HyperCube Networks, LLC

HyperCube Networks Guide to STIR/SHAKEN

Overview

Illegal robocalls are a nuisance and a vehicle for bad actors to commit fraud. The recent surge in robocalls is due to the accessibility of tools that enable fraudsters to spoof outbound dialing numbers and effortlessly generate millions of calls. This has led to consumers losing trust in phone calls.

To combat these rampant, intrusive (and sometimes fraudulent) calls, President Trump signed the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act into law on December 30, 2019. The TRACED Act requires service providers help reduce the number of illegal robocalls by implementing STIR/SHAKEN standards for caller I.D. authentication by June 2021.

Communications service providers (CSPs) can use this guide to learn about STIR/SHAKEN framework and how it works in order to prepare for implementation.

Table of Contents

Communication Excellence

https://www.west.com/**HyperCube-Networks**

Background

STIR, known as **S**ecure **T**elephony **I**dentity **R**evisited and SHAKEN, **S**ecure **H**andling of **A**sserted information using to**KEN**s, are telecom industry standards that allow communication service providers (CSPs) to cryptographically sign calls in the SIP (Session Initiation Protocol) header.

STIR: Secure Telephony Identity Revisited

STIR is a set of technical standards developed by the Internet Engineering Task Force (IETF), which verify that a calling party is authorized to use a specific telephone number.

SHAKEN: Signature-based Handling of Asserted information using toKENs

SHAKEN is a framework developed by the Alliance of Telecommunications Industry Solutions (ATIS) for service providers to use when implementing STIR-using IP networks.

STIR/SHAKEN was created as a tool to help reduce the number of illegally spoofed calls, fight against malicious robocalling and protect consumers against fraud and abuse and ultimately rebuild trust in the communications industry.

With STIR/SHAKEN, calls are authenticated by the originating service provider, then verified by the terminating service provider, allowing consumers to have greater confidence that the call is authentic.

It is important to note that STIR/SHAKEN is not a technology that blocks all suspect calls, as not every automated solicitation call is deemed illegal. Calls from charities or debt collectors, for example, are often permissible. STIR/SHAKEN is a tool to provide indications of when calling fraud may be occurring. And STIR/SHAKEN provides a tool that service providers may use in their fraud investigations and in their call-blocking programs for illicit calls.

Carriers have already started implementing the STIR/SHAKEN protocol to verify callers and numbers, which should cut down on the number of robocalls received.

STIR/SHAKEN Call Flow, Authentication/Attestation and Verification Process

A service provider may be the originating service provider (OSP), the terminating service provider (TSP) or neither. The latter case would be an intermediate service provider where the OSP is earlier in the call path (upstream) and the TSP is later in the call path (downstream). The OSP performs authentication, intermediaries (if any) pass the authentication from the OSP and the TSP performs verification.

STIR/SHAKEN Attestation

A. Full Attestation: The signing provider:

- Is responsible for the origination of the call onto the IP- based service provider voice network.
- Has a direct authenticated relationship with the customer and can identify the customer.
- Has established a verified association with the telephone number used for the call.

B. Partial Attestation: The signing provider:

- Is responsible for the origination of the call onto the IP-based service provider voice network.
- Has a direct authenticated relationship with the customer and can identify the customer.
- Has NOT established a verified association with the telephone number being used for the call.

C. Gateway Attestation: The signing provider:

- Has no relationship with the initiator of the call.
- Examples include non-SIP originations and international gateways (originations from outside the United States).

HyperCube Networks' Role

HyperCube Networks is committed to the deployment of STIR/SHAKEN and enhancing the framework as a standard. This is an important tool that will assist in the fulfillment of our goal of completing America's telephony traffic while ensuring the integrity of those calls to consumers.

Partnership with Ribbon and Neustar

To ensure the highest protection for our customers, we have partnered with Ribbon Communications (Ribbon) and Neustar to combat robocalling and call spoofing with enhanced tools.

The Ribbon and Neustar partnership provide the leading integrated solution to implement STIR/SHAKEN and mitigate spoofed calls and robocalls. Leveraging Ribbon and Neustar solutions, HyperCube Networks delivers a comprehensive tool to quickly detect suspicious calls and notify business and consumer customers of potential illegal robocalls and spoofed calls.

Both companies are developing tools to guide businesses and service providers through these industry changes. Neustar, for example, has created the ATIS Robocalling Testbed. This tool is part of the company's Trust Lab and serves as the industry interoperability test facility to validate the effectiveness of caller authentication standards that have been developed by the Internet Engineering Task force and The Alliance for Telecommunications Industry Solutions (ATIS). ATIS that developed SHAKEN to mitigate call spoofing on cloud-based networks. Any CSP with an assigned operating company number is eligible to participate in the Testbed.

Summary

As leading CSPs, carriers and IT providers embrace collaboration with one another they will help to deliver comprehensive tools to quickly detect suspicious calls and notify businesses and customers of potential illegal robocalls and spoofed calls. By doing so, they will help restore trust in the communications industry.

If you have questions or concerns about STIR/SHAKEN, please feel free to contact HyperCube Networks support.

Glossary

Customer: Typically, a service provider's subscriber, which may or not be the ultimate end-user of the telecommunications service. In the context of the SHAKEN attestation model, the Customer is the entity with a direct business relationship and a direct user-to-network interface with the OSP. Enterprises, hosted/cloud service providers, Over the Top (OTT) providers and other service resellers may be considered customers of an OSP depending on the use case.

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

Hosted/Cloud Service Provider: Entity providing telephony services for multiple business entities, either using calling TNs supplied by them to the business entity or provided by the business entity in a Bring Your Own Number (BYON) model. These include hosted Private Branch Exchange (PBX), Unified Communications providers, Communications Platform as a Service (CPaaS) providers, Contact Centers, etc. In the context of the use cases described in this document, the hosted/cloud service provider is considered the "Customer" of the OSP. Note that a hosted/cloud service provider could also be an OSP and not a separate entity.

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

OTT Provider: Entity providing telephony services for end users via OTT mechanisms, which require PSTN interworking in order to support calls to traditional called parties on the public network. Similar to cloud service providers, these entities may provide TNs to their customers or support BYON capabilities. In the use cases described in this document an OTT provider is considered a Customer of the OSP.

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

Terminating Service Provider (TSP): The SP whose network terminates the call (i.e., serving the called party). The TSP performs the SHAKEN Verification function.

TN Reseller: Entity that is assigned TNs by a TNSP and in turn provides those TNs to various entities (e.g., end user enterprises, contact centers, cloud providers, OTT providers, and other service resellers) that behave as TN Customers or may also resell TNs to other TN Resellers who serve those customer entities. A TN Reseller may also act as a service reseller or serve in the role of other SP types.

About HyperCube Networks

HyperCube Networks develops innovative, cloud-based technology to make it easier, more effective and efficient to deliver connections that count in this increasingly complex world. Our solutions connect people with each other and the information needed to gain insights for better decisions on the issues that matter most.

HyperCube Networks has sales and/or operations in the United States, Canada, Europe, the Middle East, Asia Pacific, Latin America and South America. HyperCube Networks is controlled by affiliates of certain funds managed by Apollo Global Management, LLC. For more information, please call 1-800- 841-9000 or visit https://www.west.com/hypercube-networks.

HyperCube Networks, LLC