04:72:47:09:1B:62:3C:9F:A
9:21:67:55:82:E9:01:92:3D:
43:F5:8E:B3:2B9

BANDWIDTH EBOOK

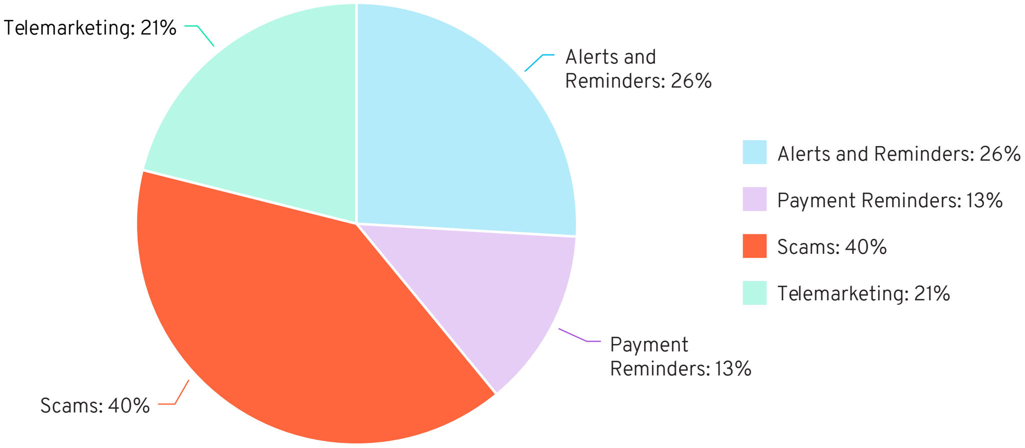
Guide to STIR/SHAKEN for Service Providers

04:72:47:09:1B:62:3C:9F:A9:21:67:55:8
2:E9:01:92:3D:43:F5:8E:B3:2B:0E:0F:E
D:C0:C3:98:C4:31:C9:FE:C5:C3:79

bandwidth

Introduction

Telecom fraud, including robocalling and phone number spoofing, costs 32.7 billion dollars worldwide. There are more than 4 to 5 billion robocalls made each month in the U.S., and robocall mitigation software provider YouMail estimates that as many as 40% of those calls are fraudulent.



To address the persistent and pervasive problem of robocalling in the U.S., the FCC has adopted rules for caller ID authentication requirements, based in large part upon the STIR/SHAKEN standards. The FCC issued its initial rules in March 2020, giving telecommunications service providers until June 30, 2021 to implement a STIR/SHAKEN solution.

This guide is intended to assist communications service providers (and their enterprise customers) in understanding the STIR/SHAKEN framework and its current limitations. Because STIR/SHAKEN is rapidly evolving in advance of the June 2021 deadline, this guide focuses on defining STIR/SHAKEN and answering some of the most common questions we hear in our regular conversations with our customers.

Table of contents

What is STIR/SHAKEN?

STIR/SHAKEN is a technology framework designed to help reduce fraudulent robocalling and illegal phone number spoofing.

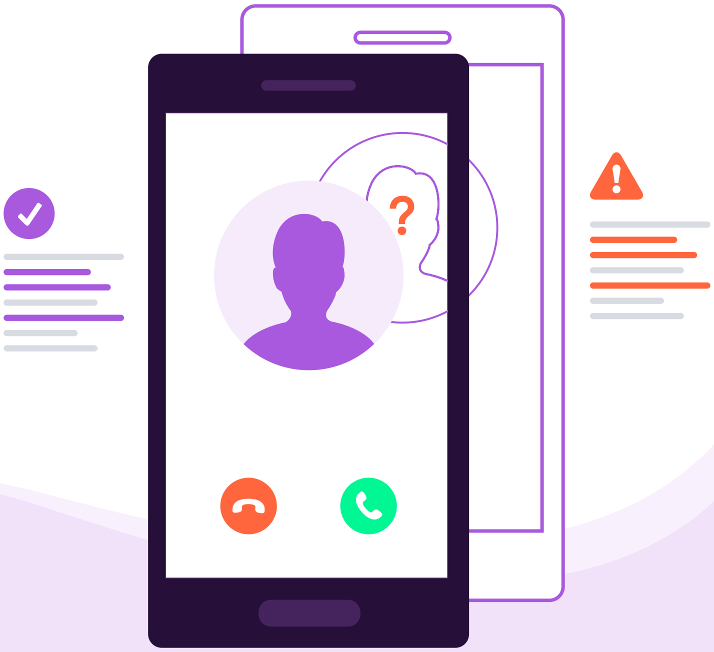
Secure Telephone Identity Revisited (STIR) are the protocols that allow service providers to create a digital signature for a call that includes calling party information. It also allows the digital signature to be verified by the terminating service provider or party. The STIR protocols were developed by the Internet Engineering Task Force (IETF) working group.

