEN work, their technical architecture, the regulatory frameworks enforcing them, challenges faced in implementation, current status and impact, and anticipated future developments.

Overview of STIR and SHAKEN

Secure Telephone Identity Revisited (STIR): STIR is the technical standard defined by the IETF to provide a secure mechanism for validating the origin of SIP calls. At its core, STIR defines a new SIP header called the **Identity header**, which carries a digital signature (in the form of a token) covering key call identity information docs.fcc.govdocs.fcc.gov. When a call is initiated over SIP, the originating service provider creates a signed token – called a **PASSporT** (Personal Assertion Token) – that includes the caller's number, the intended callee's number, timestamp, and other metadata. This PASSporT is essentially a JSON Web Token (JWT) carrying claims about the call, signed with the originating provider's private key transnexus.comtransnexus.com. The signature allows the destination carrier to verify that the calling number was indeed attested by the originating provider and not tampered with. The IETF's STIR specifications include **RFC 8224**, which defines the SIP Identity header and how the signature is attached to SIP messages, and **RFC 8225**, which defines the PASSporT token format and cryptographic signing procedures. In simple terms, STIR provides the *what* and *how* – what information is signed (caller ID data) and how it is signed and transported in SIP.

Signature-based Handling of Asserted information using toKENs (SHAKEN): SHAKEN is the implementation framework that applies STIR in carrier networks and defines the operational and policy aspects. It was developed by an industry task force (ATIS and SIP Forum) to create a standardized profile for using STIR in the telephone network, including how certificates are managed and how "attestation levels" are assigned ribboncommunications.com. While STIR is the underlying protocol, SHAKEN provides the *guidelines and governance* for deployment: it specifies the network elements involved in signing and verifying calls, the three attestation levels (A, B, C) to indicate the caller ID confidence, and the public-key infrastructure (PKI) to ensure trust across different providers. In essence, SHAKEN is a set of ATIS standards (notably ATIS-1000074 and related documents) that tells service providers how to implement STIR in an interoperable way on IP networks. For example, SHAKEN spells out how a carrier should obtain a digital certificate from an approved Certificate Authority, how to use it to sign call identities, and how to validate signatures on incoming calls docs.fcc.govcstga.ca. It also defines the governance roles (like a centralized policy administrator and governance authority) to prevent unauthorized entities from signing calls. STIR and SHAKEN work hand in hand: STIR provides the cryptographic tools, and SHAKEN provides the deployment and policy framework. Together, they form the STIR/SHAKEN framework for caller ID authentication.

Problems Addressed by STIR/SHAKEN

STIR/SHAKEN directly addresses **caller ID spoofing**, where scammers falsify the calling number (for example, making it look like a call is coming from a local number or a trusted organization). By attaching a digital signature to the call setup, STIR/SHAKEN lets the terminating carrier **verify** that the calling number has been authenticated by the originating carrier. If a call's identity header fails verification or is missing, the terminating carrier can suspect spoofing and treat the call accordingly (e.g., flag it as likely spam or block it). This helps mitigate "neighbor spoofing" robocalls, IRS impostor scams, and other frauds that rely on fake caller IDs. STIR/SHAKEN also facilitates **traceback and enforcement**: the inclusion of an originating identifier in the token (discussed later) allows authorities to trace illegal call campaigns to the originating provider or gateway datatracker.ietf.orgcdn.atis.org. Overall, STIR/SHAKEN is a major component of the industry's strategy to curb robocalls, complementing other tools like call blocking analytics and do-not-originate lists.

It's important to note that STIR/SHAKEN is designed for calls using **SIP/IP networks**. The framework assumes calls are carried end-to-end over IP so that the SIP Identity header can travel with the call. Traditional TDM (SS7/ISUP) call paths do not natively support STIR/SHAKEN, which is a challenge we will explore later. Nonetheless, within IP-based telephony, STIR/SHAKEN provides a crucial trust layer. As we move into the technical details, we will explain exactly how the STIR/SHAKEN protocols work to authenticate a call.

Technical Architecture and Call Authentication Process

STIR/SHAKEN Architecture and Components

At a high level, deploying STIR/SHAKEN requires enhancements to both the originating side and terminating side of a call, as well as a supporting certificate infrastructure. **Figure 1** below illustrates the SHAKEN reference architecture, showing the logical components involved in signing and verifying a call's identity. These components include: an **Authentication Service (STI-AS)** in the originating provider's network that creates and signs the identity token, a **Verification Service (STI-VS)** in the terminating provider's network that verifies the token, a secure database or **certificate repository (STI-CR)** for storing public certificates, and other supporting functions like **Secure Key Store (SKS)** and **Call Validation Treatment (CVT)** for additional analytics atis.orgatis.org.

! https://transnexus.com/whitepapers/out-of-band-shaken/

Figure 1: SHAKEN reference architecture (logical call flow and certificate infrastructure) transnexus.com. In this architecture, the **originating service provider (Service Provider A)** on the left authenticates and signs the call, while the **terminating provider (Service Provider B)** on the right validates the signature. When a call is initiated by an end user (SIP User Agent) on Service Provider A's network, it is processed by the provider's call server (e.g., IMS Call Session Control Function) and handed to the provider's **STI-AS** (Authentication Service) for signing atis.orgtransnexus.com. The STI-AS accesses the provider's private signing key stored in a secure key store (SKS) to create a digital signature (the PASSporT) for the call transnexus.com. The signed PASSporT is inserted into the SIP **Identity header** of the outbound INVITE message (step 5→6 in the figure) and the call is sent towards the destination network transnexus.com. Across the interconnect (Network-to-Network Interface) between provider A and provider B, the SIP INVITE carries the Identity header with the token (step 7). Upon reaching **Service Provider B**, the call is passed to its **STI-VS** (Verification Service) which extracts the Identity header and validates it. The STI-VS fetches the originating provider's public certificate from the **STI-CR (Certificate Repository)** indicated by the Identity header's info (step 10→11) transnexus.com. Using that certificate, the STI-VS checks the signature and the integrity of the PASSporT claims (step 12) transnexus.com. If verification succeeds, the call can be treated as "verified" (the caller ID has been cryptographically authenticated); if it fails, the terminating provider knows the caller ID was likely spoofed or at least unverified. The terminating provider can then apply **Call Validation Treatment (CVT)** – e.g., label the call as "Verified" on the recipient's phone or, conversely, tag it as "Spam"/reject it if the signature was missing or bad transnexus.comtransnexus.com.

In summary, the architecture consists of: (a) **Origination components:** the user's device and originating network elements, with an STI-AS that signs calls using credentials; (b) **Termination components:** the terminating network's STI-VS that validates calls; and (c) **Governance components:** a certificate authority infrastructure (STI-CR, STI-PA, etc.) that distributes and trusts the signing certificates. The call flow can be summarized in steps:

1. **Call Setup:** The caller's device (UA) sends a SIP INVITE to its provider (Service Provider A). The provider's call control (SBC or call server) identifies the call needs STIR authentication atis.org.

2. **Authentication Service:** The originating provider's STI-AS generates a PASSporT for the call. It gathers call data: the originating number, destination number, and current timestamp, and determines the appropriate **attestation level** (A, B, or C, explained below). It then creates a PASSporT JSON object with these fields and signs it using its private key (retrieved securely, often from an SKS) transnexus.comtransnexus.com. The signature algorithm used is typically ECDSA with SHA-256 (as per STIR standards, default "ES256" elliptic curve signing).

3. **SIP Identity Header Insertion:** The STI-AS outputs a SIP **Identity** header containing the signed PASSporT token. This header includes the cryptographic signature and may include a pointer (URL) to the certificate needed for verification datatracker.ietf.orgdatatracker.ietf.org. The SIP INVITE leaving Service Provider A now has an Identity header attached, alongside the normal call setup headers.

4. **Call Transit:** The call is handed to the next network (perhaps via an IP interconnection or Session Border Controller). Intermediate transit carriers are expected to pass along the Identity header untouched. (If any transit carrier is not SIP-capable or strips the header, the verification will fail on the other end. We discuss this risk in **Implementation Challenges**.)

5. **Verification Service:** When the call reaches the terminating provider (Service Provider B), their network receives the SIP INVITE with the Identity header. Service Provider B invokes its **STI-VS** to validate the call. The STI-VS uses the information in the Identity header to fetch the signing certificate of the originating provider. Specifically, the PASSporT token contains a `"x5u"` field (or similar) which is a URI pointing to the public certificate of the signer transnexus.com. The STI-VS makes an HTTPS query to the **Certificate Repository (STI-CR)** URL to retrieve the certificate (if not already cached).

6. **Signature Verification:** Using the public key from the obtained certificate, the STI-VS checks the signature on the PASSporT. It also checks that the signed data (caller number, callee number, timestamp, etc.) matches the actual call details in the SIP INVITE (to ensure the token wasn't replayed or altered) transnexus.comtransnexus.com. It verifies the certificate chain (ensuring the certificate was issued by a trusted authority in the SHAKEN ecosystem) transnexus.com. If all checks pass, the token is validated – meaning the call's origin is authenticated.

7. **Call Completion and Treatment:** The terminating provider now has a result: either **"Verification PASS"** (caller ID valid) or **"Verification FAIL"** (no valid signature). This result can be used in call handling. For a valid call, the provider may pass a notification to the called user's phone (many carriers display " ✅ Verified" or a checkmark for calls with valid A-level attestation). If the verification fails or the attestation level is low, the provider might route the call to voicemail or tag it with a warning (e.g., "Spam Likely"), or even block it if it's known to be malicious docs.fcc.gov. The specifics depend on each provider's call **analytics** and policies (often STIR/SHAKEN feeds into broader robocall detection algorithms rather than being a sole determinant).

The above process relies on a robust **public key infrastructure (PKI)** to manage the digital certificates used for signing and verifying. One half of STIR/SHAKEN is the real-time call signing, and the other half is this certificate governance that ensures all service providers trust each other's signatures. We will now dive deeper into some of these technical elements: attestation levels, the PASSporT token structure, and the certificate management framework.

PASSporT and SIP Identity Header

The fundamental data structure used in STIR is the PASSporT, which is essentially a secure token carrying call identity info. Technically, a PASSporT is a JSON Web Token (JWT) with defined claims, digitally signed using the originating service provider's private key datatracker.ietf.org. In STIR/SHAKEN usage, the PASSporT includes both standard claims and SHAKEN-specific extensions. The core fields/claims in a STIR/SHAKEN PASSporT include:

- **Originating identity (`"orig"`):** the caller's telephone number (calling party number).
- **Destination identity (`"dest"`):** the called number(s) (one or multiple, depending on whether the call is to a single user or a conference, etc.).
- **Timestamp (`"iat"`):** the "issued-at" time (UNIX timestamp) when the token was generated. This helps prevent replay attacks – tokens are valid only for a short time window.
- **Attestation level (`"attest"`):** a SHAKEN-specific claim indicating the level of confidence/verification the originating provider has in the caller's identity (explained in detail below) datatracker.ietf.org.
- **Origination identifier (`"origid"`):** another SHAKEN-specific claim – a unique identifier for the call as assigned by the originating provider datatracker.ietf.org. This is typically a UUID that can be used for tracing the source of the call (especially useful in investigations of illegal calls, as it can tie together multiple calls from the same source).
- **Certificate reference (`"x5u"`):** (in the token header) a URI pointing to the public certificate of the signer, so that verifiers know where to fetch the certificate datatracker.ietf.orgdatatracker.ietf.org. Alternatively, a certificate thumbprint (`"x5t"`) could be included to identify the certificate by fingerprint, but SHAKEN generally uses `x5u` with an HTTPS URL to a certificate repository.

