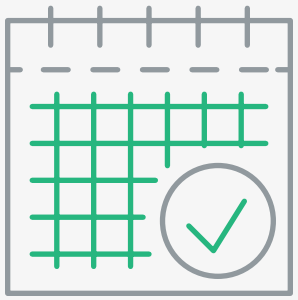
TOP TEN STIR/SHAKEN TIPS FOR CARRIERS

neustar®
A TransUnion® Company

TIP 1

Start Now – It Can Take Up to a Year to Implement STIR/SHAKEN.



If you're a Communications Service Provider (CSP) that received an extension to implement STIR/SHAKEN, it's still at the top of your to-do list.

The FCC's June 2021 deadline has come and gone, but it takes up to a year to implement STIR/SHAKEN, so your extension only buys you so much time.

So, let's get going!

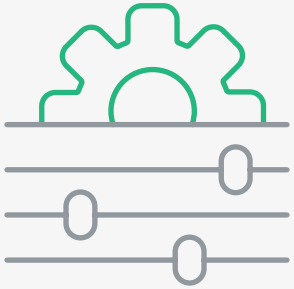
You'll need to build a lot of slack into your process to ensure that unintended technical and bureaucratic hurdles don't cause you to miss the deadline.

As your organization embarks on the STIR/SHAKEN implementation process, keep these key takeaways in mind:

- **Network upgrades** – Carriers must often upgrade their network elements or wait for upgrades from upstream or downstream service providers to support STIR/SHAKEN, which can lead to implementation delays. There are many points along the call path that need to be addressed to implement, so begin testing early to uncover hurdles that can slow deployment.
- **Attestation gap** – When more complex enterprise configurations are considered, determining the proper attestation level to assign to a call can be challenging. Carriers and enterprises should consider approaches such as certificate delegation or TN database to address these issues.
- **Implementation** – The standards makers and regulators are still determining how to address issues that arise from limitations in the STIR/SHAKEN ecosystem such as TDM networks. We anticipate answers as rollout continues.

TIP 2

You Must Lay the Groundwork for STIR/SHAKEN.



For many carriers, you may have already completed these prerequisite steps. But, if not, to participate in the ecosystem, you need to:

- Ensure your **2021 FCC 499-A Form**, indicating whether you need to contribute revenues to the Universal Service Fund, is on file with the FCC.
- Get an Operating Company Number (OCN). This number registers your company within the National Exchange Carrier Association (NECA) and is an important prerequisite that allows you to get a STIR/SHAKEN token. Make sure you allow plenty of lead time, as carriers are reporting a backlog with this process.
- Obtain access to phone numbers from the North American Numbering Plan Administrator (NANPA) and/or the National Pooling Administrator.

Follow the steps on the NANPA website.

TIP 3

Register with the Policy Administrator.

Once you meet the prerequisites on the previous page, you'll be eligible to register with the STIR/SHAKEN Policy Administrator (STI-PA). This authority will verify that you possess the information and permissions listed.

As the STI-PA in the U.S., iconectiv is responsible for coordinating, registering, and verifying Certification Authorities (CAs) through a closely controlled process outlined by the Secure Telephone Identity Governance Authority (STI-GA). ATIS manages the STI-GA, defining the rules governing the certificate management infrastructure to ensure effective use and security of SHAKEN certificates.

Policy Administrators evaluate and authorize certain trusted third parties to act as CAs and issue SHAKEN digital certificates to service providers. This both protects the authenticity and validity of the certificates and prevents people who shouldn't be signing calls from getting a certificate.

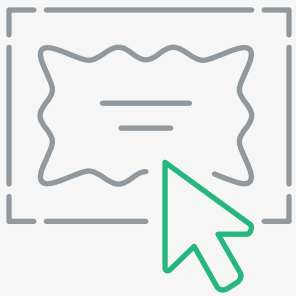
TIP 4

Make Sure You Get a Token from the Policy Administrator.

Carriers must request a Service Provider Code (SPC) or token from the PA. If the PA validates the service provider and approves the request, they then provide a token to the service provider, which contains the carrier's identifier (SPID) or Operating Company Number (OCN) and authorizes the service provider to request a certificate from a CA.

TIP 5

Select a Certification Authority.



Secure Telephone Identity Certification Authorities (STI-CAs) are critical to call authentication. CAs will be responsible for assigning digital certificates to authorized service providers that will be used to ensure calls get proper caller ID.

The PA maintains an up-to-date list of all authorized certificate issuers, which is available to all service providers. Every CA must be authorized by the PA to issue SHAKEN certificates, and they are the only means through which service providers can obtain STIR/SHAKEN certificates and comply with the TRACED Act.

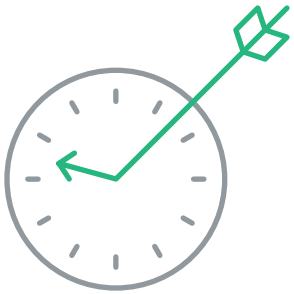
Neustar, a TransUnion company, is an approved CA!

During the process of call authentication, the terminating service provider checks that the originating service provider's certificate was created by a PA-approved CA.

TIP 6

Leave Time to Request a Certificate and Get Your Application Approved.

To get a certificate, service providers need to submit a Certificate Signing Request (CSR) and send it with their token to the CA. If the application is approved, the CA issues a certificate to the service provider.



