

OneNet Global - Robocall Mitigation Program Description

OneNet Global utilizes Bandwidth.com for originating calls to fully comply with the STIR/SHAKEN requirements.

If you've followed the communications industry at all over the past few years, you probably heard about STIR/SHAKEN. It's a technology framework that seeks to reestablish trust in voice communications by taking a stronger stance against practices like illegal spoofing for malicious robocalling to help protect consumers against fraud and abuse.

What is STIR/SHAKEN?

The Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act was signed into law on December 30, 2019, to address the problems of robocalling and illegal phone number spoofing. The

FCC's implementation of this law includes requirements for Service Providers to implement robocall mitigation solutions within 18 months of the passage of the law, or June 30, 2021.

Secure Telephone Identity Revisited (STIR) and Secure Handling of Asserted information using toKENS (SHAKEN) are telecom industry standards designed to enable service providers to cryptographically sign (or attest) calls in the Session Initiation Protocol (SIP) header.

The process uses a trusted public key infrastructure to enhance the integrity of the originating call identifying data sent across networks. With STIR/SHAKEN, SIP headers will include a level of confidence indicator from the originating service provider to signal whether the party originating the call has the right to use the number via the attestation field.

There are 3 levels of attestation that can be indicated by the originating service provider:

- **Full (A) Attestation** - the service provider has authenticated the customer originating the call and they're authorized to use the calling number.
- **Partial (B) Attestation** - the service provider has authenticated the customer originating the call but can't verify they're authorized to use the calling number.
- **Gateway (C) Attestation** - the service provider has authenticated from where it received the call, but can't authenticate the call source (e.g., International Gateway call).

In addition to the attestation level, the originating service provider provides data in the header to facilitate traceback identifying where the call entered their network.

What is the driving force behind STIR/SHAKEN adoption?

Fraud and abuse in the form of robocalling and, in particular, illegally spoofed robocalling, is the number one consumer complaint to the FCC. STIR/SHAKEN is just one tool in a broader industry initiative that seeks to prevent bad actors from exploiting businesses and consumers.

At the same time, consumers expect and demand the successful delivery of relevant communications, such as school closure notifications or prescription reminders.

Bandwidth is actively engaged in efforts to implement the most robust call authentication framework possible, while also working diligently to stop the transmission of illegal robocalling on our network holistically. We continue to lead industry efforts and best practices, including a three-pronged operational approach (prevent, detect, and mitigate) to stopping illegal robocalls.

Read more about Bandwidth's [approach to fighting telecom fraud](#).

What is the difference between STIR and SHAKEN?

STIR is a working group within the Internet Engineering Task Force (IETF), an organization that develops and promotes internet standards. STIR produces the internet standards that form the basis of what is referred to as STIR/SHAKEN, including:

- [RFC 8224](#)
- [RFC 8225](#)
- [RFC 8226](#)

SHAKEN defines the extensions and industry framework for the deployment and interworking of the technology in service provider networks. Additional draft standards are currently being developed to target use cases beyond the scope of those addressed by SHAKEN ([ATIS-1000074.v002](#)).

How does STIR/SHAKEN work in a call path?

When originating a call on the network, the originating service provider's Secure Telephone Identity Authentication Service (STI-AS) creates an encrypted SIP identity header that includes the following data:

- Attestation level
- Date and time
- Calling number
- Called number
- Orig ID for analytics and/or traceback
- Location of certificate repository
- Signature
- Encryption algorithm

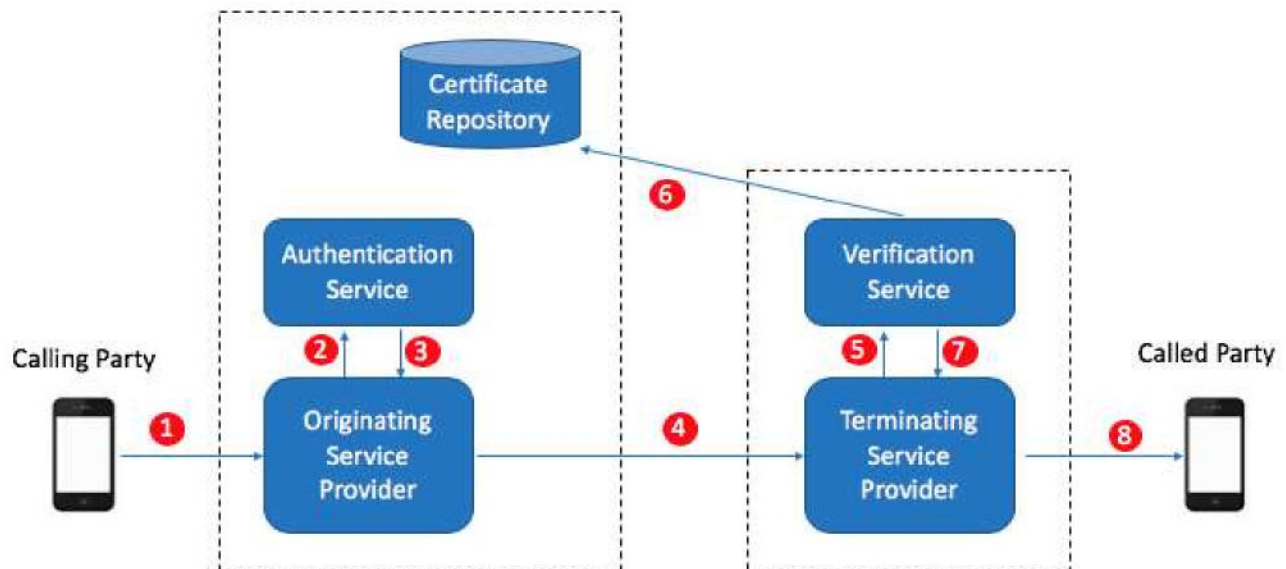
The SIP INVITE with the SIP Identity header is sent by the originating service provider and received by the terminating service provider.

The terminating service provider invokes an STI Verification Service (STI-VS) to decode the SIP identity header and perform verification of the data transmitted in the call. Depending on the results of the verification, information can be passed in a verification status or verstat parameter indicating the results of the verification step.

The call is completed to the receiving party with potentially some optional treatment like a display that is dependent on the level of attestation and the resulting verification. For example, this could be “valid number” or green checkbox for a fully attested call, or labeled as “possible spam” for a gateway-attested call without full attestation.

The following diagram shows the high-level call flow for SHAKEN calls:

STIR SHAKEN Call Flow



1. SIP INVITE is received by the originating service provider who looks at the call source (customer) and calling number to determine the level of attestation to provide for the call.
2. The originating service provider sends SIP INVITE to the authentication service.
3. Authentication service returns SIP INVITE with SIP Identity Header containing PASSporT header, PASSporT payload, PASSporT signature, encryption algorithm, and location of certificate repository.
4. SIP INVITE with Identity header is sent to the terminating service provider.
5. Terminating service provider sends SIP INVITE with Identity header to Verification Service.
6. Verification Service obtains the digital certificate with the public key, decodes the identity header, and verifies that the originating service provider is authorized to originate calls for the calling number.
7. Verification Service returns results indicating whether the Identity Header was valid and whether TN Validation passed, failed, or wasn't performed.
8. The terminating service provider completes the call to the called party.

How is Bandwidth signing calls?

- Outbound calls from Bandwidth customers using U.S. phone numbers in their account are signed with “A” or full attestation.
- Outbound calls from Bandwidth customers using phone numbers that are not in their account are signed with “B” or partial attestation.
- Bandwidth doesn't currently sign any calls with “C” or gateway attestation.