Secure Handling of Asserted Information Using toKENs (SHAKEN) is the framework for how STIR is to be deployed service providers within their networks.

The Alliance Telecommunications Industry Standards (ATIS) has developed three key standards that form the basis of STIR/SHAKEN:

- ATIS-1000074 - Secure Handling Of Asserted Information Using toKENs (SHAKEN)
- ATIS-1000080 - Secure Handling of Asserted information using toKENs
- (SHAKEN): Governance Model and Certificate Management
- ATIS-1000084 - Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators

Let’s look at the steps involved with signing a call that aligns with the standards.



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"

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

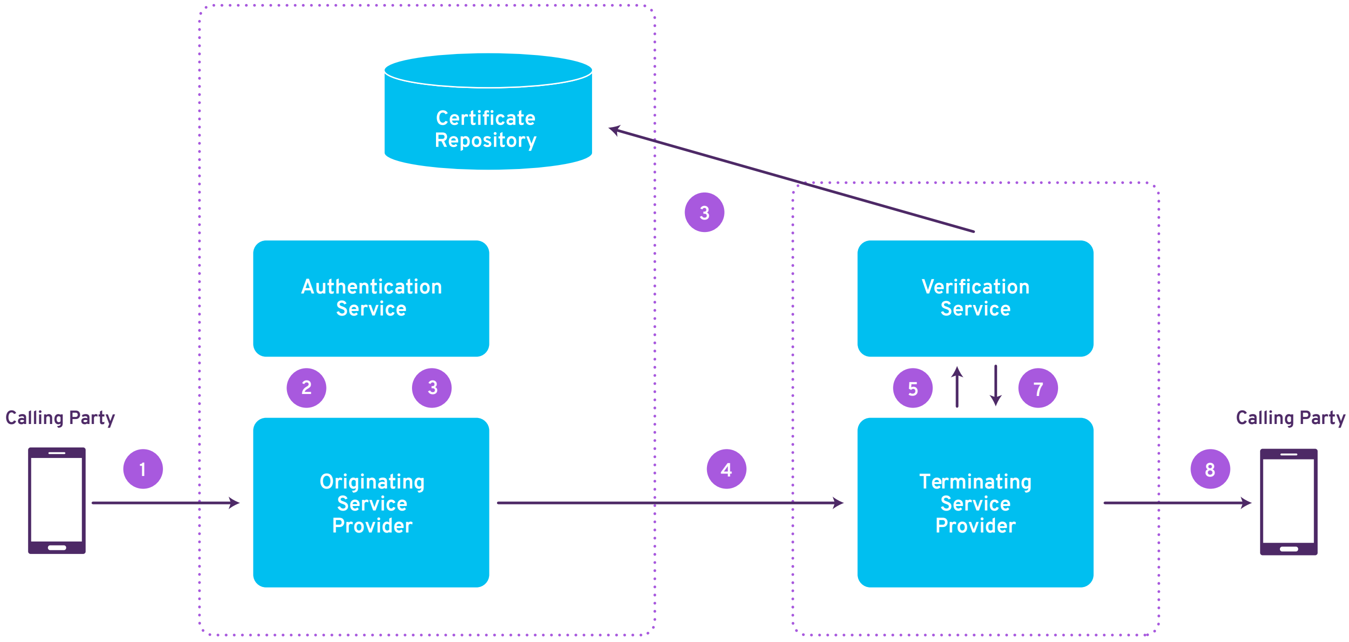
7. Included in the SIP INVITE is the:

