STIR/SHAKEN

Addressing Caller ID Spoofing

Introduction

Robocalls calls are the major source of consumer complaints at the FCC. What was once a nuisance has become a plague to U.S consumers receiving an estimated 3.9 billion robocalls in just January 2022, making this 12 robocalls per person in one month. An estimated 32% were considered as scams.[1]

The FCC allows service providers to block calls identify as fraudulent, but most service providers are preferring to leave the final decision up to the end customer. While call blocking is one part of the robocall solution, another part is identifying bad actors who use robocalls to take advantage of unsuspecting consumers by using numbers assigned to others (spoofing). Bad actors use cheap and accessible technologies to spoof their caller identity and scam victims with threats or free "offers".

Although many voice service providers use homegrown or 3rd party applications to provide call blocking and caller identification verification, the regulatory and industry focus, in North America, has been on caller ID authentication, signing, and verification based on STIR/SHAKEN standards.

This solution brief provides some background on STIR/SHAKEN and details what Ribbon has developed to support our customers implementation of STIR/SHAKEN.

Definitions:

- **STIR** (Secure Telephony Identity Revisited) is the proposed standard developed by IETF that defines a signature to verify the calling number, and specifies how it will be transported in SIP "on the wire."

- **SHAKEN** (Signature-based Handling of Asserted information using toKENs) is the framework document developed by the ATIS/SIP Forum IP-NNI task force to provide an implementation profile for service providers implementing STIR. STIR/SHAKEN will be the basis for verifying calls, classifying calls and facilitating the ability to trust the caller ID information.

[1] https://robocallindex.com

Caller Authentication

The idea behind STIR/SHAKEN is to mitigate unwanted robocalls and bad actors who use caller ID spoofing to increase the chances of successfully scamming subscriber.

STIR is used to enhance the SIP protocol to provide a mechanism for service providers to verify that the originator of a VoIP call is highly likely to be valid (i.e. not a spoofed/fraudulent calling party). The goal of these enhancements is to make it considerably more difficult for bad actors to spoof the identity of a call for malevolent or other purposes. Examples of such activities are spoofing voice messaging or credit card validation services; engaging in confidence schemes by masquerading as legitimate enterprises looking for information or cash (e.g., banks for personal identification or the IRS for swindling); or to get through blocked caller lists (e.g., robocalling).

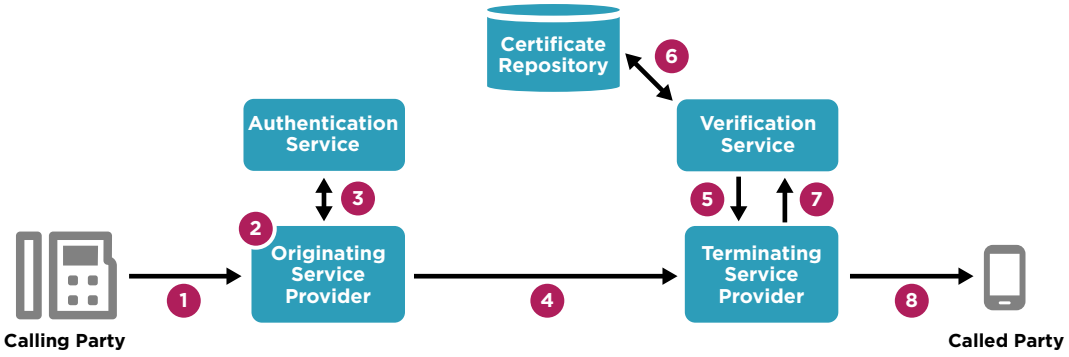

Figure 1: Call Flow Illustrating How STIR/SHAKEN Works

STIR mitigates these problems, but is not a 100% solution. Moreover, STIR does not work in all call scenarios. The following table is a summary of the call scenarios and STIR's contribution to the mitigation of the caller ID spoofing problem.

STIR Calling Scenarios in the U.S.