All these fields are bundled into the token, which is then signed. The signature covers the PASSporT header and payload. STIR allows two forms: full PASSporT (includes the entire JSON in the SIP Identity header in base64) or "compact form". However, **SHAKEN requires the full form** (including all claims) for maximum information – the SHAKEN specifications explicitly say the compact form is not used datatracker.ietf.org. The entire PASSporT token (header.claims.signature) is then base64-encoded and placed in the SIP `Identity:` header. For example, a SIP INVITE with an Identity header might look like:

bash

Copy

```
Identity: eyJhbGciOiJFUzI1Ni... (long base64 token) ;info=<https://cert.shaken.provider.net/cert/AS12345.cer>;alg=ES256;ppt="shaken"
```

Where `info` is pointing to the certificate URL and `ppt="shaken"` indicates the PASSporT type is SHAKEN. The terminating side's verification service uses the info to retrieve the certificate and the alg (algorithm) to verify the signature datatracker.ietf.orgdatatracker.ietf.org. If the verification succeeds, the call is cryptographically authenticated. The terminating provider can then use the attestation value to decide how to treat the call (for instance, an A attestation call might be let through normally, whereas a call with C attestation or a broken signature might be blocked or flagged).

Attestation Levels (A, B, C)

Attestation levels are a cornerstone of SHAKEN's extension to STIR. They provide a simple indicator of how confident the originating service provider is in the caller's identity and right to use the number. The SHAKEN framework defines **three levels of attestation** datatracker.ietf.org:

- **Full Attestation (Level A):** The highest level of trust. The originating service provider **has authenticated the calling party and confirms they are authorized to use the calling number** transnexus.com. In practice, this means the call originates from the provider's own subscriber or customer, and the provider has a direct relationship with that user and assigned them that phone number. Example: A customer registered on the provider's network (such as a mobile subscriber or VoIP subscriber of that carrier) placing a call using their own number gets A-level attestation. "A" attestation essentially says, *"This is my customer and I gave them this number; I can vouch for this caller ID."*

- **Partial Attestation (Level B):** The originating provider has **authenticated the source of the call (e.g., knows the customer/device placing the call), but cannot verify that the caller is authorized to use the number** transnexus.com. This often applies to scenarios like calls coming from an enterprise PBX or a call center that is using a number not directly assigned by the originating carrier. For example, a business might send calls through a trunk, and the calling numbers presented could be the business's numbers which the provider isn't able to individually verify per call. The provider knows the call came from a known customer (e.g., a PBX trunk from a corporate client) but isn't certain that the specific calling number is legitimate (perhaps the enterprise could be spoofing or using a number that it shouldn't). B attestation says, *"This call came from my network and I know the entity that sent it, but I can't guarantee the calling number is one I assigned to them."*

- **Gateway Attestation (Level C):** The lowest level. The provider is simply the **entry point (gateway) into the IP network and cannot authenticate the call source** beyond that transnexus.com. This is used typically when a call is received from an **untrusted or non-STIR/SHAKEN-capable source**, such as an international gateway or a TDM interconnection from another carrier. The provider can only attest that it received the call on a particular interface, but it doesn't know the origin. C attestation says, *"I got this call from somewhere else (e.g., another network) and have no verified info about the origin – so I'm just tagging where it entered my network."* For example, a U.S. gateway receiving a call from an overseas carrier would assign C.

These attestation levels are included in the PASSporT (`"attest": "A"`, `"B"`, or `"C"`). The terminating provider, after verifying the signature, can examine the attestation value to gauge the trustworthiness of the caller ID. A-level calls are the most trustworthy (fully verified caller on a known number), B are somewhat in-between, and C are essentially unverified calls. In practice, many analytics engines and call blocking apps treat B and especially C calls with more scrutiny. For instance, a validated A-level call might display as "Caller Verified" to the recipient, whereas a C-level might not get such indication and may be more likely flagged as potential spam by analytics.

Attestation also plays a role in traceback. If a malicious call still comes through with A attestation, it means the originating provider signed it as a known customer – this provides a clear starting point for enforcement (the provider is accountable). If it's B or C, it indicates the call originated elsewhere or wasn't fully verified, suggesting the need to trace further back (e.g., if C, one might have to look at which gateway passed it).

The concept of attestation has been widely praised as a pragmatic way to handle the complex reality of telephone networks, where not every call can be verified to the same degree. Regulators have put emphasis on **preventing "over-attestation"**, meaning carriers should not give A attestation to calls that don't meet the criteria. Unfortunately, there have been instances of "over-attestation" – some providers improperly labeling calls as A when they shouldn't, either due to error or to evade spam detection. This undermines the trust model tnsi.com. Industry and oversight bodies (like the STI-GA in the U.S.) have been monitoring this and can sanction misbehaving providers (more on this in the **Industry Adoption** section).

Certificate Infrastructure and Trust Governance

Underpinning the entire STIR/SHAKEN framework is a **public key infrastructure (PKI)** that enables trust between different service providers. The PKI ensures that when Verizon receives a call signed by AT&T, Verizon can verify the signature using a certificate that it trusts was issued to AT&T. In other words, carriers need a way to trust each other's signing keys. This is accomplished through a hierarchical certificate system governed by neutral authorities.

In the STIR/SHAKEN model, each participating **service provider (SP)** obtains a digital certificate that it uses to sign calls. This certificate binds the provider's identity (often indicated by a "Service Provider Code" or SPC) to a public key. The certificate is issued by a trusted **Certification Authority (CA)** – in SHAKEN terms, an **STI-CA** (Secure Telephone Identity Certificate Authority) cstga.cacstga.ca. All STI-CAs are accredited and overseen by a central **Policy Administrator** under rules set by a **Governance Authority**. In the United States, for example, the **STI Governance Authority (STI-GA)** (operating under ATIS) defines the policies and accredits CAs, and the **STI Policy Administrator (STI-PA)** (iconectiv, selected by the STI-GA) enforces those policies – issuing credentials (called **SPC tokens**) to service providers and authorizing CAs to issue certificates cstga.cacstga.ca. A service provider must undergo vetting (e.g., have an appropriate regulatory authorization and numbering resources) and then register with the STI-PA to get an **SPC token**. This token is basically a token that the provider presents to an approved STI-CA to obtain a signing certificate. The STI-CA, seeing a valid token, issues the certificate to the provider (the certificate typically includes the provider's unique identifier, like their Operating Company Number or SPC, in an extension field).

All STI-Certificates chain up to a common **trust anchor** (or a small set of trust anchors) so that every verifier can trust signatures from any authorized provider. In the U.S., the STI-PA (iconectiv) manages the root of trust – effectively, the STI-PA's root certificate (or list of authorized CA roots) is distributed to all service providers as the trust anchor. This means if a carrier receives a certificate

claiming to be from "STI-CA X", it will trust it only if "STI-CA X" is on the approved list and the certificate chains to the root. The SHAKEN governance model ensures there is **only one governance system per country/region** – e.g., one STI-GA and STI-PA in the U.S., one in Canada (the Canadian Secure Telephone Identity Governance Authority, CST-GA), etc., to keep the trust system coordinated cstga.cacstga.ca.

Key roles in the governance system (based on ATIS-1000080 model cstga.cacstga.ca):

- **Secure Telephone Identity Governance Authority (STI-GA):** Industry-led body that sets policies for certificate issuance and participation. The STI-GA ensures the system's integrity (e.g., deciding who can be a CA, what providers must do to qualify). The STI-GA in the U.S. has a board with industry representatives and works closely with the FCC.
- **Secure Telephone Identity Policy Administrator (STI-PA):** The operational authority that implements the GA's rules. It runs the infrastructure to register service providers and manage tokens and the list of approved CAs cstga.cacstga.ca. In the U.S., iconectiv serves this role. The STI-PA issues the **SPC tokens** to service providers and provides a directory of approved certificates (the certificate repository). It effectively is the trust anchor – certificates not issued under the STI-PA's authority won't be trusted.
- **Secure Telephone Identity Certification Authorities (STI-CAs):** These are the certificate issuers. There can be multiple CAs to foster competition and redundancy. In the U.S., as of 2022, there were over a dozen authorized STI-CAs (e.g., large providers and certificate companies can operate CAs). STI-CAs issue STI certificates to service providers once they have the SPC token proving they're authorized sti-ga.atis.orgsti-ga.atis.org. The CAs publish the certificates (often to a central repository or their own online repositories) so that verifiers can fetch them.
- **Service Provider (SP):** The voice service provider (carrier or VoIP provider) who signs calls. The SP obtains a certificate, operates STI-AS and STI-VS functions, and is responsible for signing calls correctly (with proper attestation) and verifying incoming calls. The providers are the end-entities in this PKI.

When an originating service provider signs a call, it includes its certificate reference in the Identity header. The terminating provider uses that to download and validate the certificate. The certificate tells the verifier which provider signed the call (and that the provider was authorized by the trust framework). If the certificate is not valid or from an unknown CA, the verification fails. Thus, **only**

calls signed by authorized providers will verify. This is critical: it prevents scammers from simply self-signing with their own random keys. If a bad actor tried to sign calls without a valid certificate, the terminating carriers would not trust it because it wouldn't chain to the known root.

The certificate infrastructure went live in late 2019 in North America. By the end of 2019, the U.S. STI-GA had selected the STI-PA and approved the first STI-CAs sti-ga.atis.org, and the system launched (the first certificates were issued and the framework operational by early 2020). Canada followed a similar model, with its own governance (the CST-GA) and using the same technical standards (in fact, the U.S. and Canadian systems are very similar and many CAs serve both). Each service provider typically has at least one certificate. Certificates can be rotated and have relatively short lifetimes (to limit risk of compromise; they can be revoked if needed via Certificate Revocation Lists or OCSP, though in practice STIR/SHAKEN certs often have short expiry rather than relying on revocation). The STI-PA maintains a real-time list of authorized service providers and can revoke a provider's token (which would invalidate future certs for them) if they are found to be misusing the system cdn.atis.orgcdn.atis.org.

To illustrate the trust: imagine provider X (with OCN 1234) gets a certificate that essentially says "This is provider X (1234), and here is their public key" signed by STI-CA ABC, which is trusted by the STI-PA. When provider X signs a call, they include a reference to that cert. The verifier fetches it, sees "issued by STI-CA ABC under STI-PA root", and thus trusts that the key belongs to a valid provider. The verifier checks the signature with that key and knows "Yes, provider X attests this call". If provider X is known for bad behavior, further action can be taken (such as blocking or later revocation of their authorization). This trust framework is what makes STIR/SHAKEN an **ecosystem solution** rather than a simple bilateral exchange – it required industry consensus on governance, which was a significant part of the development.

Standards and Key Specifications

To provide references, the following are some of the key standards and documents defining STIR/SHAKEN:

- **RFC 8224 – Authenticated Identity Management in SIP (2018):** Defines the mechanics of the SIP Identity header and how a PASSporT token is attached to a SIP INVITE 10dlc.org. This replaced RFC 4474, an earlier attempt at caller ID verification, hence the "revisited" in STIR.
- **RFC 8225 – Personal Assertion Token (PASSporT) (2017):** Specifies the JSON token format for conveying calling identity information securely (the JWT schema, claim types, signature algorithms, etc.). It defines base claims like "orig", "dest", "iat" and how they're signed.

- **ATIS-1000074 – SHAKEN: Signature-based Handling of Asserted Information Using Tokens (2017):** The primary industry standard from ATIS that details the SHAKEN framework. It covers how STIR is used in IP networks, the definition of attestation levels, and baseline operational considerations. (This is referenced in many documents as the core SHAKEN spec datatracker.ietf.org.)

