The Evolution of STIR/SHAKEN

Where It Came from, and Where It's Going

Summary

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.

STIR/SHAKEN is a series of protocols and a governance framework that ensure caller ID has not been spoofed, ultimately reducing the number of illegal robocalls. The industry began with STIR and has added SHAKEN to address this problem.

History of STIR

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.

SIP was introduced in early 2000s, and as SIP adoption increased, so did robocalls. To address the growing issue, the IETF turned to cryptographic tools that provide a way to assert a caller's identity by using certificates to authenticate the caller. However, STIR did not define the ecosystem or establish how carriers should implement these standards.

History of SHAKEN

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. SHAKEN introduces a governance model that designates the roles and responsibilities of the policy administrator (STI-PA) and certificate authority (STI-CA), and it outlines who is eligible to receive certificates (US carriers with OCNs). It also defines additional data fields not included in STIR that enable traceback capabilities and a level of trust (attestation) based upon the carrier's relationship to the telephone number.

How Does STIR/SHAKEN Work?

The Players

Federal Communication Commission (FCC): Primary authority for Communications law, regulation and technological innovation. Composed of 5 members who are appointed by the President and serve a 5 year term.

Governance Authority (GA): acts as a board of directors that influences policies and standards. The GA is made up of industry representatives from carriers (large and small) and equipment manufacturers.

Policy Authority (PA): The PA is a trusted steward selected by the governance authority that manages the enforcement of issuing tokens to carriers. To enable STIR/SHAKEN, a carrier needs to first obtain a token from the PA to prove it is an authorized service provider.

Certificate Authority (CA): The certificate authority are trusted third parties approved by the PA that issues certificates to carriers wishing to originate calls. To ensure the requestor is eligible for a certificate, the CA first validates the credentials of the organization requesting the certificate with the PA.

Originating Service Provider: As part of STIR/SHAKEN specification, the originating service provider is the service provider that attests to ownership of a phone number that originated from its network. This enables the terminating service provider to "trust" that the call was originated from a valid source and was not spoofed.

Terminating Service Provider: This is the service provider that has a relationship with the call recipient. The terminating service provider validates that the call information has not been tampered with and completes the call.

The Setup

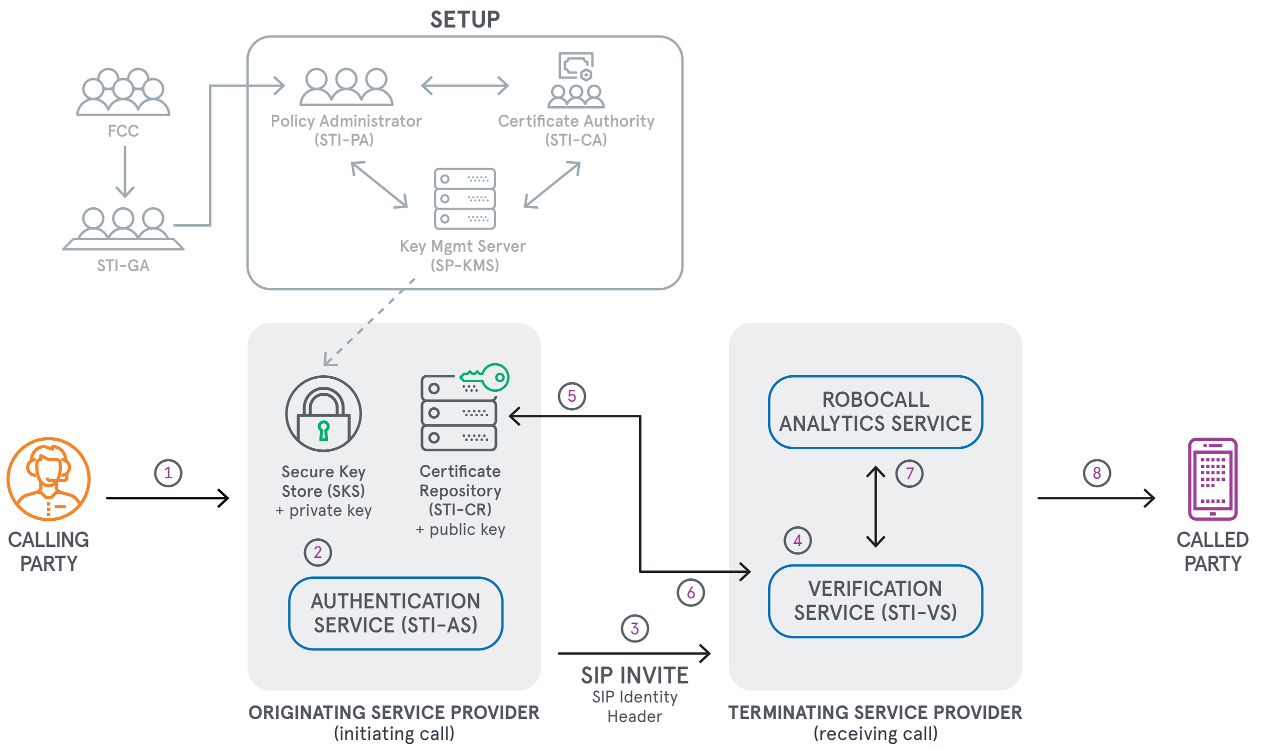
The originating service provider obtains a token (credentials) proving it is who it says it is, and then shares with the CA to get a certificate. The token is a form of identity that enables the carrier to receive a certificate that allows the originating service provider to digitally sign its calls.

