

Cleod9 Voice

STIR/SHAKEN Policy

PURPOSE: FCC rules require providers to implement STIR/SHAKEN in the Internet Protocol (IP) portions of their networks by June 30, 2021, so that Americans can benefit from this important technology and start to have faith in their phone calls again. As of April 20, 2021, the FCC requires that all providers certify in the Robocall Mitigation Database that they have fully implemented STIR/SHAKEN or have instituted a robocall mitigation program to ensure that they are not originating illegal robocalls.

DA/FCC #: FCC-20-42

Docket/RM: 17-97, 20-67

FCC Record Citation: 35 FCC Rcd 3241 (4)

GOAL: Present evidence to the FCC as to the reasonable effort taken by Cleod9 Voice to implement STIR/SHAKEN as it pertains to the regulations listed above. Cleod9 Voice implements strategies, combined with partnerships with other carriers, to implement STIR/SHAKEN under the “reseller” designation. Our mission is to provide a quality service to our customer by preventing fraudsters from scamming consumers or businesses through robocalling and illegal phone number spoofing, while ensuring that legitimate calls reach the intended recipient or our customer. Prior to this FCC regulation, Cleod9 Voice was compliant by using legitimate caller ID information, utilizing telephone numbers that were owned by either Cleod9 Voice or our customer, and by avoiding business deals involving illegal robocalling entities.

Table of Contents

- I. INTRODUCTION
- II. Outbound STIR/SHAKEN call flow & attestation
- III. Inbound call flow & verification
- IV. Analytics engines and call blocking
- V. PBX Programming

Cleod9 Voice

STIR/SHAKEN Policy

I. INTRODUCTION

To combat the abuses of robocalling, Cleod9 Voice is actively working to implement the most robust call origination and termination possible, while also working diligently to stop illegal number spoofing from its service.

We, through our carrier Bandwidth, have adopted a three-pronged operational approach to stop and prevent illegal robocalls, while also expanding on industry efforts and best practices, as well as aligning with the Federal Communications Commission's (FCC) guidance.

Prevention

We and our carrier are working vigorously to prevent unlawful robocalls originating from our network. We have implemented a stringent screening process that prevent companies with potentially fraudulent robocalling traffic from becoming customers. We have also informed and empowered our customers with the information necessary to identify these unlawful calls, as defined by the FCC.

Detection

We, and our carrier, have an extensive fraud mitigation team dedicated to identifying and analyzing potential robocall campaigns on our network and determining if they are lawful or not. In alignment with the FCC rules, Bandwidth is in the midst of augmenting its robocall detection technology that identifies and blocks unlawful robocalls from traversing our network.

Mitigation

Once an unlawful robocall campaign is detected, Bandwidth takes several steps to stop all current and future unlawful calls. They have developed call blocking tools that prevent calls with specific unlawful ANI/'FROM' TN characteristics from traversing the Bandwidth network. Bandwidth personnel regularly analyzes network traffic looking for unlawful robocall campaigns and utilizes our call blocking tools when appropriate. We work diligently with our customers to stop all detected unlawful robocall campaigns and proactively communicate with those customers that may be in the path of unlawful robocalls.

Cleod9 Voice

STIR/SHAKEN Policy

II. Outbound STIR/SHAKEN call flow & attestation

During an outbound call:

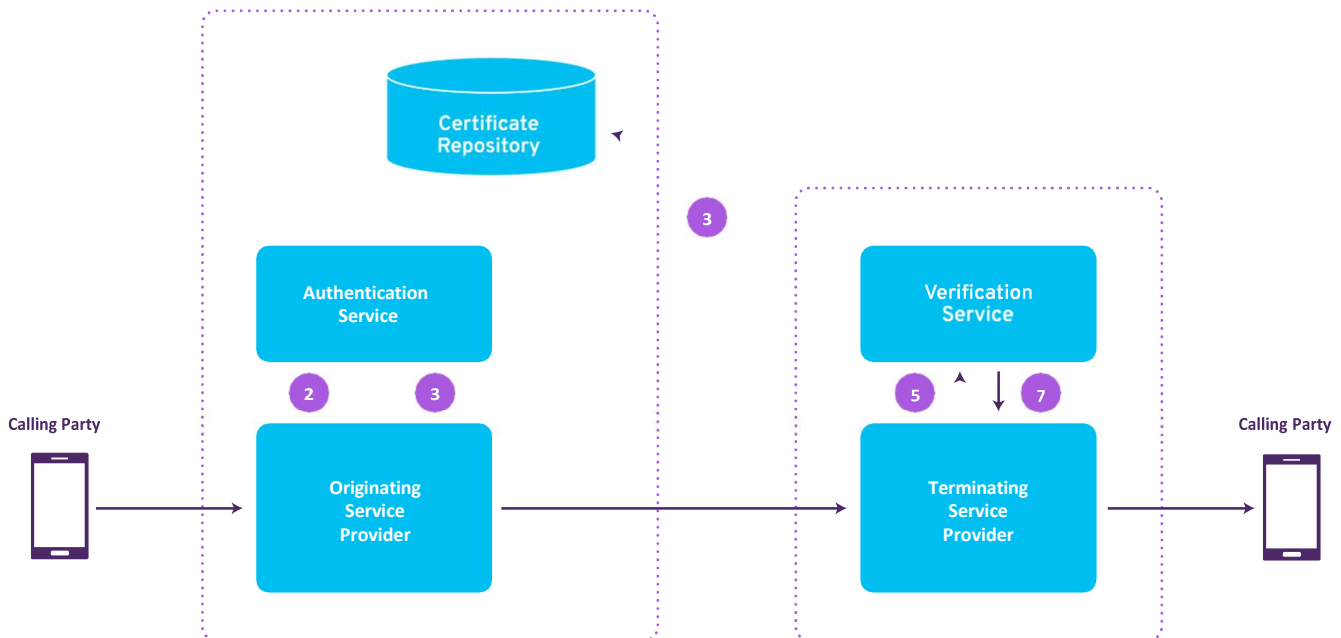
1. A SIP INVITE is received by the originating service provider (OSP)
2. The OSP looks at the call source (the customer) and the calling number to determine how best to sign (or attest) based on the validity of this information
3. To sign calls, approved service providers (like Bandwidth) must be vetted by the STI Policy Administrator (STI-PA) and issued a digital STIR/SHAKEN certificate by a STI Certificate Authority (STI-CA)
4. Attestation is determined by the following parameters:

