Robocallers, SPAM, and Nuisance Callers

OVERVIEW

Fraudulent calls and robocallers are on the rise. The federal Do Not Call (DNC) list only matters if the caller is scrupulous but has otherwise become useless because fraudsters don't follow the law and easily manipulate the called from number, often making the call appear local by spoofing numbers in the same area code or even same NPANXX. The FCC estimates that 47% of the approximately 5 billion robocalls made per month are fraudulent [1] . This does not mean that all automated calling ("robocalling"), also known as an outbound dialer, predictive dialer, etc, is unlawful. In fact, Evolve IP helps our clients gain efficiency by offering outbound dialing products. The difference is whether the called-from number legitimately belongs to the caller or that the caller has the right to use the called-from number for legitimate purposes. (on behalf of their client, etc).

Pallone-Thune Act and Spammers

WHAT THE GOVERNMENT IS ASKING FOR

In mid-2019 the FCC began asking service providers to implement a technology that authenticates the caller at the start of a call, and a means by which the service provider of the called number can verify that identity and either (1) block the call or (2) identify it as a possible SPAM call in the caller ID, and on 12/30/2019 the President of the United States signed into the law the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act. which gives service providers like Evolve IP 18-months to implement the technology.

CURRENT STATE (STIR/SHAKEN)

To meet the requirements outlined by the Pallone-Thune Act the industry had been working on a solution, which has resulted in a technology known as STIR/SHAKEN, which stands for **S**ecure **T**elephony **I**dentity **R**evisited and **S**ecure **H**andling of **A**sserted information using to**KEN**s), and is documented in RFC 8588.

The STIR/SHAKEN protocol works similar to how web browsers authenticate webpages using digital certificates, with some minor differences. Instead of the server giving its certificate and the client (browser) determining the certificate's authenticity, STIR/SHAKEN will include an encrypted token, sent in-band in the call's SIP messaging and/or via an out-of-band API message, that the terminating carrier will use to validate the authenticity of the caller. This will occur on a call by call basis and the level of authenticity will be dependent on the caller. The following diagram shows an overview of the authentication process: [2]

HOW STIR/SHAKEN WORKS IN A NETWORK
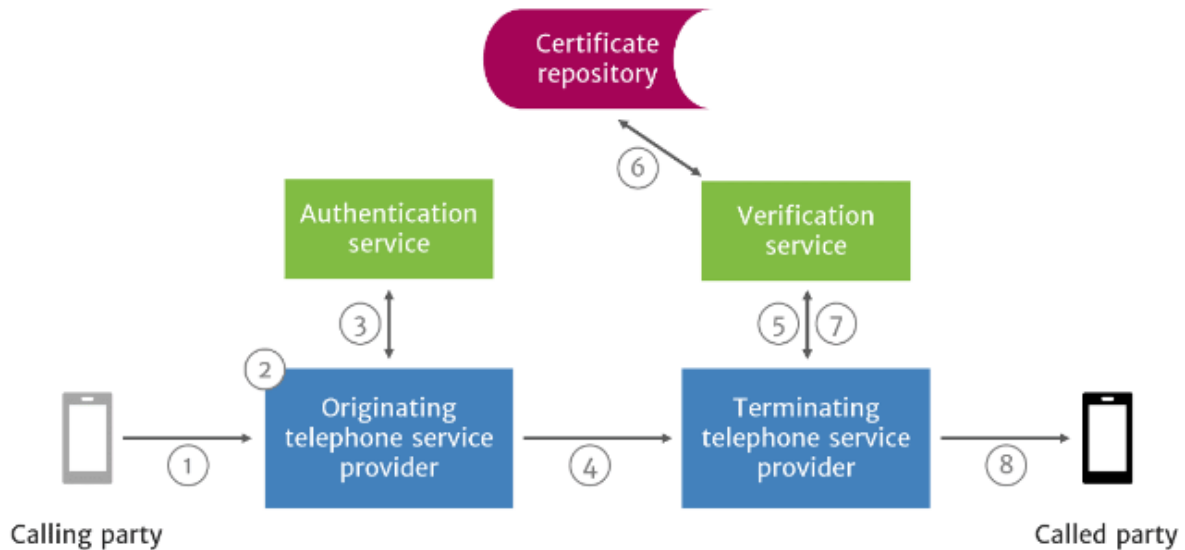
- **Attestation** on outbound calls on originating calls. Attestation may be one of three possible levels:
  - **Full Attestation (A):** The service provider has authenticated the calling party and they are authorized to use the calling number.
    An example of this case is a subscriber registered with the originating telephone service provider's softswitch.
  - **Partial Attestation (B):** The service provider has authenticated the call origination, but cannot verify the call source is authorized to use the calling number.
    An example of this use case is a telephone number behind an enterprise PBX.
  - **Gateway Attestation (C):** The service provider has authenticated from where it received the call, but cannot authenticate the call source.
    An example of this case would be a call received from an international gateway.