Below are the steps required:

- Originating service provider requests a token from the PA
- PA grants originating service provider a token
- Originating service provider sends the token to the CA and requests a certificate
- CA validates the identity of the originating service provider requesting the certificate with the PA
- Originating service provider generates a key pair
- CA wraps a cerificate around public key and sends to the Originating Service Provider
- Originating service provider uses the certificate to authenticate (sign) calls

This process establishes a chain of trust so that the recipient of the call can be confident that the caller ID has not been tampered with.

HOW STIR/SHAKEN WORKS


SETUP
FCC
STI-GA
Policy Administrator (STI-PA)
Certificate Authority (STI-CA)
Key Mgmt Server (SP-KMS)
CALLING PARTY
1
Secure Key Store (SKS) + private key
Certificate Repository (STI-CR) + public key
2
AUTHENTICATION SERVICE (STI-AS)
ORIGINATING SERVICE PROVIDER (initiating call)
5
6
3
SIP INVITE
SIP Identity Header
ROBOCALL ANALYTICS SERVICE
7
4
VERIFICATION SERVICE (STI-VS)
TERMINATING SERVICE PROVIDER (receiving call)
8
CALLED PARTY

1. A user wants to originate a call
- Calling party dials number of called party they wish to reach
- Calling party device sends request to their service provider

2. Originating service provider invokes authentication service
- Authentication service validates the relationship with calling party
- Assigns attestation level (A, B, C)
- Generates SIP Identity Header (PASSporT) using authentication service and private key, obtained from SKS, to sign (authenticate) call

3. Originating service provider sends SIP INVITE to terminating service provider

4. Terminating service provider invokes its verification service

5. Initiates a service request to the originating service provider’s certificate repository for a certificate and public key

6. Originating service provider returns certificate and public key
- Verification service validates the call is from an authenticated source
- Examine certificate issuer to ensure from originating service provider
- Validates CA that issued certificate is from the list in Trust Store approved by policy administrator

7. Examines robocall analytics to determine if TN is known spammer

8. Terminating service provider sends attestation level (ABC) and completes call

SHAKEN Attestation

ATTESTATION LEVELS EXPLAINED

SHAKEN attestation is the "trust" or "proof" that a call is not spoofed based on the originating service provider's relationship to the telephone number. There are three different levels of attestation:

A. FULL ATTESTATION

Service Provider A to Service Provider B:

"This is my customer. I gave them this telephone number. This call originated on my network."

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

Service Provider A to Service Provider B:

"This is my customer. This call originated on my network. However, I did not give them this telephone number."

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 used for the call

C. GATEWAY ATTESTATION

Service Provider A to Service Provider B:

"This call originated outside my network.

The signing provider:

- has no relationship to the initiator of the call (e.g., international gateways).

The SHAKEN attestation value can be used as an input to robocall analytic algorithms to determine the riskiness of a call.

Now What?

STIR/SHAKEN utilizes a combination of technical, legal, and behavioral solutions; it's an evolving process that continues to be refined in order to address the dynamic needs of the marketplace. Expected upcoming improvements include the support of non-IP networks, enterprise multi-carrier implementation, and standardizing how attestation is displayed on devices.

Excerpt from Nuestar documention.