Attestation Level	Industry (ATIS) Standard	How Bandwidth Assigns Attestation
Full or “A”	The service provider knows the customer and their right to use the phone number	You are a Bandwidth customer using a Bandwidth phone number
Partial or “B”	The service provider knows the customer, but not the source of the phone number	You are a Bandwidth customer using another provider’s phone number • 3rd-party contact center using enterprise’s phone number • Calling-on-behalf-of (COBO) home device using mobile number • Legitimate number spoofing (caller ID appears from one phone number but call is originated from another number)
Gateway or “C”	The service provider has originated the call onto the network but can’t authenticate the call source e.g., international gateway	Bandwidth does not currently attest any calls as “C”

Cleod9 Voice

STIR/SHAKEN Policy

5. The originating service provider sends a SIP INVITE to an Authentication Service (STI-AS)
6. The Authentication Service returns the SIP INVITE with a SIP Identity Header containing a PASSporT header, PASSporT payload, PASSporT signature, encryption algorithm and location of Certificate Repository
7. Included in the SIP INVITE is the:
 - a. Calling number
 - b. Number being called
 - c. Current date/timestamp
 - d. Attestation level
 - e. Unique originating identifier (Orig ID) for traceback
8. The SIP INVITE with the Identity Header is sent to the terminating service provider (TSP)



III. Inbound call flow & verification

For inbound calls to the terminating service provider (TSP), the SHAKEN framework outlines the steps to decode and validate the call:

1. The TSP sends the SIP INVITE with the Identity Header to a Verification Service (STI-VS)
2. The Verification Service obtains the digital certificate using a public key from a Certificate Repository
3. The Verification Service decrypts the SIP Identity Header and compares it to the SIP INVITE using the public key of the certificate from the Certificate Repository
4. The call is reviewed using several validation parameters to confirm:

Cleod9 Voice

STIR/SHAKEN Policy

- The digital signature is valid
- The caller ID matches information the SIP header
- The originating service provider has a valid certificate
- The originating service provider has the right to use the telephone number

5. Freshness check on date/timestamp

- This information is conveyed as a verification status or VERSTAT with three potential results:
- TN-Validation-Passed: the call met all the validation conditions
- TN-Validation-Failed: the identity header failed the verification step
- No-TN-Validation: the identity header was valid but the call did not have “A” level attestation

IV. Analytics engines and call blocking

Attestation provides a level of validation to the call within the STIR/SHAKEN framework. Analytics, on the other hand, is software used by carriers to enable call blocking or spam detection. Analytics must take attestation into consideration but are not included in the STIR/SHAKEN standards. In other words, analytics can be used along with attestation when determining whether to complete or block a call.

Different analytics solutions have different decision-making parameters and may or may not treat STIR/SHAKEN information the same from one analytics provider to the next. For this reason, calls that are signed with an “A” aren’t necessarily guaranteed to be delivered by any given service provider. At the same time, calls that are signed with a “B” may not automatically be blocked.

Let’s examine this issue using the diagram below. A call that is signed with an “A” is likely to be terminated without any issues. However, there are certain types of legitimate calls that may be marked as suspected spam or blocked by terminating carriers anyway. For example, a high volume of calls from a single number in a short timeframe (such as a school district sending mass notification to parents), could result in an analytics decision to block a call.

Cleod9 Voice

STIR/SHAKEN Policy

The good news is that calls signed with a “B” attestation that don’t fall into the problematic use cases should be fine. However, calls that are partially signed AND are flagged by the analytics providers are very likely to fail verification and be blocked by the terminating service provider.

In addition to STIR/SHAKEN information, analytics tools often take other indicators into account. Things like whether the calling number has aged, is experiencing a low answer seizure ratio (ASR) or has initiated a high number of short duration calls. They can also factor in crowdsourced information that may indicate a number that’s associated with fraudulent activity.

V. PBX Programming

Utilizing specific programming through the Wildix Platform built in AWS, Cleod9 Voice has complete control over outbound caller ID information on a company and per user base. At no time does Cleod9 Voice place information inside of the outbound caller ID fields where that number is not specifically owned by the customer or user.

Since Bandwidth uses IP address whitelisting in order to provide a SIP Trunk connection, each caller ID is controlled through Bandwidth. Those SIP trunks are then programmed specifically for each PBX that exists in a live environment in the trunk section of the Wildix programming portal.