- **ATIS-1000080 – SHAKEN Governance Model and Certificate Management (2018):** Defines the certificate governance structure (STI-GA, STI-PA, STI-CA roles and protocols) cstga.cacstga.ca. It includes the processes for providers to obtain certificates (using ACME protocol to request certs with their token, etc.).

- **ATIS-1000084 – STI Certificate Policy (2018):** Lays out policies for certificate authorities issuing STI certificates (security requirements, certificate contents, etc.). Essentially the rulebook that all authorized STI-CAs must follow.

- **RFC 8588 – STIR Certificate Delegation (2019):** Defines a way to delegate authority to sign calls (allowing a parent certificate to issue a subordinate used by intermediate entities). Not heavily used initially, but forms basis for enterprise delegation (see future outlook).

- **RFC 8946 – PASSporT Extension for Diverted Calls (2021):** An extension so that if a call is forwarded (diverted), the intermediate hop can indicate the original identity in a secure way datatracker.ietf.org. This helps STIR work through call forwarding scenarios by using a "div" PASSporT to carry original call info.

- **Drafts for Rich Call Data (RCD) Extension:** Ongoing IETF work (soon to be RFC) to allow PASSporT to carry extra data like caller name, logo, call reason, etc., in a secure way datatracker.ietf.org. This is aimed at enhancing caller ID beyond just a number (discussed later).

- **ATIS-1000095 & 1000096 – Call Authentication for TDM Interconnect (2020–2021):** Technical reports evaluating how to extend STIR/SHAKEN to non-IP networks. ATIS-1000095 suggests using ISUP signaling parameters to carry attestation info for TDM calls learn.rbbn.com, while ATIS-1000096 describes an out-of-band mechanism to send PASSporT data over the internet in parallel to a TDM call learn.rbbn.com. These are not core specs but address the TDM challenge (covered in **Implementation Challenges**).

- **3GPP and ETSI adaptations:** As STIR/SHAKEN is North America-centric, 3GPP has incorporated support in IMS standards (3GPP TS 24.229, etc.) mapping SHAKEN into IMS/SIP for wireless networks. ETSI has technical specifications referencing SHAKEN for use in European contexts (though Europe has not yet mandated it network-wide).

With the technical foundation laid out, we will now move on to the **regulatory frameworks** that have driven the deployment of STIR/SHAKEN, and then to practical aspects of implementation and impact.

Regulatory Framework and Mandates

Regulators in the United States and Canada – two countries hit particularly hard by robocalls – have strongly pushed for STIR/SHAKEN adoption. This section outlines the key mandates, rules, and timelines established by authorities like the U.S. Federal Communications Commission (FCC) and the Canadian Radio-television and Telecommunications Commission (CRTC).

United States: FCC and the TRACED Act

In the U.S., the roll-out of STIR/SHAKEN was catalyzed by the *TRACED Act* (Telephone Robocall Abuse Criminal Enforcement and Deterrence Act) enacted in December 2019. This law directed the FCC to require all voice service providers to implement call authentication technology (i.e., STIR/SHAKEN) in their IP networks en.wikipedia.org. Prior to the TRACED Act, the FCC had been urging voluntary adoption – major carriers like AT&T, Verizon, T-Mobile had begun limited deployments and bilateral call authentication exchanges by 2019. But the new law made it a regulatory mandate.

The FCC responded with orders in 2020 setting firm deadlines. In **March 2020**, the FCC adopted rules requiring "all originating and terminating voice service providers" to implement STIR/SHAKEN in the IP portions of their networks by **June 30, 2021** docs.fcc.gov. This requirement was for providers that had IP technology in their call transport – those using TDM for everything were given more leeway (since STIR/SHAKEN can't work on TDM without an alternative). Recognizing that smaller and rural carriers might need more time (due to cost or technology constraints), the FCC granted extensions to certain classes of providers:

- **Large voice providers (100K+ subscribers):** No extension – must implement by June 30, 2021.
- **Small voice providers (100,000 or fewer subscribers):** Initially a two-year extension to June 30, 2023 fasken.com. However, the FCC later **shortened the extension for one category of small providers** – those that are non-facilities-based and/or generate large call volumes – to

June 30, 2022 docs.fcc.gov. This was because evidence showed many robocall scams were emanating from certain small VoIP providers. The FCC didn't want bad actors hiding behind the "small provider" extension.

- **Voice service providers with TDM network parts:** The TRACED Act allowed extensions for providers that "materially rely on a non-IP network" until a solution for non-IP call authentication is available. The FCC indeed granted such providers (often rural LECs with TDM switches) an extension beyond 2021. They are required to either upgrade to IP or implement a robocall mitigation program in the interim.

- **Intermediate providers (transit carriers):** They were required to implement STIR/SHAKEN a bit later – the FCC set a June 30, 2021 deadline for any that originate/terminate calls, and by June 30, 2023 for all others in the call path to be able to pass along STIR info docs.fcc.gov.

- **Gateway providers (providers that bring in calls from foreign sources into the U.S.):** In 2022, the FCC adopted rules requiring gateway providers to implement STIR/SHAKEN by June 30, 2023 as well docs.fcc.gov. The rationale is that many robocalls originate overseas; requiring the U.S. entry point to sign and verify those calls (or at least attach a signature that it's the gateway) can improve traceability.

In addition to mandates to implement STIR/SHAKEN, the FCC has several complementary regulatory measures:

- **Robocall Mitigation Database (RMD):** Effective Fall 2021, the FCC required all voice providers to file certifications in a public database indicating their call authentication status – full STIR/SHAKEN, partial, or none – and if not full, what robocall mitigation measures they have in place. As of September 2021, intermediate and terminating carriers were forbidden from accepting traffic from any provider not listed in the database docs.fcc.gov. This essentially forces all providers to either implement STIR/SHAKEN or at least have a mitigation plan on record, or else their calls get blocked by the rest of industry. It's a strong incentive.

- **Enforcement and Cease-and-Desist:** The FCC, through its Enforcement Bureau, has taken action against entities that facilitate illegal robocalls. STIR/SHAKEN data is aiding these efforts by making it easier to trace call sources. The FCC has sent cease-and-desist letters to providers transmitting large volumes of spam calls and even proposed hefty fines (e.g. $120M+ fines in some cases) for prolific robocallers. In some instances, they've worked with the STI-GA to revoke a bad provider's signing credentials cdn.atis.orgcdn.atis.org.

- **Caller ID Authentication in Caller ID services:** The FCC requires that if a call has been authenticated (signed) and verified, that status should be transmitted to consumers wherever possible – for instance, a "Caller Verified" label on phones. Major mobile carriers have implemented this in their smartphone calling apps since 2019–2020.

- **Ongoing Rule Refinement:** The FCC continues to update rules: for example, in December 2022 and May 2023 orders, they took further steps like extending STIR/SHAKEN to text messages (in a limited way, ordering a study), shortening the small provider extension for certain categories, and clarifying that outsourcing signing to third parties doesn't remove a provider's responsibility (the FCC 24-120 order in 2024 explicitly required that even if a provider uses a hosted STIR/SHAKEN service, it must use its **own certificate** and retain responsibility for correct attestation docs.fcc.govdocs.fcc.gov).

In summary, the U.S. regulatory timeline was: **2019** – voluntary phase and TRACED Act passed; **2020** – FCC mandate order (Report and Order) setting 2021 deadline; **2021** – STIR/SHAKEN goes live in IP networks of big carriers (June 30) and non-compliant providers start getting blocked; **2022** – extension shortened for certain small VoIP providers (due to abuse concerns) to June 2022; **2023** – essentially all providers that can implement were required to do so by June 30, 2023 docs.fcc.gov. By 2023, the U.S. had a near-universal STIR/SHAKEN participation among IP carriers, with only those on legacy systems or with special exemptions (very few) not signing calls. The FCC's aggressive stance, combined with industry cooperation via the STI-GA, has made the U.S. a leader in deployment.

Canada: CRTC Mandate and CST-GA

Canada moved in parallel with the U.S., if slightly trailing in timeline. The Canadian regulator (CRTC) was closely watching the STIR/SHAKEN developments and collaborating with the FCC. On December 9, 2019, a noteworthy event took place: the **first official cross-border STIR/SHAKEN-authenticated call** between the U.S. and Canada. It was a call between networks (Comcast and TELUS) joined by then-FCC Chairman Ajit Pai and CRTC Chairman Ian Scott to demonstrate the tech's ability; they issued a joint statement endorsing STIR/SHAKEN transnexus.comcrtc.gc.ca.

The CRTC had actually signaled its expectations early on. In 2018, the CRTC stated it expected Canadian telecom service providers to implement caller ID authentication measures by March 2019 fasken.com – an ambitious timeline that turned out to be premature. That initial deadline was extended multiple times as the technology and standards were still being solidified. Key milestones in Canada:

- **2019:** CRTC set an expectation for implementation by September 30, 2020 (after extending the March 2019 date) fasken.com. Providers that could not meet it were asked to provide explanations.

- **September 2020:** The deadline was further extended by 9 months, aligning with the U.S. June 30, 2021 timeline fasken.com. The CRTC explicitly noted it wanted to synchronize with the FCC's schedule, since many providers operate cross-border and equipment vendors needed time.

- **March 2021:** The CRTC, apparently seeing progress, moved from "expectation" to **requirement**. In CRTC Decision 2021-123 (April 2021), the CRTC mandated that **all Canadian TSPs implement STIR/SHAKEN in their IP networks by November 30, 2021** fasken.com. This was effectively the hard deadline. Importantly, **no exemptions were granted** – unlike the FCC, which gave small carriers extra time, the CRTC applied the requirement universally fasken.com. The CRTC reasoned that even smaller providers should be capable of either implementing or partnering to implement, and excluding them would leave a hole for abuse.

- **November 30, 2021:** Implementation date in Canada. By this date, all Canadian carriers were expected to have STIR/SHAKEN up and running on IP portions of their network. The CRTC also required carriers to file **readiness reports** by August 2021 and then every 6 months going forward on their STIR/SHAKEN status telnyx.com. This reporting regime is stricter than in the U.S., reflecting the "no exemptions" approach – it keeps all providers accountable regularly.

On the governance side, Canada established the **Canadian Secure Token Governance Authority (CST-GA)** which, in cooperation with ATIS, oversees the Canadian implementation. The CST-GA selected its own Policy Administrator (which turned out also to be iconectiv, the same as the U.S., simplifying cross-border compatibility) and set up a list of authorized Canadian STI-CAs. Canadian carriers obtain certificates through that system. The Canadian framework uses the same three attestation levels and technical specs as the U.S. (since both are based on ATIS standards). A difference is simply scale – Canada has fewer providers and many rely on vendors/shared infrastructure, so some opted to use outsourced STIR/SHAKEN services.

By early 2022, the largest Canadian carriers (Bell, Rogers, TELUS, etc.) were signing calls and verifying incoming calls. There were some growing pains; for instance, initially some wireless calls were not showing as verified due to handovers between networks, but those were ironed out. The CRTC has been monitoring the effectiveness on scam call reduction. They noted that STIR/SHAKEN

is **not a silver bullet** but an important tool, and they complemented it with other measures (e.g., a 2022 CRTC decision mandated telecoms to implement network-level call blocking for blatantly spoofed calls, like invalid numbers, in addition to STIR/SHAKEN).

One notable event: On the implementation deadline (Nov 30, 2021), at least one smaller Canadian operator asked for an extension specifically for 9-1-1 service lines (some technical issues in applying STIR/SHAKEN to certain 911 scenarios). The CRTC granted a deferral for 911 circuits conditionally crtc.gc.ca, but otherwise held firm that all voice traffic should be signed if IP-based.

In summary, Canada's regulatory stance is: *everyone must implement STIR/SHAKEN, and do it by end of 2021*. No carve-outs for small carriers; instead, the CRTC expects industry cooperation (smaller TSPs could work with larger ones or vendor solutions). By aligning with the U.S. timeline, Canada ensured a coordinated North American approach.