Originating Network	Terminating Network	Mitigation of Spoofing
PSTN	PSTN	No Impact
SIP-Domestic	SIP-Domestic	High Impact
SIP-Domestic	PSTN	Medium Impact
PSTN	SIP-Domestic	Low Impact
SIP-International	PSTN	Low Impact

In short, STIR was initiated in the U.S. to address compromised identities in SIP-signaled networks. And, the specifics of how the authorization mechanism works, for all practical purposes, will be a U.S.-centric solution for the foreseeable future. "This is because the approach requires one to trust the certificate authority issuing the signing credentials. That is an issue of policy, not technology. As such, that will require industry agreement or regulation, which by its nature will be dealt with by the various national telecommunications authorities."[2] Beyond the US, Canada has issued regulatory rulings mandating STIR/SHAKEN implementation and many other countries are looking at the potential for STIR/SHAKEN in their telecommunications industries.

STIR/SHAKEN does not address calls that originate, transit, or terminate on TDM switches. Yet, because TDM switching still remains in many service provider networks, the industry is now working to define solutions that will extend STIR/SHAKEN to support TDM.

Ribbon Call Trust™ Support for STIR/SHAKEN

Ribbon Call Trust is our Identity Assurance solution providing a complete offer for STIR/SHAKEN. The Ribbon products that apply for STIR/SHAKEN are Session Border Controllers (SBCs), Policy and Routing server (PSX), TDM/IP Gateway (GSX), Call Controllers, and Secure Telephone Identity (STI).

Ribbon SBCs, PSX, and GSX have been validated on their compliance with the caller authentication standards ("Secure Telephone Identity (STI) Test Plan" (TLT-2018-00010), and Authentication and Verification Services) developed by the Internet Engineering Task Force (IETF) and ATIS.

[2] https://s2erc.georgetown.edu/sites/s2erc/files/files/upload/stir_status_and_analysis.pdf

Ribbon STI addresses these specific functions:

- **Secure Telephone Identity** - Authentication Service (STI-AS) and the associated functions of Service Provider Key Management Service (SP-KMS) and Secure Key Store (SKS) to process originating network requests for signed assertion of a caller's identity
- **Secure Telephone Identity** - Verification Service (STI-VS) and the associated function of Secure Telephone Identity Certificate Repository (STI-CR) to process terminating network requests for certificate verification of a caller's identity. Note: Ribbon provides the STI-CR function as a cloud-hosted service on Ribbon Identity Hub
- **Secure Telephone Identity** – Certificate Authority (STI-CA) as a cloud-hosted service on Ribbon Identity Hub. STI-CA provides the following capabilities:
- **Accept SHAKEN Certificate Signing Requests (CSRs)** for new certificates
- **Automatically validate Service Provider Code (SPC) Tokens** and issue standards-compliant SHAKEN signing certificates that include the required Telephone Number Authorization List extension.
- **Revoke certificates if needed and notify the Secure Telephone Identity** – Policy Administrator (STI-PA).

As shown in the Figure 2 below, in an originating service provider's network a session border controller (this could also be a call controller or gateway) will generate and pass an authorization request to the PSX. In turn, the PSX routes the authentication request to Ribbon's STIR/SHAKEN solution. Note also, the PSX interworks with any ATIS-82 certified 3rd party STI solution. Ribbon STI provides all the functions and services required for caller ID authentication and signing and then responds to the PSX authorization request. The PSX will receive signature information and pass that back to the SBC (or gateway or call controller) to be forward to the next network hop.

In the terminating service provider's network the (or gateway or call controller) will generate a verification request and send it to the PSX to be forwarded to the STI function. Ribbon STI provides all the functions and services required for caller ID verification and then responds to the PSX verification request. The PSX will receive the verification information and pass it back to the device requesting the verification.

With Ribbon, our SBC portfolio as well as our gateway (GSX) support flexible handling of error conditions, e.g. “reject the call”, “continue with the call”, “continue with the call and remove Identity header” if signature verification fails.