   - Calling number
   - Number being called
   - Current date/timestamp
   - Attestation level
   - Unique originating identifier (Orig ID) for traceback

IDENTITY HEADER

```
Identity:
eyJhbGci0iJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1Ijoi
aHR0cHM6Ly9iYW5kd2lkdGgtc2hha2VuLXRlc3QtY2VydHMuczMuYW1hem9uYXdzLmNvbS9id3NoYWtl
bmVuZHVzZXJjZXJ0LnBlbSJ9.eyJhdHRlc3Qi0iJBIiwiZGVzdCI6eyJ0biI6WyIxMjA2MzM0OTUwMS
JdfSwiaWF0IjoxNTgwODQ1OTI3LCJvcmlnIjp7InRuIjoiMTk4NDM4OTE5MjgifSwib3JpZ2lkIjoiM
jkyNGU2MDMtODFkOC0zNmE5LWExNTItYTc3YmE3MDY1NmYyIn0Lq4T-fdajsWBNFtHiBd6xYErgY7nat
C0VCbXz7ZjqZh91j8v9NSduwyqP72YJ35jH2ZHh9sRuaX8m67wkReFLw;info=<https://bandwidth-
shaken-test-certs.s3.amazonaws.com/bwshakenendusercert.pem>;alg=ES256;ppt=shaken
```

8. The SIP INVITE with the Identity Header is sent to the terminating service provider (TSP)



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:
    - 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

The SIP validation information appears as:

```
sip:+19843891928;verstat=TN-Validation-Passed@67.231.3.4 3:5060;user=phone
```

Inbound call treatment

Once verification is complete, the receiving party can determine whether to deliver the call based on attestation level, VERSTAT results, and third-party analytics. Potential options include:

- Complete the call
- Complete the call and alert the recipient to its validity i.e., mark call identified as spam with an “X” and mark a valid call with a green
- Block the call

At this time, analytics engines do not factor in attestation level in the decision to block calls, but that will likely change once STIR/SHAKEN is widely deployed. If you’re currently having trouble with blocked calls, please refer to Bandwidth’s support article with resources to help whitelist calls with the Tier 1 carriers.

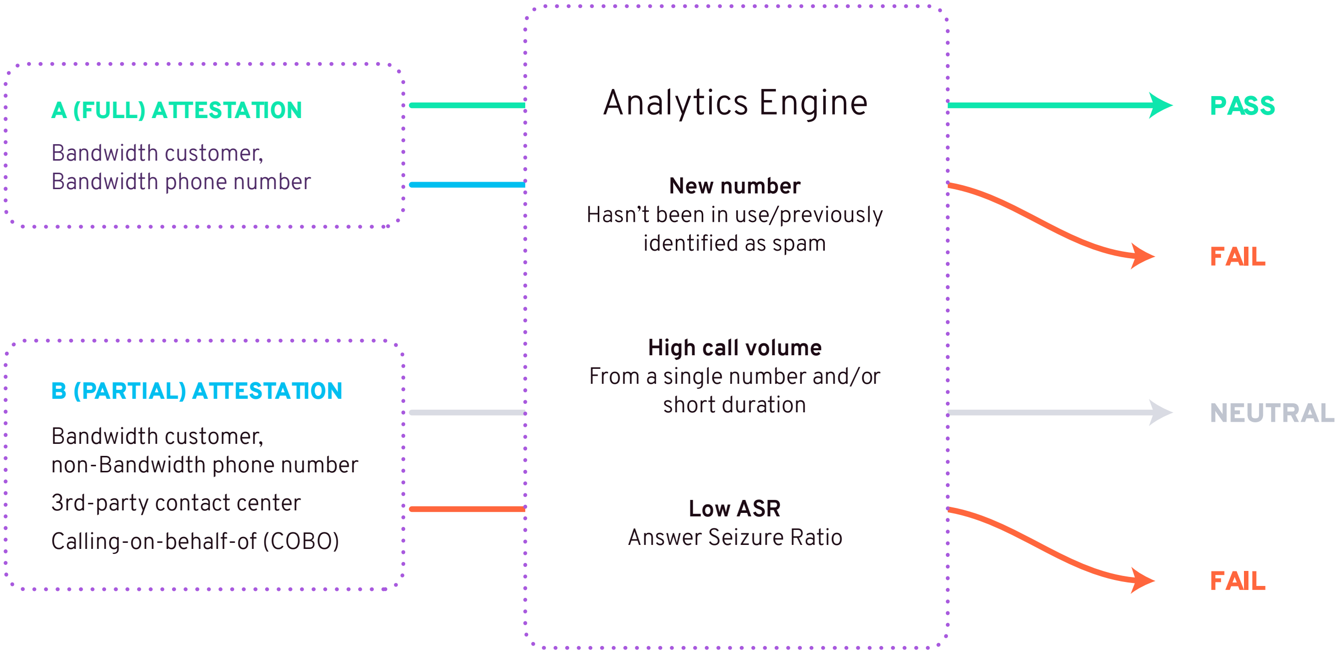
Speaking of analytics engines, attestation and analytics are frequently confused concepts, so let’s take a look at how they will work together in a STIR/SHAKEN call.