Other Countries and International Outlook

Outside the U.S. and Canada, the adoption of STIR/SHAKEN is still in early stages, but interest is growing. A few points on global status:

- **United Kingdom:** The UK's Ofcom has studied STIR/SHAKEN but has so far not mandated it. In 2022, Ofcom issued a consultation on CLI (Calling Line Identification) authentication, looking at STIR/SHAKEN and other options ofcom.org.uk. Ofcom noted that the UK's telephone network still has substantial TDM legacy and a mix of providers, making immediate implementation complex and costly. As of early 2023, Ofcom opted not to require STIR/SHAKEN yet, citing those challenges (indeed, Ofcom described it as "complex, costly and time-consuming" to impose quickly) commsrisk.com. Instead, the UK has focused on measures like requiring providers to block inbound international calls spoofing UK numbers and improving *Know Your Customer* rules. There is ongoing discussion, and some UK operators might implement STIR/SHAKEN on IP interconnects voluntarily in the future.

- **European Union:** The EU has not mandated STIR/SHAKEN either. However, there are initiatives in some countries/regions for call verification. France, for instance, implemented a mandate for filtering spam calls and has considered technical solutions for CLI validation. The European regulators are certainly aware of STIR/SHAKEN – ETSI (a European standards body) published a report analyzing how it could work in EU networks etsi.org. Given the EU's fragmented telecom landscape, a coordinated mandate may take time. Instead, individual carriers (especially those that operate in the U.S. as well) might adopt it on bilateral bases. The GSMA and various industry forums are examining it.

- **Other Countries:** No country has gone as far as the U.S./Canada in requiring STIR/SHAKEN broadly yet. However, Australia's communications authority ACMA has expressed interest in combating spoofing and could consider such frameworks. Some countries in Asia have huge volumes of scam calls (e.g., India) but their networks and regulatory environments differ; they have not implemented STIR, focusing instead on Do Not Call and AI-based blocking. That said, if STIR/SHAKEN proves successful in North America, it is likely to inspire similar efforts elsewhere or even a global expansion.

- **Cross-Border and International Calls:** A major emerging issue is how to extend the trust of STIR/SHAKEN beyond national borders. Currently, a call originating in the U.S. and terminating in Canada can be verified because both countries use essentially the same framework (indeed, the first cross-border verified call was demonstrated in 2019). The U.S. and Canada are working on mutual recognition so that, for example, a Canadian carrier will trust a certificate issued under the U.S. STI-GA governance and vice versa cdn.atis.org. The STI-GA's 2024 report mentions efforts to allow verification of calls between the U.S. and other countries by defining requirements to share certificate information cdn.atis.org. For other international calls (say from Europe to U.S.), there isn't a system in place yet. The FCC has urged international cooperation, and it's conceivable that a global or regional governance could develop (perhaps coordinated by ITU or bilateral agreements).

In short, North America is spearheading STIR/SHAKEN deployment by regulatory mandate. Other regions are in exploratory or voluntary phases. The expectation is that as robocalls and CLI spoofing are a global problem, more countries will adopt similar frameworks or join the existing one. The technical standards exist for global use; the challenge is aligning governance and legal aspects across borders. The future outlook section will touch on how this might unfold.

Implementation Challenges for Carriers

Implementing STIR/SHAKEN across a diverse telecommunications infrastructure has presented several **challenges**. These range from technical hurdles (e.g. legacy network compatibility) to operational and economic issues (e.g. costs for small carriers, coordinating multiple carriers). Below, we discuss the main challenges and how the industry has been addressing them.

1. Non-IP (TDM) Networks and Legacy Systems

Perhaps the biggest technical challenge is that **STIR/SHAKEN was built for IP-based SIP networks**, yet many voice calls still traverse **TDM (Time-Division Multiplexing) networks** or other legacy systems (like SS7 signaling). Particularly in rural areas, or in interconnects between older switches, calls might not be end-to-end SIP. If a call travels over a TDM segment, the SIP headers (including the Identity header) might be lost or not transferred, breaking the STIR/SHAKEN verification. As the Ribbon Communications whitepaper succinctly put it: *"The STIR/SHAKEN framework is ineffective if any leg of the call path is TDM"* learn.rbbn.com.

Reasons this is a problem:

- Some small or rural **service providers are not fully IP-enabled**. They might handle calls only via traditional TDM trunks with neighboring carriers, meaning they have no way to carry the SIP Identity headers transnexus.com.
- Many providers that *have* IP networks internally **still use TDM interconnection** for certain routes, or they rely on wholesale transit carriers that use TDM on some legs transnexus.com.
- Even large mobile carriers, which are mostly IP, sometimes send calls through tandem switches or exchange carriers that use TDM. A call could start as VoIP, hit a TDM link, then convert back to IP later. The identity signature won't survive that unless special handling is done.
- **International calls** coming into the U.S. often come over legacy international gateways which may not support passing through STIR headers.

In these scenarios, even a provider who has deployed STIR/SHAKEN can find that a significant portion of their calls still arrive at the destination without a verifiable Identity header (through no fault of their own). This is seen as an **"incomplete coverage"** problem for STIR/SHAKEN. According to industry analysis:

- *"Many calls are routed over call paths that are not SIP end-to-end. The SHAKEN reference architecture will not work for such calls."* transnexus.com. In fact, **any single TDM hop breaks the chain**.
- Specifically, challenges include:
    - Some providers *lack SIP capability entirely* (can't sign or verify) transnexus.com.

- Providers with SIP networks but **TDM interconnects outside their control** lose the STIR info when calls go over those interconnects transnexus.com.
- Even IP providers can have calls that *temporarily leave IP* (e.g., handed to an older carrier) and thus "SHAKEN investment and effort is wasted for such calls" transnexus.com.
- All these cases mean failure to achieve SHAKEN's goals wherever the coverage isn't end-to-end transnexus.com.

To address this, industry experts have been working on **two main solutions**:

(a) Out-of-Band STIR/SHAKEN: This approach involves sending the PASSporT separately from the call when the call itself can't carry it. ATIS-1000096 describes a mechanism where the originating carrier can upload the PASSporT to a trusted database (or send it via HTTPS to the terminating carrier) when a call is routed over a non-IP path learn.rbbn.com. The terminating carrier, upon receiving a call without an Identity header, could query this out-of-band repository (using a lookup key such as the calling and called numbers plus timestamp) to retrieve the PASSporT and then verify it. This effectively tunnels the STIR/SHAKEN data around the TDM segment. The concept has been prototyped; one implementation is known as the "Out-of-Band SHAKEN" service. The benefit is it doesn't require changes to TDM switches; it only requires both ends (originating and terminating carriers) to coordinate via an IP database. However, deployment requires broad adoption of a common out-of-band service or hub, and agreement on protocols. It's an ongoing effort – the STI-GA in 2022 was exploring governance for an out-of-band solution, but as of 2025, it's not yet widely in production.

(b) In-Band TDM Signal Mapping: ATIS-1000095 takes another approach: try to squeeze some attestation information into existing TDM signaling. Traditional SS7/ISUP signaling has a **"Screening Indicator" (SI)** field and possibly some User-User or Generic Address fields that can convey limited info. ATIS-1000095 suggests using the ISUP Screening Indicator (which historically indicates whether the caller ID is network-provided or user-provided, etc.) to map to A/B/C attestation learn.rbbn.com learn.rbbn.com. For example, one value of SI could represent "A attestation," another for B, etc., by bilateral agreement of the carriers. This way, when a call goes into TDM, the originating gateway can set the SI such that when it comes out of TDM on the other side, the terminating gateway can translate that back into an attestation level (even though the actual signature was lost). The obvious limitation is that this only gives attestation, not a full cryptographic signature. It's a hint that could be useful in routing decisions, but it doesn't provide end-to-end verification. Additionally, using the SI for this purpose might conflict with existing uses and requires pairwise agreements. ATIS-1000095 tries to use a field that's not critical for other uses, but it's a

hacky solution. It *"minimizes impact on existing TDM switches"* learn.rbbn.com since it reuses an existing parameter, but it **does not carry the actual PASSporT** – so the terminating side must trust the attestation value without being able to verify the caller's identity cryptographically.

Both approaches have pros and cons. ATIS-1000097 (a report) compared these methods and noted that as of its writing, there was *"no consensus on a single approach"* for non-IP call authentication learn.rbbn.com learn.rbbn.com. The FCC put out a **Notice of Inquiry in October 2022** seeking input on how to handle non-IP networks learn.rbbn.com. The comments were split; some favored out-of-band, others the in-band mapping, and others suggested mandating IP upgrades. The outcome is still pending, but it appears the industry might adopt a combination: out-of-band for calls where both ends support it, and perhaps bilateral in-band agreements in other cases.

In the meantime, the FCC gave non-IP reliant providers an extension (they don't have to implement STIR/SHAKEN until a solution is available, per TRACED Act). However, they cannot just sit idle – they were required to implement a **robocall mitigation program**. Many such providers focus on monitoring and blocking known bad traffic. Still, this is a gap area: as of 2025, calls that traverse outside the IP STIR/SHAKEN ecosystem may not be authenticated. This is one reason why, despite STIR/SHAKEN deployment, consumers still get some spoofed calls – because those calls might be coming through networks where STIR/SHAKEN couldn't be applied. Closing this gap is a high priority moving forward.

2. Integration for Small/VoIP Providers

Smaller voice service providers, including new VoIP entrants, faced challenges in implementing STIR/SHAKEN due to **cost and complexity**. Setting up STIR/SHAKEN involves acquiring certificates, upgrading or installing SIP network elements (STI-AS/STI-VS), and integrating with call platforms. For a small rural telco or a small VoIP reseller, this could be a significant expense. Some specific challenges:

- **Cost of Certificates and Policy Access:** Providers must pay fees to the STI-PA and potentially to STI-CAs for certificates (in the U.S., there's an annual fee based on size/revenues to fund the governance system). While not huge, these fees and the process could be a barrier for very small companies.

- **Equipment Upgrades:** Many small telcos use older switches that may not support SIP Identity header handling. Upgrading to STIR/SHAKEN might mean installing a SIP SBC or software that can do STI-AS and STI-VS functions. That's a capital investment they may have deferred.

- **Expertise:** STIR/SHAKEN is technical; small providers may not have in-house experts. They might be intimidated by managing certificates, configuring servers, etc.

To overcome this, an ecosystem of **vendors and shared solutions** emerged. For example:

- **Hosted STIR/SHAKEN Services:** Companies like TransNexus, Neustar (now TransUnion), Ribbon, NetNumber, etc., offer cloud-based STIR/SHAKEN services. A small provider can route their calls (or at least the SIP signaling) through a cloud service that signs and/or verifies on their behalf. The FCC explicitly allowed this kind of delegation *with conditions* – the provider must still use its own certificate and be responsible for attestation decisions docs.fcc.gov. Essentially, the provider can outsource the technical act of signing, but not the policy responsibility. Many small VoIP providers have opted for this approach – it's often marketed as "STIR/SHAKEN as a Service".

- **Industry Collaboratives:** Some industry groups or larger carriers extended help to smaller ones. For instance, in Canada, smaller carriers could possibly piggyback on bigger ones' infrastructure (though due to policy, they'd still need their own certs). In the U.S., some consortiums or wholesale carriers integrated STIR/SHAKEN into their offerings so that their customers (smaller phone companies) inherit the capability.

- **Open-Source and Softswitch Support:** Projects like Asterisk and FreeSWITCH added STIR/SHAKEN support modules docs.asterisk.org. So a small VoIP provider running a softswitch could implement those modules to start signing calls, using open-source code coupled with a certificate from the STI-PA ecosystem. This helped lower the software cost barrier.