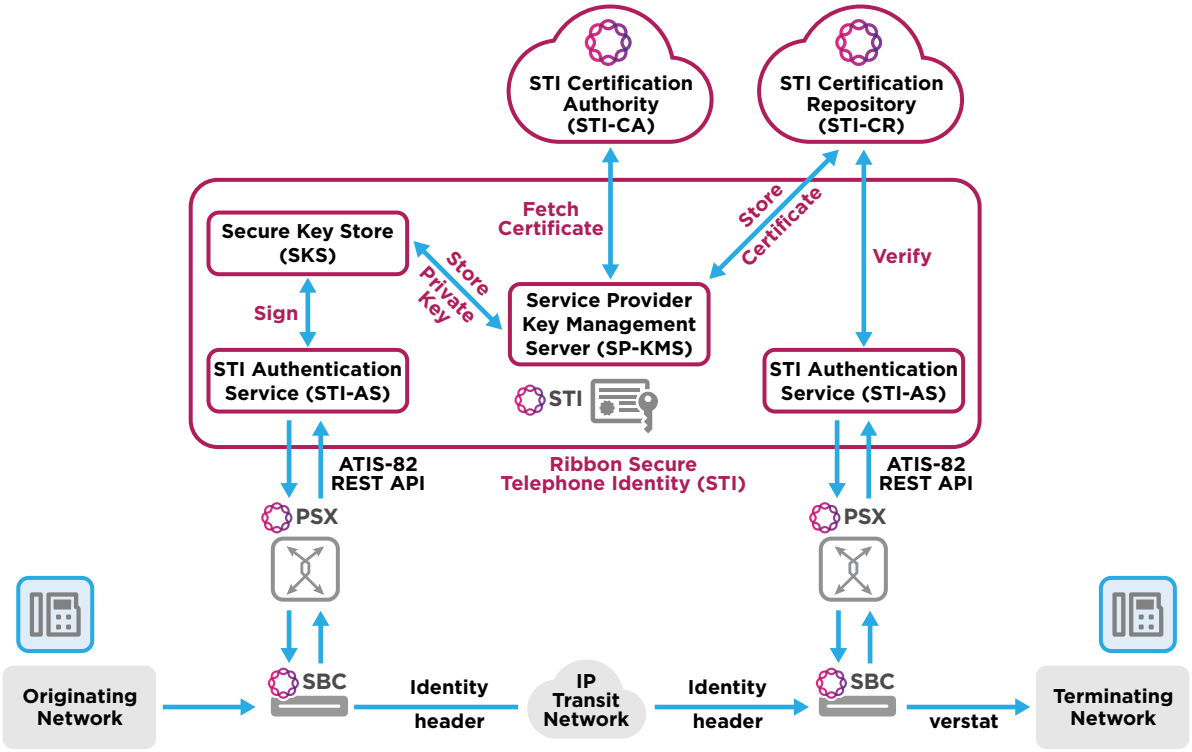

Figure 2. Ribbon STIR/SHAKEN implementation

Summary

Although several providers and third parties offer call blocking and caller identification verification products, there are no simple solutions to address the big challenges of Identity Assurance. Ribbon is leading the way with Ribbon Call Trust to authenticate and verify caller ID in compliance with STIR/SHAKEN, to determine caller intent and reputation, and to provide optimal call validation treatment so consumers regain their confidence in the phone call.

Contact Us Contact us to learn more about Ribbon solutions.

About Ribbon

Ribbon Communications (Nasdaq: RBBN) delivers communications software, IP and optical networking solutions to service providers, enterprises and critical infrastructure sectors globally. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge software-centric solutions, cloud-native offers, leading-edge security and analytics tools, along with IP and optical networking solutions for 5G. We maintain a keen focus on our commitments to Environmental, Social and Governance (ESG) matters, offering an annual Sustainability Report to our stakeholders. To learn more about Ribbon visit rbbn.com.