EVOLVE IP's POSITION

Currently there are two methods to authenticate calls for STIR/SHAKEN.

- In-band STIR/SHAKEN which includes encrypted token (PaSSporT) in the SIP request
- Out-of-band STIR/SHAKEN leverages a database referred to as a "Call Placement Server" to store encrypted tokens (PaSSporTs)

Evolve IP has already implemented Out of band STIR/SHAKEN which when leveraged by destination carrier will have full attestation (A)

This is illustrated below

OUT-OF-BAND SHAKEN CALL SCENARIO
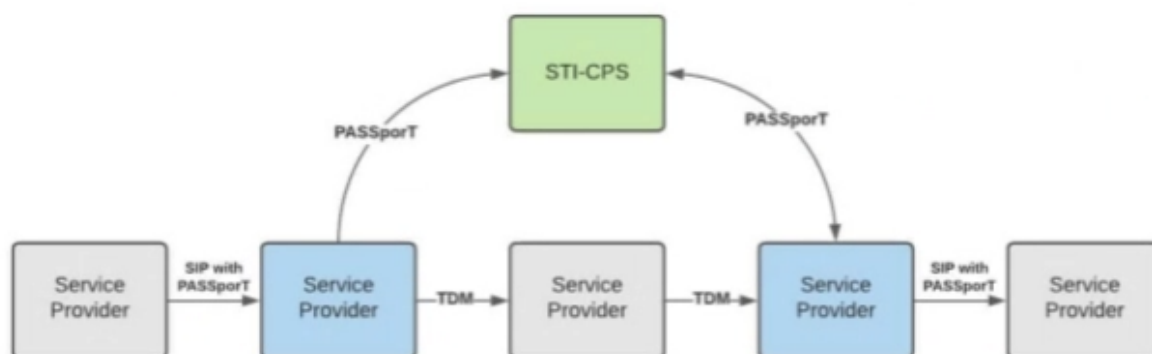
Evolve IPs network carriers also provide partial attestation (B) through In-Band STIR/SHAKEN

In 2022 Evolve IP will be making network upgrades so that they can also provide full attestation (A) through In-Band STIR/SHAKEN

WHAT YOU CAN DO NOW

If you are receiving unwanted SPAM / robocalls inbound

- **UCaaS** - in OSSmosis, you can block numbers at the Location level: Telephony Set Up / Location / Actions (icon bottom right corner) / Blocked Numbers
- **CCaaS (ECS)** - to block a number in the Evolve Contact Center (ECS) refer to: **ECS Setup: Blocking an Inbound Number**

What to do if your number is incorrectly marked as a SPAM / robocaller

It is up to the destination carrier to determine methods for authenticating calls (in-band, out-of-band or both) and which calls they mark as "Possible SPAM"

Evolve IP can only guarantee that an encrypted token for full attestation (A) is posted to the out-of-band call placement server and that our outbound carriers also include the partial Attestation (B) when it leaves their network.
If you receive reports that your calls are being marked as SPAM please contact our support team so they can validate both of the above have occurred.

It is also possible for you to request that a carrier whitelist your number. Below is a list of the major US cellular carriers with links to request numbers to be removed from the SPAM list. We will endeavor to update this list periodically as new portals are made available.

AT&T Wireless	https://hiyahelp.zendesk.com/hc/en-us/requests/new
Verizon Wireless	https://voicespamfeedback.com/vsf/
T-Mobile	https://reportarobocall.com/trf/
First Orion, Hiya, TNS	https://www.freecallerregistry.com/fcr/