There were also transitional measures: since the FCC gave small providers up to 2023 (and less for some), those who hadn't implemented by 2021 had to file a robocall mitigation plan. Essentially they had to state how they are monitoring and preventing abuse of their network until they do implement STIR/SHAKEN. The FCC signaled that **no provider can avoid STIR/SHAKEN indefinitely**, so by mid-2023 most small providers were rushing to comply or partner with someone who could assist.

Another issue for smaller or new providers is **obtaining telephone numbers and ensuring legitimate use** – STIR/SHAKEN doesn't fix scam calls if the scammer can acquire their own number (e.g., get a VoIP number legitimately and then make scam calls – those would be signed with full attestation!). This is more a policy issue, but it intersects with implementation: there have been cases where lightly-regulated VoIP providers signed calls that turned out to be fraudulent (because the scammers were their "customers"). This revealed a need for better **Know-Your-Customer (KYC)** practices among providers. Some industry initiatives, like **voice service provider vetting**, are being considered (where providers more thoroughly verify who they assign numbers to). In

effect, STIR/SHAKEN shifts some responsibility to the originating provider to police their own customers, since if they sign bad calls, they can be traced and potentially held accountable. Smaller providers have had to grapple with this responsibility, which is new for some.

3. Attestation Assignment and Enterprise Calling

Implementing the attestation levels properly has been tricky in certain scenarios, especially with enterprise call originations and multi-hop call setups. Challenges in this area:

- **Enterprises and PBXs:** When a large enterprise (say a bank's call center) places outbound calls, it might do so through a trunk with a carrier. The carrier knows the enterprise, but the phone numbers used could be from various ranges (some possibly not directly allocated by that carrier). According to SHAKEN rules, the carrier should give these calls B attestation because it hasn't individually verified each calling number belongs to that enterprise (the enterprise might control that on its PBX). However, this means even legitimate enterprise calls often show up as not fully verified (B) which could lead to them being treated with caution by recipients. Enterprises expressed concern that their calls (like important notifications) might be erroneously flagged as spam due to B attestation. The **challenge** was enabling enterprises to have their calls receive A-level attestation.

  The industry solution in progress is **"Delegate Certificates"** or **"Enterprise STIR."** This allows a carrier to delegate a portion of its authority to an enterprise or a Responsible Organization (RespOrg) for toll-free numbers. For instance, the carrier can issue a subordinate certificate to the enterprise (or the enterprise obtains a certificate via a delegate process) which allows the enterprise to sign calls on its own with the carrier's oversight. ATIS and the STI-GA have been working on this: a delegate certificate system was planned (with a target originally in late 2021 for some aspects) sti-ga.atis.org. An enterprise that has a delegate cert and has been vetted for certain numbers could sign its calls, and the carrier's STIR/SHAKEN framework would accept those signatures as attestation A. The FCC in a late 2022 proceeding (Fourth R&O) gave a green light to use of delegate certificates for things like toll-free RespOrgs. As of 2024, the policy and standards are being finalized to implement this. This is an example of a challenge (enterprise calls getting B) leading to an improvement (delegate certs to effectively give enterprises the power to get A-level trust, under controlled conditions).

- **Multi-hop Attestations:** If a call passes through multiple VoIP providers before reaching the terminating carrier, how is attestation handled? Ideally, only the originating provider (closest to the caller) should sign with A/B/C. Intermediate transit providers typically should not re-sign or should pass it through. SHAKEN allows only one signature at a time (though an Identity header

could technically be added by an intermediate if they "stir" it again). In practice, intermediate carriers usually just forward the Identity header. Implementation challenge arises if an intermediate carrier significantly alters the call (like doing a voicemail forwarding, etc.). Standards like the diverted call extension (RFC 8946) and others are helping clarify this. But providers had to adjust processes to ensure they don't strip the headers. Early on, some SBCs needed patches to pass the Identity header (some by default dropped unknown headers). Ensuring **interoperability** across various vendor equipment was a task – by now, most vendors (Oracle, Ribbon, Cisco, etc.) support STIR header handling in their SBC products, after some updates.

- **Over-attestation and Policing:** As mentioned, some providers might be too liberal (e.g., giving A attestation to traffic that's really coming from other carriers, effectively masquerading as the origin). Implementation guidelines (ATIS-1000074) specify what each attestation means, but enforcing that was initially on the honor system. The STI-GA and FCC have since made it clear that mis-attesting calls is a serious violation. In 2022 and 2023, there were instances where certain VoIP wholesalers were found to be giving out A attestation to robocall traffic that they should have labeled C (since it was coming from overseas gateways). The response has been that those providers risk getting their certificates revoked cdn.atis.orgcdn.atis.org. Technical challenge here is partly solved by analytics – companies like TNS and USTelecom's Traceback Group started detecting patterns like "this provider has an unusually high volume of A-attested calls that are then determined illegal." Those patterns trigger investigations. Thus, implementation includes setting up monitoring. From a carrier perspective, they now must maintain systems not only to sign calls but to log and potentially report on how they're attesting calls.

4. Interoperability and Deployment at Scale

Ensuring **interoperability** among dozens (eventually hundreds) of providers' implementations was a non-trivial challenge. STIR/SHAKEN had to work across networks with different equipment and policies. Some factors:

- **Certificate Management and Caching:** Verification services need to retrieve certificates quickly to avoid delaying call setup. If every call triggered an HTTPS fetch of a certificate, that could be a bottleneck. Implementers had to build caching strategies. Standards allow caching of certificates for their validity period. Carriers and vendors implemented local certificate stores. There were also discussions about a centralized cache or distribution – in the U.S., the STI-PA provides a centralized **Certificate Repository (STI-CR)** where all STI-CAs publish their

certs transnexus.com. In practice, many verification services first check the STI-CR for the cert (which contains all certs from all CAs in one place, updated frequently) which speeds things up. Ensuring all this works seamlessly was an initial deployment hurdle.

- **SIP Variations:** Not all carriers SIP interconnect in the same way (some use SIP-I, some SIP-T, etc.). There were minor interoperability issues like how the Identity header is treated in SIP-I encapsulation, or how to handle calls that fork to multiple endpoints, etc. The IP-NNI Task Force put out detailed profiles to standardize these. By following those profiles, carriers achieved compatibility.

- **Testing and Certification:** Industry groups organized interoperability tests (e.g., SIP Forum's STI interoperability events) to allow carriers and vendors to test call signing/verification across networks. This helped uncover bugs early. For example, initial tests showed some issues in verifying tokens with certain character encodings or how the "+" in phone numbers were handled in JSON – those were fixed in implementations.

- **Volume and Performance:** STIR/SHAKEN systems had to be engineered to handle high call volumes without introducing noticeable call setup delay. A digital signature and verification operation is relatively fast (milliseconds), but at telecom scale (millions of calls per hour), it adds up. Carriers had to optimize the cryptographic operations, often using hardware security modules (HSMs) or optimized libraries for signing. According to reports, adding STIR/SHAKEN did introduce a slight increase in SIP call setup time, but if done right it was on the order of tens of milliseconds, which is generally acceptable. Performance tuning was a part of many implementations.

- **Coverage Gaps:** Initially, not every carrier was signing, so a verified call might go through one carrier that strips the header inadvertently. Over time, as more carriers came on board and as enforcement (block if not signed) kicked in, these gaps closed. By late 2022, major carriers reported high percentages of traffic being signed tnsi.com. Interoperability now is high within North America's IP networks.

To sum up, the implementation phase of STIR/SHAKEN required significant industry coordination and technical problem-solving. Legacy network compatibility stands out as the toughest unresolved issue (workarounds exist but not universally deployed yet). Smaller carriers needed help which came in the form of outsourced solutions. Attestation needed careful policies to avoid abuse, and those policies continue to be refined. Despite the challenges, carriers succeeded in deploying STIR/SHAKEN widely by 2021–2022, setting the stage for measurable impacts on call spoofing – which we will explore next.

Industry Adoption, Impact, and Current Status

With mandates in place and technical challenges being addressed, STIR/SHAKEN has now been deployed by a large portion of the telecom industry in North America. This section reviews the current status of adoption (especially in the U.S. and Canada), the observed benefits and impact on robocall/scam mitigation, as well as limitations and criticisms that have emerged.

Deployment Status in 2023 (U.S. and Canada)

In the United States, **industry adoption is extensive**. As of the mid-2020s, all major voice service providers (Verizon, AT&T, T-Mobile, Comcast, Charter, etc.) and the vast majority of smaller and VoIP providers are participating in STIR/SHAKEN. By mid-2021, over 300 service providers had been authorized to obtain certificates from the STI-PA sti-ga.atis.org, and that number has continued to grow. The STI-PA's public list of authorized service providers crossed 550 by 2023 (indicating broad industry coverage, including many regional and rural carriers). There are also 20+ approved STI-CAs now, providing a competitive supply of certificates under governance sti-ga.atis.org.

In terms of call traffic: One metric to look at is the percentage of calls that carry STIR/SHAKEN signatures. Data collected by industry analytics firms indicate that this has risen steadily. **Transaction Network Services (TNS)** reported that by 2022, *74% of calls originating from Tier-1 U.S. carriers were signed* with STIR/SHAKEN tnsi.com. This is significant – the big carriers handle a large share of total call volume, so a majority of those calls now have some level of attestation. Smaller carriers lagged behind initially, but they have improved: TNS's 2023 report noted that smaller and intermediate carriers increased their signing too (21% of their calls signed in 2023, up from 15% in 2022) gsma.com. Overall, by late 2024, roughly **45–50% of all U.S. call traffic was carrying a STIR/SHAKEN signature at termination** transnexus.com. This might seem only half, but remember that includes all unwanted robocalls (many of which come from outside U.S. or non-compliant sources) and also legitimate calls from non-IP networks. Achieving near 50% coverage of all calls in a few years is a strong start.

On the terminating end, carriers have integrated verification results into their consumer call experiences. Most notably, mobile carriers on smartphones: e.g., Verizon's Call Filter, AT&T's Call Protect, and T-Mobile's Scam Shield apps/OS features now display a ✅ checkmark or "[V]" symbol for verified calls. Many VoIP desk phones (for business) also have firmware updates to show a verification indicator on inbound calls. This lets users know when a call has been authenticated. It's not universal across all devices yet (landline phones, for instance, might just get a subtle indicator like an extra piece of caller ID text), but it's becoming more common.

In Canada, all the major telecom operators (Bell, Rogers, TELUS, Shaw, Videotron, etc.) have deployed STIR/SHAKEN since the end of 2021. Canada's CST-GA in its status reports likely shows near-universal signing for IP calls among their members. Because of the no-exemption policy, even small Canadian TSPs had to either implement or partner up by 2022. One practical caveat: Canada has some legacy rural exchanges and one national VoIP interconnect system; if those haven't fully upgraded, some calls within Canada might still be unsigned. But overall, Canada achieved full participation on paper. Canadian carriers also display verified call indicators to customers (for example, Rogers and Bell rolled out "Caller ID Verified" notifications on smartphones in 2022).

One interesting cross-border note: As of the first half of 2022, some fraction of U.S.-Canada calls were being successfully verified across borders. The FCC and CRTC worked to enable this, and indeed **calls signed under the U.S. system can be verified in Canada** and vice versa, since both trust iconectiv as STI-PA (essentially sharing the trust root). There was a formal recognition process via the STI-GA and CST-GA. This makes the U.S.-Canada region the first international deployment of caller ID authentication.