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.



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.

Addressing valid partial attestation use cases

Work within The Alliance Telecommunications Industry Standards (ATIS) has resulted in several proposals for additional improvements in the STIR/SHAKEN framework, all with the goal of elevating trust in the attestation of calls. As of this writing, we expect that two such improvements are poised to be incorporated into the overall framework very soon:

- Certificate delegation
- Central Telephone Number Database or “registry”

Certificate delegation

Certificate delegation is a further technical standard that ATIS recently formally adopted that is intended to allow a telephone service provider (delegating from) to create a digital certificate for its approved customers (delegating to) to use only with authorized telephone numbers. For example, if you’re a Bandwidth customer for outbound voice calling, with proper authorization you’ll be able to direct us to a valid delegated certificate from your alternate numbering provider. Then we would invoke our local policy to sign such calls with an “A” attestation.

In November 2020 Bandwidth (and several other providers) signed a letter to the STIR/SHAKEN Governance Authority (STI-GA) urging the incorporation of ATIS certificate delegation standard into the governing framework policies.

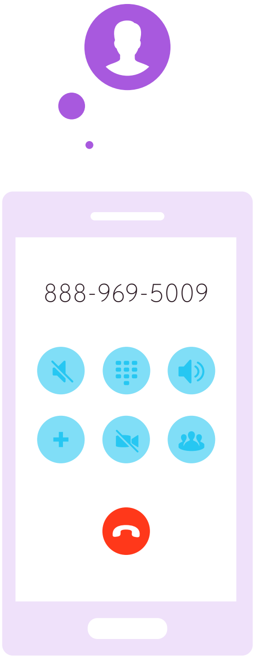
Bandwidth is currently running a proof of concept for using certificate delegation, and expects to have a solution generally available in Q1 2021.

Central Telephone Number Database (CTND)

The CTND is another potential enhancement to the framework. The concept is an industry-authorized repository of TNs created and mapped to participating enterprises. Each enterprise is assigned a unique identifier. The carrier or IVoIP provider supplying phone number resources would update the database when an enterprise requests a new number, and the originating service provider would access the database to confirm the enterprises' right to use that TN. It would also include any delegated authorities for the enterprise such as a 3rd-party contact center.

Both of these potential options would help validly elevate the level of attestation for legitimate use cases—ones that might otherwise receive partial attestation. So it's important for service providers to determine whether they must fully deploy their own STIR/SHAKEN solution or whether they can partner with aanother service provider to enable STIR/SHAKEN call signing.

Do you need to sign your own calls?



The desire by service providers to sign calls directly is usually fueled by concerns that legitimate but partially attested calls will be blocked by a downstream provider.

Because Bandwidth has implemented STIR/SHAKEN in our network, we're able to support most of our customers' requirements for call signing, but we certainly understand the question and the concern. In a STIR/SHAKEN world, certain traffic may be partially attested either because the provider relies on least cost routing (LCR) or has enterprise customers who legitimately spoof or mask the calling party phone number.