CA responsibilities include:

- Validating Service Provider Code (SPC) token issued by the STI-PA
- Accepting Certificate Signing Requests (CSRs) for SHAKEN certificates
- Issuing standards-compliant SHAKEN signing certificates, including the Telephone Number Authorization List (TNAuthList) extension
- Publishing certificates to a hosted STI-Certificate Repository (STI-CR) for relying parties
- Revoking certificates if needed and notifying the STI-PA
- Accepting Certificate Signing Requests to renew them before they expire
- Sharing the Neustar root STI-CA public certificate to support SHAKEN call verification and chain validation

TIP 7

You'll Need Software That Brings All of These Steps Together.

A critical step in the deployment of STIR/SHAKEN is the need for software services that perform core functions associated with the specification, including STI-AS, STI-VS, SP-KMS, SKS, and SI-CR.

STI-AS – AUTHENTICATION SERVER

This hosts the API that signs authentication requests made under STIR/SHAKEN. If a third party wants to know whether calls made by your network are legitimate, STI-AS is the service that activates.

STI-VS – VERIFICATION SERVER

If your network needs to verify that a call made by a third party is genuine, the API within the server verifies its public key.

SP-KMS – KEY MANAGEMENT SERVER

This server interacts with the CA to receive certificates and the PA to receive tokens; then, it generates a public key pair to sign and verify requests.

TIP 7

You'll Need Software That Brings All of These Steps Together.

(CONTINUED)

SKS – SECURE KEY STORE

This is among the most important components of your STIR/SHAKEN implementation, as it contains the key pair generated by the SP-KMS and serves it via the application server. If this server is ever breached, attackers could use these keys to make spam calls without being detected.

STI-CR – CERTIFICATE REPOSITORY

This hosts public keys for verification purposes. These keys are freely available to third parties as a counterpart to the secure SKS.

These core functions all need to interact with one another in an orchestrated manner to properly sign and verify calls made under the STIR/SHAKEN framework. Since their interactions may require network upgrades and are complex, they need to be thoroughly tested.

TIP 8

Do Testing in a Lab Environment.

Testing usually consists of three stages. The first stage is internal, contained in a lab environment, using simulated calls.

This contained environment is important—if STIR/SHAKEN goes live with errors, it could result in service disruptions where legitimate calls are blocked and marked as spam.

The ATIS Robocalling Testbed, exclusively hosted by the Neustar Trust Lab, serves as the industry interoperability test facility to validate the effectiveness of caller authentication standards developed by the Internet Engineering Task Force (IETF) and ATIS.

ATIS developed SHAKEN as an implementation framework for service providers to better combat robocalls and call spoofing on IP-based networks.

The Neustar Trust Lab

Neustar provides technical support for the relevant connectivity information, representative network configuration, its SHAKEN software functionality, and supported test scenarios amongst participants.

The virtual test environment removes obstacles and accelerates the validation of caller authentication standards and supports extensive call tracing, helping to quickly troubleshoot during testing sessions. Through Neustar's content collaboration platform, detailed call traces are shared in almost real time and test results are formally published, summarized and shared at various levels.

The Neustar Trust Lab serves as the virtual industry testbed for communications service providers, equipment manufacturers, and software suppliers to remotely test solutions developed for the SHAKEN framework. Participants in the testbed collaborate to test against applicable ATIS standards.

How Can You Take Part?

Any service provider with an assigned Operating Company Number (OCN), as maintained by the National Exchange Carrier Association, Inc. (NECA), is eligible to participate free of charge. Other parties, testing in cooperation with an eligible service provider, may also participate if they have solutions relevant to the SHAKEN framework available to test.

Contact **Neustar** to learn more.

TIP 9

Then, Get Out of the Lab Environment and into Production!

The second step is to get out of the lab environment and start experimentally signing and verifying calls that originate and end within your network. Start small with a portion of your network and at a time that will mitigate the impact if there is an unexpected issue.

Once you can pull this off, it's time to move on to the final stage of testing calls that end and originate with third-party networks. Although successful tests will allow your STIR/SHAKEN implementation to go live, this doesn't mean that you're "out of the woods." Moving STIR/SHAKEN from a lab environment to a production environment is more than just flipping a switch.

By implementing STIR/SHAKEN, you have affected a transformation of your company, one that will affect your engineers, your operators, and your customers.

TIP 10

Don’t Forget to Tell Everybody.

Your STIR/SHAKEN implementation will materially affect the way that enterprises and consumers make and receive calls. Your customers will receive new warning messages when receiving potential spam calls, and your business customers need to be briefed on the pitfalls of attestation when making calls that could potentially be marked as spam.

While this may seem obvious, many times, technical implementations discount the need to notify stakeholders of how their experience will change. Make sure you register in the FCC’s Robocall Mitigation Database (RMDB).

Count on a Neutral Expert for Help.

The landscape continues to shift, so make sure you partner with a vendor that is staying abreast of the latest technical and regulatory changes.

As an approved Certification Authority and co-author of the STIR certificate management standards, Neustar plays an integral role in the governance structure for STIR/SHAKEN. We're at the forefront of the industry's quest to mitigate illegal robocalling and call spoofing. Learn more about our Certified Caller (STIR/SHAKEN) and Certificate Manager offering for service providers.

Visit our Trusted Call Resource Center to learn how STIR/SHAKEN is impacting your customers and how you can help them, and what resources and solutions Neustar offers.

EB-CSP-250506 02.11.2022

neustar®
A TransUnion® Company