Outside North America, adoption remains minimal as of 2023. A few U.S. carriers have started signing calls to destinations abroad even though the far-end can't verify (for example, U.S. carriers sign everything by default; if that call goes to say the UK, the Identity header is just ignored by the UK carrier). Some global carriers in their labs are testing STIR/SHAKEN for future use. The **GSMA** (mobile carriers association) included STIR/SHAKEN as part of a "Mobile Phone Spam and Scam" working group recommendations for future frameworks gsma.com. So while global adoption is slow, the influence of the STIR/SHAKEN model is spreading.

To summarize current deployment: In the U.S. and Canada, STIR/SHAKEN is broadly deployed among carriers handling the vast majority of calls. Well over a billion calls per day are now signed and/or verified across these networks. This represents one of the fastest industry-wide implementations of a new protocol in telecom history (helped by regulatory push). Of course, **full coverage** is not 100% – remaining gaps include some VoIP fringe operators, TDM-only portions, and international ingress calls which we'll discuss in limitations.

Benefits and Early Impact on Scam Mitigation

STIR/SHAKEN's ultimate purpose is to reduce **illegal spoofing** and make scam/spam robocalls easier to identify or block. While it's still relatively early (a couple of years since broad deployment), there are observable benefits and data points indicating positive impact:

- **Reduction in blatantly spoofed calls:** Scammers who used to impersonate numbers randomly (e.g., neighbor spoofing where they call you from a number similar to yours) now face a hurdle. If they originate calls from a provider participating in STIR/SHAKEN, those calls would either carry a "C" attestation (if coming from a gateway) or fail verification – terminating carriers can then highly suspect or outright block them. Many carriers now automatically block calls that purport to be from area codes or exchanges that are invalid or not assigned, which STIR/SHAKEN helps confirm (no legitimate provider would sign a truly invalid number). The FCC noted that STIR/SHAKEN info can be used to **"protect subscribers from unwanted and illegally spoofed calls"** by allowing blocking of those that fail authentication docs.fcc.gov. In practical terms, industry robocall analytics companies have reported fewer total spoofed robocalls reaching consumers. TNS's data showed unwanted robocall volume in the U.S. **dropped to 70 billion in 2022**, down from an estimated 78 billion in 2021 tnsi.com. While 70 billion is still enormous, this reversal of the growth trend was attributed to **STIR/SHAKEN implementation plus aggressive blocking and enforcement** tnsi.com. It's one of the first declines observed after years of increases.

- **Improved accuracy of call filtering:** Carriers and third-party apps use STIR/SHAKEN verification results as an input to their spam scoring systems. A verified A-level call is unlikely to be flagged as spam (unless there's other evidence it's unwanted), which helps *legitimate* calls get through. Conversely, an unsigned call or one that's signed with C (gateway) is given more scrutiny. This dynamic helps reduce false positives and false negatives in robocall blocking. For example, before STIR/SHAKEN, a legitimate call from a bank might be erroneously blocked if analytics thought it looked like spam. Now, if that call is signed with A attestation by the bank's carrier, the analytics can recognize it as probably trustworthy. This benefit will grow as more enterprises are able to get A-level attestation through delegate certificates.

- **Faster traceback and enforcement:** When illegal calls do get through, STIR/SHAKEN greatly aids **traceback efforts** by enforcement agencies and the USTelecom Traceback Group. The inclusion of the `origid` (origination identifier) in the PASSporT token means that an investigator who has a suspect call can ask the originating provider (via traceback request) to identify the source using that `origid`. Even without `origid`, having the chain of signing helps – the terminating carrier sees who signed the call (which provider), so they know exactly which network to start the traceback with. Before STIR, traceback had to rely on phone records and cooperation step by step which was slower. Now it's more direct. The STI-GA has actively used this capability: in 2022–2023, the STI-GA received complaints from state Attorneys General about certain providers signing large volumes of scam calls cdn.atis.org. Using STIR data, they confirmed misuse and in at least two cases **revoked the STIR certificates** of rogue providers

cdn.atis.org (effectively kicking them out of the authenticated call ecosystem until they reform). One provider had its credentials restored after demonstrating compliance improvements cdn.atis.org. This kind of self-policing was impossible before – you couldn't "ban" a provider from sending calls, but now you can remove their ability to sign calls if they abuse it. Other providers will then treat their traffic as suspect or block it entirely.

- **Consumer Awareness and Trust:** Although hard to quantify, there is an intended psychological benefit: when consumers start seeing "Caller Verified" or checkmarks on calls (particularly from legitimate businesses or known contacts), they can gain confidence in answering those calls. Conversely, when they see no verification, they might be more cautious. Over time, this could improve phone call answer rates for wanted calls and reduce success of scam attempts. It will take continued consumer education, but the pieces are in place. The FCC and carriers have been educating the public that "If you see 'Verified' on your caller ID, it means the call is likely not spoofed." Some smartphones have explanatory text; for example, newer Android phones show "Verified Caller" with a subtext about the call being verified by the carrier. This restores some trust in the medium of calling, which had been deteriorating.

- **Metrics and Early Stats:** A concrete statistic reported by TransNexus (which processes call traffic for many providers) is that by late 2024, about **30.8% of calls were arriving with full A-level attestation**, ~4% with B, and ~9% with C (the remainder unsigned) transnexus.com. Those numbers indicate a large share of calls are now coming in as verified (30.8% A-level as of Nov 2024) transnexus.com. Every one of those calls in theory is a call where the consumer can have higher trust or at least where enforcement can trace quickly if it's abusive. Additionally, data showed that **the percentage of robocalls among A-attested calls was dropping for most providers**, meaning the truly illegitimate call sources were being pushed out of the A-level (either forced to lower attestation or removed) transnexus.com. That's a sign of progress: STIR/SHAKEN is helping isolate bad traffic (often now showing up with C attestation or no signature), which can then be blocked by analytics, while more good traffic can be verified as safe.

- **Case Study – Cross-Carrier Verification:** Shortly after implementing STIR/SHAKEN, carriers started verifying calls across networks. For example, T-Mobile and Comcast in 2019 announced that they could verify calls between their subscriber bases (both had STIR/SHAKEN in place). By 2020, **all the major U.S. wireless carriers were exchanging verified calls** (T-Mobile, AT&T, Verizon did a three-way verification implementation). The result is if you call from one mobile network to another and both have STIR/SHAKEN, the callee might see a "[CallerID] ✅ "

indicator. These carrier partnerships were precursors to the FCC mandate and demonstrated the concept. Now, with the mandate, it's not just select partnerships but industry-wide. Even many VoIP and cable providers are in the mix.

- **Impact on Scam Tactics:** There is anecdotal evidence that STIR/SHAKEN is altering scammer tactics. Some robocallers have shifted to using **non-spoofed numbers** – for instance, obtaining numerous prepaid SIM cards or VoIP numbers and cycling through them (so the number is real and might even pass STIR verification as A). This is a limitation we'll discuss below, but the very fact of this shift indicates that pure spoofing is less effective. In other words, STIR/SHAKEN is making *cheap random spoofing* much harder, forcing bad actors to try costlier or more complex methods (which ideally reduces overall volume and makes them easier to catch when they use traceable numbers).

Ongoing Limitations and Criticisms

Despite the positive steps, STIR/SHAKEN is not a panacea for all robocall issues. Both technical limitations and practical evasions mean that while helpful, it has **limitations**:

- **It doesn't stop all unwanted calls:** STIR/SHAKEN's job is to verify caller ID, not to determine if a call is legal or desired. A verified call can still be a robocall or scam – it just means the number isn't spoofed. For example, a scammer might legally acquire a pool of VoIP numbers and call from those; STIR/SHAKEN will happily mark those calls as verified (attestation A) because the originating provider knows the customer and the number. The content of the call could still be fraudulent ("your car warranty has expired…") even though the number is genuine. As one report put it, *"the signing of a call is a valuable tool, but it is not a silver bullet to preventing unwanted calls."* tnsi.com. The industry recognizes that STIR/SHAKEN must work in tandem with robocall analytics and consumer tools. It mostly helps with *identity-based* blocking (stopping impostor scams where caller ID was the weapon). It doesn't directly address volume robocalls from *legitimate* sources (e.g., telemarketers using their own number).

- **Coverage gaps (international, legacy)** remain: As discussed, calls from non-compliant foreign regions or that transit TDM will lack verification. Scammers are exploiting this by moving operations abroad or routing calls in convoluted ways to pass through networks that strip signatures. The FCC's move to require **gateway providers** to sign calls from overseas with at least a C attestation helps somewhat (it tags the call as foreign-originated) docs.fcc.gov. But ultimately, until other countries implement STIR/SHAKEN or a compatible system, calls from those countries will not be fully verifiable. There is a risk scammers simply move offshore to avoid the U.S. authentication net – indeed, a lot of robocall traffic already comes from overseas

call centers. The system will catch them at the gateway with a C attestation, but distinguishing which foreign calls are good vs bad still relies on analytics beyond just the presence of a C token.

- **Attestation abuse and "verification fatigue":** If some providers improperly give A attestation to calls that shouldn't have it, this can reduce trust in the "Caller Verified" indicator. For example, in early 2022, some smaller VoIP carriers were found signing large volumes of traffic with A that turned out to be illegal robocalls tnsi.com. This **over-attestation** undermines the framework. The industry has been reacting by warning and punishing those providers cdn.atis.orgcdn.atis.org. But it's a game of whack-a-mole to an extent. The good news is that because of certificate revocation ability, there is a real consequence for those abusing attestation – something that didn't exist pre-STIR. The hope is that will deter over-attestation over time. Meanwhile, terminating carriers might start using additional info (like analytics on call patterns) even for calls marked "Verified" to ensure they aren't obviously robocalls (for instance, if a supposedly "Verified" number suddenly makes thousands of short-duration calls, it might be flagged regardless of attestation).

- **Enterprise call display and privacy:** Some have raised concerns about how STIR/SHAKEN interacts with legitimate services like enterprise spoofing (where a call center uses a main number as caller ID for all outgoing calls – that's actually authorized by the enterprise). With STIR/SHAKEN, if the enterprise's provider gives those calls B attestation, some have worried they could be treated as less trustworthy. This is a nuance that is being solved with delegate certificates as mentioned. But initially it led to some enterprise calls not showing as verified, which could be seen as a limitation until the enterprise attestation solution is fully in place.

- **Implementation costs and complexity:** A criticism, especially from small telcos and certain technical experts, is that STIR/SHAKEN introduced a heavy governance and cost overhead (managing certificates, paying fees, updating equipment) that might be disproportionate to the benefit for some smaller or rural areas. Some small carriers argued they had never been the source of spoofed robocalls but still had to spend money to comply. The counter-argument from regulators was that gaps anywhere can be exploited, so everyone needed to play their part.

- **Dependency on centralized authority:** Some internet freedom or security pundits disliked that STIR/SHAKEN created a centralized PKI with a limited set of authorities (FCC-selected GA, a single PA, etc.). They argue this could introduce single points of failure or even be misused (hypothetically, could the government use it to shut off voice service for a provider by revoking

certs? It's not designed for that, but it's a theoretical power). However, in practice the governance is multi-stakeholder and intended for the narrow purpose of stopping spoofing. The upside of central coordination was deemed worth it for this application.

- **Satisfaction of end-users:** As of now, many consumers might not yet perceive a huge difference in unwanted calls – robocall volume is still high (tens of billions annually). Some critics note that **scam robocalls are still rampant**, so they question if STIR/SHAKEN is working. The response from industry is that STIR/SHAKEN is indeed reducing one major vector (caller ID spoofing), but scammers adapt, and thus the fight continues on multiple fronts. STIR/SHAKEN wasn't expected to eliminate robocalls overnight, but to remove the *impersonation* capability which was amplifying their effectiveness. Over time, as enforcement leverages STIR and as more calls get authenticated, it should measurably reduce specific categories of fraud (like IRS scam calls that relied on spoofing the IRS phone number, etc., which should be much harder now).