An example would be a physician (or a 3rd-party contact center) calling a patient from their cell phone, while the patient's caller ID displays the number of the medical practice. Because of this, many service providers may want to have their own control over how their calls are signed.

What's involved in signing your own calls

Getting approved to sign your own calls is a considerable undertaking. The current token access policies set the requirements for LECs and Interconnected VoIP (IVoIP) providers to obtain a Service Provider Code (SPC) token to sign calls as:

- A 499A on file with the FCC
- An Operating Company Number (OCN)
- Numbering Authority approval from the FCC (See note below)
- Completion of a STI-PA Test Plan with the Policy Administrator (iconectiv)
- Obtaining valid certificates from an approved Certificate Authority (e.g.: Neustar, TransNexus, NetNumber
- Implementation of a STIR/SHAKEN solution in your network

NOTE: In November 2020, the STIR/SHAKEN Governance Authority (STI GA) announced a new policy that will eliminate the requirement to obtain Numbering Authority from the FCC. The new policy states that service providers must certify with the FCC either that they have implemented STIR/SHAKEN or that they have a robocall mitigation program in place. The new policy is likely to come into effect in March 2021 when the FCC is expected to make an online portal available for certification applications.

Some providers and consulting firms appear to be offering services to assist IVoIP providers with filing the necessary paperwork outlined here for fees that can range from $5K to $10K and take anywhere from 7 to 9 months to finalize.

Even if you are able to obtain IVoIP numbering authority, you will also ultimately need to deploy a STIR/SHAKEN solution in your network, which obviously represents additional costs and associated allocation of resources. Most importantly, this includes the ongoing responsibility for management and compliance in the evolving STIR/SHAKEN ecosystem.

Finally, having STIR/SHAKEN deployed within your network is not a guarantee that calls won't be blocked by a terminating provider. While the FCC has required that STIR/SHAKEN be at least taken into account, as we discussed in the previous section, analytics engines don't rely on STIR/SHAKEN attestation alone for call treatment decisions.

If you choose to sign your own calls...

While most of our customers work with Bandwidth for their STIR/SHAKEN call treatment, a few of our customers have begun the process of call signing, or are taking the steps necessary to obtain their own certificates. To support customers that want to go in this direction, and in keeping with additional FCC mandates, Bandwidth is developing a solution that will transit the SIP identity headers to the terminating service provider so that the certificate information remains intact. We expect this transit identity solution to be generally available in Q1 of 2021.

Recommendations & next steps

☑ Speak with an attorney to clarify your STIR/SHAKEN strategy

☑ Determine if you need to sign your own calls

☑ Consult with your equipment vendor to understand their capabilities

☑ Stay current on evolving regulatory and technology developments:

- Bandwidth's STIR/SHAKEN Resource Center
- Secure Telephone Identity Governance Authority (STI GA)
- ATIS Robocalling Initiatives
- SIP Forum/ATIS NNI Taskforce
- Federal Communications Commission

Conclusion

As a leading carrier with tens of millions of phone numbers on our network, Bandwidth is well ahead of the industry's schedule for STIR/SHAKEN implementation. We deployed STIR/SHAKEN protocols within our network in December of 2019, and have since completed interoperability agreements with major carriers including Verizon Wireless, T-Mobile, and Comcast. As of this writing, Bandwidth is already signing more than 4 billion calls each month on behalf of our customers.

Our experts are also active within industry working groups and with the FCC. Bandwidth is currently working across the ecosystem to address our customers' valid and legitimate use cases that in many instances aren't well covered by the current standards. And we will continue to communicate any changes with our customers as they occur.

We understand that STIR/SHAKEN is complicated and that you may have concerns that you're lagging behind your peers when it comes to meeting upcoming compliance deadlines.

The Bandwidth team can help you navigate the implications of STIR/SHAKEN and the potential call blocking that can occur.

For further assistance, contact your Bandwidth Account Manager or visit our STIR/SHAKEN Resource Center: bandwidth.com/regulations/stir-shaken