In summary, STIR/SHAKEN's deployment has brought clear **improvements in call integrity**, but it's not an absolute solution for the robocall problem. It works best in conjunction with other measures. The early data and case studies show it has positive effects – fewer spoofed calls, more traceability, and some reduction in total spam – while also revealing new areas to work on (like dealing with spam from legitimate numbers, integrating with international frameworks, and ensuring no corner of the network is left open to abuse).

The next section will look ahead at how STIR/SHAKEN and related efforts will evolve to tackle these remaining challenges and adapt to emerging threats.

Future Outlook and Evolving Enhancements

STIR/SHAKEN is not a static solution; it continues to evolve through technical enhancements, policy refinements, and potential expansion to new applications. In this final section, we outline the future outlook for STIR/SHAKEN and caller ID authentication broadly – including emerging threats scammers may use and improvements on the horizon to bolster the framework.

Enhancements in Caller Identity: Rich Call Data (RCD)

One promising enhancement is the introduction of **Rich Call Data (RCD)** in the call signaling. While STIR/SHAKEN currently vouches for a phone number, it doesn't convey any information about who is behind the number (beyond what a separate caller ID name database might provide, which is often not trusted). The idea of **PASSporT Extension for Rich Call Data** datatracker.ietf.org is to allow the

caller (if it's a business or verified entity) to include additional data, such as the caller's name, logo, location, and even the reason for the call, within a signed token. This can transform what the call recipient sees: instead of just a number (and maybe a text caller ID name that could be inaccurate), the user could see, for example, a company's name, their logo or brand image, and a short message like "Verification code call" or "Appointment reminder". Because this information would be signed as part of the PASSporT, it can't be easily spoofed – the verification on the receiving end would ensure the data was provided by the legitimate caller's service provider (and possibly that the business itself was verified by the provider).

RCD is currently being standardized (as of 2025, drafts have been through the IETF STIR working group). Some carriers and companies (like Neustar/TransUnion, First Orion, etc.) are already trialing "**branded calling**" solutions which are proprietary but conceptually similar – they work with carriers to display richer info for certain vetted calls (for example, T-Mobile's "Caller Verified Plus" service for businesses). Once RCD via PASSporT is finalized and adopted, it will integrate into STIR/SHAKEN: the call's Identity header will include an extended PASSporT with the rich data. Terminating phones will need software to display that data (smartphones likely will, maybe via carrier apps or OS integration).

The benefit of RCD is twofold: it helps **legitimate callers** reach customers more effectively (people are more likely to answer when they see it's, say, their bank calling about a known issue, with the bank's logo), and it further deters scammers (who won't be able to easily impersonate the rich info of, say, a government agency, since that would require certificate credentials they don't have). In the ongoing war against phone scams, making legitimate calls stand out is key – RCD plus STIR is the way to do that. We can expect to see RCD deployments begin in earnest in the next couple of years, especially in the U.S. where business callers are keen to improve answer rates and regulators encourage any tool that helps differentiate good vs bad calls.

Enterprise Involvement and Delegate Certificates

As discussed in challenges, the need to give enterprises a way to achieve full attestation for their calls has led to the development of **delegate certificates**. The STIR/SHAKEN framework is being extended so that entities like **Responsible Organizations (RespOrgs)** for toll-free numbers or large enterprises can be granted a form of subordinate authority to sign calls on behalf of their provider sti-ga.atis.org.

How this works in practice is becoming clearer: The STI-GA in the U.S. has been setting up policy for what they call "Delegate Certificates and Resp Org Authorization". Under this, if an enterprise or RespOrg undergoes vetting (to prove they control certain numbers and have good practices), an

authorized service provider can request a delegate certificate for them. This certificate would allow the enterprise to sign calls with its own key, which the service provider's systems will recognize and treat as A attestation (because the enterprise is effectively trusted as if it were the provider for those calls). The service provider still has ultimate responsibility – they are the ones enabling it – but it alleviates them from having to directly originate every call.

In October 2021, the STI-GA had aimed to implement a policy to allow delegate certificates for RespOrgs sti-ga.atis.org. Progress was a bit slow due to technical and coordination complexities, but by 2024 the framework for delegate certs was largely in place. The FCC in an order (FCC 22-37, May 2022) specifically paved the way by ruling that delegate certificates could be used and that RespOrgs should be allowed to participate in STIR/SHAKEN to help sign toll-free calls. We expect that in 2025 and beyond, more enterprises and calling platforms (like cloud contact centers) will start using delegate certs to sign calls directly. The end result should be **more calls getting A-level attestation** even if they come from third-party platforms, as long as those platforms are trusted and authorized.

This development is important for *preventing a gap* that scammers could exploit: previously, scammers might hide behind the fact that big providers gave B attestation to a lot of calls (so the scam calls blended in with many legitimate B calls from enterprises). In the future, we hope to see mostly A or C – A for known good calls (including enterprises with delegate certs) and C for unknown/untrusted (like foreign or legacy). B attestation might become rarer, which simplifies filtering (B was always a grey zone).

Expansion to Text Messages?

Robocalls' sibling problem is **robotexts** (spam SMS messages). In recent years, scam texts have also surged. The STIR framework by design was voice/SIP oriented, but the concept of verifying the source of a message is analogous. There have been discussions and some preliminary work on extending caller ID authentication to SMS. For instance, one could imagine attaching a PASSporT token to an SMS or using a separate channel to verify that a text originated from the number it claims.

The TRACED Act actually required the FCC to consider applying caller ID authentication to "non-voice communications" as well, which mainly means SMS. In 2023, the FCC released a Notice of Inquiry on **applying STIR/SHAKEN-like tech to texts**. This is challenging because SMS is an old protocol (SS7 MAP) and doesn't carry arbitrary extra data like SIP does. One concept is to use the SIP-based MESSAGE or RCS (Rich Communication Services) as a vehicle, but SMS is still dominant

and largely not IP in the same way. Alternatively, an out-of-band verification system for texts could be developed (for example, when you get a text, your carrier could query a database to see if it was indeed sent by the owner of that number's carrier).

This is an emerging area. No standard solution exists yet (IETF has no SMS-specific STIR standard as of now). However, given increasing SMS phishing (smishing) problems, we may see innovations or at least more stringent measures on SMS (like requiring registration of 10DLC sender IDs, which is already happening for A2P SMS in the U.S.). So while not exactly STIR/SHAKEN, the spirit of authenticating the source might carry into messaging.

Global Cooperation and Verification Across Borders

A key part of the future will be making STIR/SHAKEN or similar frameworks work internationally. The U.S. STI-GA has mentioned efforts to allow non-U.S. service providers to participate in a controlled way cdn.atis.org. One can imagine a scenario where, say, a trusted carrier in the UK or India could get a certificate recognized by the U.S. governance, allowing their calls to U.S. numbers to be signed and verified. This would require bilateral or multilateral agreements and likely alignment of policy (for example, ensuring those foreign carriers vet callers properly).

One step in this direction: The STI-GA's 2024 report indicates a technical committee is defining requirements to let foreign providers access the list of authorized STI-CAs and the Certificate Revocation List (which implies possibly allowing them to get a cert under the U.S. system or at least trust ours) cdn.atis.org. We might see pilot programs where a foreign gateway signs calls with an "office" in the U.S. trust system. Another path is if foreign regulators set up their own STI-GAs and then cross-certify with the U.S./Canada. For example, if the UK set up a trust authority, perhaps the U.S. could eventually trust UK-signed calls if there's confidence in their system, and vice versa.

It's conceivable that in 5+ years, STIR/SHAKEN (or whatever it might be called globally) could be as ubiquitous as HTTPS certificates on the web – something mostly invisible to users but providing underlying trust. Getting there will require overcoming policy barriers in each country and upgrading tech in places that are behind.

Combating Evolving Scam Tactics

As STIR/SHAKEN closes one door (number spoofing), scammers will look for windows. We already noted some shift to tactics like using real numbers. Here are some potential threats and responses:

- **Scammers using real allocated numbers (no spoof):** This is happening – for instance, scam call centers obtaining blocks of VoIP numbers. They don't spoof random ones; they cycle through their own numbers (which may be rotated or replaced if they get blocked). STIR/SHAKEN will show these as verified because technically they are. The burden then shifts to analytics to identify that, say, number +1-313-555-0123 is originating calls that behave like scams (many short calls, mass volume, lots of consumer complaints) even though it's "verified." This is where **robocall analytics and blocking** still play a crucial role. The industry is integrating STIR data with these analytics: for example, a call can be both verified and labeled "Spam Risk" if it's from a number known to make spam calls. In future, expect these analytics to become more sophisticated, possibly with increased cooperation (e.g., carriers sharing feedback on what numbers might be bad actors even if they are verified).

- **Snowshoeing and number rotation:** Scammers may try to outrun analytics by frequently changing numbers (snowshoe spamming). However, STIR/SHAKEN and related rules make it easier to trace back and cut off the source. If a small VoIP provider is enabling this by giving them numbers, that provider can be flagged. The FCC has shown it will take action in such cases, e.g., telling upstream carriers to block traffic from certain providers if they're facilitating bad traffic. This pressure should incentivize carriers to better police customer behavior (the KYC concept – know who you're giving numbers to and monitor their usage).

- **Integration with call-blocking apps and user feedback:** In the future, verified caller info might allow apps to present simple user feedback options ("Was this call legitimate?" yes/no). If many mark a "verified" call as spam, that can be fed back to possibly revoke the caller's privileges or alert their provider. Essentially, STIR/SHAKEN provides accountability – tying calls to providers – so that feedback can be routed effectively to the responsible party. We may see a tighter feedback loop where unwanted call reports lead to quicker mitigation against the source, using the STIR/SHAKEN identity as the link.

- **New channels and impersonation methods:** Voice calls might not be the only vector – scammers also use voicemail drops, messaging apps, etc. STIR/SHAKEN doesn't cover those. But the general principle of identity verification could inspire similar frameworks in those domains. For instance, there's talk of verifying the origin of WhatsApp or RCS business messages (some of which is done via verification badges by the app platforms). A broad trend is emerging: **identity verification** in communications, to restore trust. STIR/SHAKEN is at the forefront for telephone calls, and its success or lessons will likely inform other channels.

Ongoing Evolution of Standards

The technical standards will continue to be refined:

- The IETF STIR working group has been extending PASSporT for various scenarios. We mentioned RCD and diversion. Another extension under discussion is for **encrypted call identity** – there are cases where a caller might not want to reveal their number to the end user (for privacy) yet still have the call be authenticated for traceback purposes. A draft known as "PASSporT SHAKEN with encrypted origination identity" was floated to allow encryption of the calling number in the token (so it's not visible to eavesdroppers) but still verifiable by authorized parties. This could help with cases like domestic violence hotline calls, etc., where the number should be protected. This might become a standard if consensus is reached.

- The ATIS/SIP Forum IP-NNI task force will likely issue updated versions of SHAKEN standards (v4, v5…) to incorporate delegate certificates, out-of-band references, and any new operational best practices learned.

- There is talk of refining attestation or adding more granular attestation indicators. For example, an idea was floated about an **"E" attestation for enterprise** (meaning call was signed by a delegate enterprise cert) or other differentiators. The aim would be to let analytics distinguish that scenario from a normal consumer A call. However, this might be handled implicitly by certificate info rather than adding new letters.

- **Certificate Revocation and Management:** As the ecosystem matures, there may be upgrades in how revocations are communicated (possibly faster OCSP checks) or how often certificates are renewed. The STI-PA could impose shorter lifetimes if needed for security. Automation of certificate acquisition via ACME has been working well so far.

- **STI-GA Policy:** On the governance side, the STI-GA is reviewing its policies periodically. They recently changed rules to allow suspending a bad actor's cert privileges more flexibly (not just outright permanent revocation but temporary suspensions too). They also improved the process for handling complaints. We can expect the governance to tighten further if new forms of abuse appear.

Finally, one can imagine a future where **most calls worldwide are signed**, and the concept of an unsigned call becomes akin to an unencrypted website with an HTTP URL – technically still possible, but users (or networks) treat it as suspicious. This is likely many years away, but the groundwork is laid. The FCC has even inquired whether at some point they should mandate that terminating providers **block** any unauthenticated calls by default (they haven't gone that far yet, since there are

still legitimate reasons a call might be unsigned, like coming from 911 centers or small rural switches). But as those gaps close, we might see a shift from mitigation to outright prevention: i.e., if it's not signed, it might not be allowed through, period.

In conclusion, the STIR/SHAKEN framework has a strong future trajectory. It represents a major modernization of the telephone system's trust model, bringing it closer to the security we expect on the internet. The fight against robocalls and call spoofing is ongoing, with STIR/SHAKEN being a central weapon. Continued collaboration between industry, regulators, and standards bodies will be key to adapt the system to new needs and ensure that the hard-won progress in restoring trust in phone calls is maintained and expanded in the coming years.

Conclusion

STIR/SHAKEN has emerged as a foundational protocol suite for securing caller ID in the modern telephone network. Through cryptographic call signing (STIR) and a comprehensive implementation framework (SHAKEN), it addresses the long-standing problem of caller ID spoofing that has fueled the epidemic of robocalls and phone scams. This report has explored the background and motivation for STIR/SHAKEN, delved into its technical architecture (from PASSporT tokens and SIP Identity headers to certificate governance and attestation levels), and reviewed the regulatory drivers that made it a reality in the United States and Canada.

We have seen that the **deployment of STIR/SHAKEN**, accelerated by FCC and CRTC mandates, is largely complete across major carriers, with hundreds of providers now signing and verifying calls on a routine basis. Early evidence indicates meaningful benefits: fewer obviously spoofed calls, improved traceback for enforcement, and the ability for consumers to regain some trust in incoming calls marked as verified. At the same time, we've acknowledged the **limitations** – it's not a cure-all for robocalls, and determined scammers will seek out loopholes (such as using real numbers or exploiting non-IP call paths). Implementation challenges like extending coverage to TDM networks and coordinating across borders are actively being worked on by industry task forces and standards bodies.

One of the key strengths of STIR/SHAKEN is that it is **evolving**. The protocol and policies are not static: enhancements like Rich Call Data and delegate certificates are poised to make the system more powerful and flexible, allowing legitimate callers to better identify themselves and enabling the ecosystem to further distinguish wanted vs unwanted calls. As these enhancements roll out, we can expect the utility of STIR/SHAKEN to grow. In parallel, the network effect is important – the more

providers worldwide implement call authentication, the more effective it becomes. In an ideal future, every call will carry some form of verifiable identity, and illegitimate callers will find themselves increasingly shut out.

From an educational standpoint, telecommunications professionals can take away that STIR/SHAKEN is not just a single standard but a *framework involving protocols, operations, and governance*. Successful implementation requires cross-functional consideration: network engineering (to handle SIP headers and signing servers), security (to manage certificates and keys), regulatory compliance (filing certifications, adhering to attestation rules), and customer experience (ensuring that verification results are meaningfully conveyed to end users). It exemplifies a modern telecom solution where industry cooperation and technical innovation intersect.

In conclusion, STIR/SHAKEN represents a critical step toward restoring trust in the voice network. It has transformed the way caller identity is handled – from an honor system prone to abuse, to a secure system backed by cryptography and accountability. While not solving the entire robocall problem, it lays a **foundation for a safer voice communication ecosystem**. Coupled with ongoing anti-robocall efforts (like better consumer tools and stricter enforcement against bad actors), STIR/SHAKEN is making it harder for scammers to hide and easier for legitimate calls to be recognized. The continued evolution and global expansion of this framework will be crucial in the coming years, as the industry strives to stay a step ahead of those who threaten the integrity of our communication networks.

Sources:

- IETF RFC 8224 – *Authenticated Identity Management in SIP* 10dlc.orgdatatracker.ietf.org
- ATIS-1000074 and ATIS-1000080 – *SHAKEN specification and Governance Model* datatracker.ietf.orgcstga.ca
- FCC Report and Order, March 2020 – *Mandating STIR/SHAKEN adoption (FCC 20-42)* en.wikipedia.orgdocs.fcc.gov
- CRTC Decision 2021-123 – *Requiring STIR/SHAKEN in Canada by Nov 2021* fasken.com
- TransNexus Whitepapers – *Understanding STIR/SHAKEN* (technical explainer of call flow, attestation, etc.) transnexus.comtransnexus.com
- TNS Robocall Investigation Report 2023 – *Statistics on call signing and impacts* tnsi.comtnsi.com

- STI-GA 2024 Report – *Governance actions and cross-border efforts* cdn.atis.orgcdn.atis.org
- Ribbon Communications – *STIR/SHAKEN for TDM* (discussion of extending to non-IP) learn.rbbn.com learn.rbbn.com
- FCC Fourth Report and Order (FCC 24-120) – *Clarifying third-party signing arrangements and delegate certs* docs.fcc.govdocs.fcc.gov
- Joint FCC/CRTC statement 2019 – *First cross-border authenticated call and international cooperation* transnexus.comcrtc.gc.ca

---

Tags: stir/shaken, robocalls, caller id spoofing, telecommunications, sip protocol, cryptography, network security, fcc regulations

---

About ClearlyIP

ClearlyIP Inc. — Company Profile (June 2025)

---

1. Who they are

ClearlyIP is a privately-held unified-communications (UC) vendor headquartered in Appleton, Wisconsin, with additional offices in Canada and a globally distributed workforce. Founded in 2019 by veteran FreePBX/Asterisk contributors, the firm follows a "build-and-buy" growth strategy, combining in-house R&D with targeted acquisitions (e.g., the 2023 purchase of Voneto's EPlatform UCaaS). Its mission is to "design and develop the world's most respected VoIP brand" by delivering secure, modern, cloud-first communications that reduce cost and boost collaboration, while its vision focuses on unlocking the full potential of open-source VoIP for organisations of every size. The leadership team collectively brings more than 300 years of telecom experience.

---

2. Product portfolio

- **Cloud Solutions** – Including *Clearly Cloud* (flagship UCaaS), **SIP Trunking**, **SendFax.to** cloud fax, **ClusterPBX OEM**, **Business Connect** managed cloud PBX, and **EPlatform** multitenant UCaaS. These provide fully hosted voice, video, chat and collaboration with 100+ features, per-seat licensing, geo-redundant PoPs, built-in call-recording and mobile/desktop apps.

- **On-Site Phone Systems** – Including CIP PBX appliances (FreePBX pre-installed), ClusterPBX Enterprise, and Business Connect (on-prem variant). These offer local survivability for compliance-sensitive sites; appliances start at 25 extensions and scale into HA clusters.
- **IP Phones & Softphones** – Including CIP SIP Desk-phone Series (CIP-25x/27x/28x), fully white-label branding kit, and *Clearly Anywhere* softphone (iOS, Android, desktop). Features zero-touch provisioning via Cloud Device Manager or FreePBX "Clearly Devices" module; Opus, HD-voice, BLF-rich colour LCDs.
- **VoIP Gateways** – Including Analog FXS/FXO models, VoIP Fail-Over Gateway, POTS Replacement (for copper sun-set), and 2-port T1/E1 digital gateway. These bridge legacy endpoints or PSTN circuits to SIP; fail-over models keep 911 active during WAN outages.
- **Emergency Alert Systems** – Including **CodeX** room-status dashboard, **Panic Button**, and **Silent Intercom**. This K-12-focused mass-notification suite integrates with CIP PBX or third-party FreePBX for Alyssa's-Law compliance.
- **Hospitality** – Including **ComXchange** PBX plus PMS integrations, hardware & software assurance plans. Replaces aging Mitel/NEC hotel PBXs; supports guest-room phones, 911 localisation, check-in/out APIs.
- **Device & System Management** – Including **Cloud Device Manager** and **Update Control (Mirror)**. Provides multi-vendor auto-provisioning, firmware management, and secure FreePBX mirror updates.
- **XCast Suite** – Including Hosted PBX, SIP trunking, carrier/call-centre solutions, SOHO plans, and XCL mobile app. Delivers value-oriented, high-volume VoIP from ClearlyIP's carrier network.

---

3. Services

- **Telecom Consulting & Custom Development** – FreePBX/Asterisk architecture reviews, mergers & acquisitions diligence, bespoke application builds and Tier-3 support.
- **Regulatory Compliance** – E911 planning plus **Kari's Law**, **Ray Baum's Act** and **Alyssa's Law** solutions; automated dispatchable location tagging.
- **STIR/SHAKEN Certificate Management** – Signing services for Originating Service Providers, helping customers combat robocalling and maintain full attestation.
- **Attestation Lookup Tool** – Free web utility to identify a telephone number's service-provider code and SHAKEN attestation rating.
- **FreePBX® Training** – Three-day administrator boot camps (remote or on-site) covering installation, security hardening and troubleshooting.
- **Partner & OEM Programs** – Wholesale SIP trunk bundles, white-label device programs, and ClusterPBX OEM licensing.

---

4. Executive management (June 2025)

- **CEO & Co-Founder: Tony Lewis** – Former CEO of Schmooze Com (FreePBX sponsor); drives vision, acquisitions and channel network.
- **CFO & Co-Founder: Luke Duquaine** – Ex-Sangoma software engineer; oversees finance, international operations and supply-chain.
- **CTO & Co-Founder: Bryan Walters** – Long-time Asterisk contributor; leads product security and cloud architecture.
- **Chief Revenue Officer: Preston McNair** – 25+ years in channel development at Sangoma & Hargray; owns sales, marketing and partner success.
- **Chief Hospitality Strategist: Doug Schwartz** – Former 360 Networks CEO; guides hotel vertical strategy and PMS integrations.
- **Chief Business Development Officer: Bob Webb** – 30+ years telco experience (Nsight/Cellcom); cultivates ILEC/CLEC alliances for Clearly Cloud.
- **Chief Product Officer: Corey McFadden** – Founder of Voneto; architect of EPlatform UCaaS, now shapes ClearlyIP product roadmap.
- **VP Support Services: Lorne Gaetz** (appointed Jul 2024) – Former Sangoma FreePBX lead; builds 24×7 global support organisation.
- **VP Channel Sales: Tracy Liu** (appointed Jun 2024) – Channel-program veteran; expands MSP/VAR ecosystem worldwide.

---

5. Differentiators

- **Open-Source DNA:** Deep roots in the FreePBX/Asterisk community allow rapid feature releases and robust interoperability.
- **White-Label Flexibility:** Brandable phones and ClusterPBX OEM let carriers and MSPs present a fully bespoke UCaaS stack.
- **End-to-End Stack:** From hardware endpoints to cloud, gateways and compliance services, ClearlyIP owns every layer, simplifying procurement and support.
- **Education & Safety Focus:** Panic Button, CodeX and e911 tool-sets position the firm strongly in K-12 and public-sector markets.

In summary

ClearlyIP delivers a comprehensive, modular UC ecosystem—cloud, on-prem and hybrid—backed by a management team with decades of open-source telephony pedigree. Its blend of carrier-grade infrastructure, white-label flexibility and vertical-specific solutions (hospitality, education, emergency-

compliance) makes it a compelling option for ITSPs, MSPs and multi-site enterprises seeking modern, secure and cost-effective communications.

DISCLAIMER