Fact sheet

Verizon is helping to restore trust in voice calling.

The STIR/SHAKEN initiative

The Federal Communications Commission (FCC) has adopted rules requiring implementation of Caller ID authentication using technical standards known as Secure Telephone Identity Revisited/Signature-based Handling of Asserted Information Using toKENs (STIR/SHAKEN). Those rules will further the FCC's efforts to protect consumers against malicious Caller ID "spoofing," which is often used during robocall scam campaigns to trick consumers into answering their phones.

STIR/SHAKEN requires phone companies to verify that the Caller ID information transmitted with a call matches the caller's phone number. Widespread deployment of STIR/SHAKEN will reduce the effectiveness of illegal spoofing, allow law enforcement to identify bad actors more easily, and help phone companies identify calls with illegally spoofed caller ID information before those calls reach their subscribers.

The FCC requires[1] all originating and terminating voice service providers to implement STIR/SHAKEN in the Internet Protocol (IP) portions of their networks by June 30, 2021—a deadline that is consistent with Congress' direction in the 2019 Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act,[2] which (among other things) sets penalties for spoofing Caller ID data.

Verizon is implementing STIR/SHAKEN as a foundation in our inbound and outbound products. Voice over LTE (VoLTE) calls are already marked; we will be adding services and expect to be in compliance well before the FCC date of June 30, 2021.

Background

Prior to the introduction of STIR/SHAKEN, terminating carriers were unable to identify a call's originating carrier—only the provider from whom it received the traffic. In addition, illegal robocallers could further evade their identification by changing the Caller ID associated with their calls, a practice known as "spoofing."

STIR/SHAKEN is a new framework of interconnected standards for call authentication. The standards were developed by a working group of the Internet Engineering Task Force (IETF), and establish an end-to end architecture for the authentication and assertion of a telephone identity by an originating carrier and the verification of the telephone identity by a terminating carrier.

What STIR/SHAKEN does

Once implemented, calls traveling through interconnected phone networks will have their Caller ID "signed" as being valid by originating carriers and verified by other voice service providers in the call path before ultimately reaching consumers. STIR/SHAKEN digitally validates the handoff of phone calls passing through this complex web of networks, allowing the voice service provider of the consumer receiving the call to verify that a call is from the person making it.

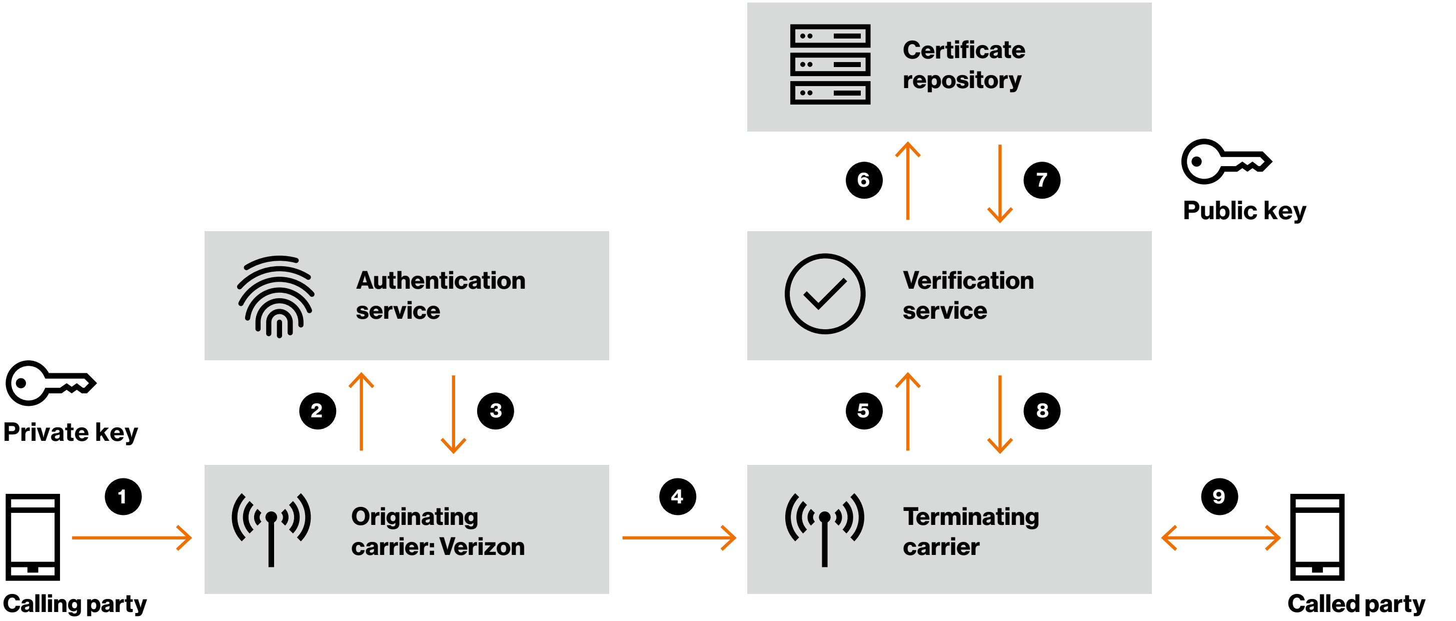
The STIR/SHAKEN standards will help identify the originating carrier behind the call and determine whether a Caller ID has been spoofed. Although the STIR/SHAKEN standards do not determine whether a call is legal or illegal, the standards will greatly enhance the integrity of Caller ID and will help to more rapidly determine the true origin of a call.

How STIR/SHAKEN works in a network

STIR/SHAKEN uses digital certificates based on common public key cryptography techniques to ensure the originating number of a telephone call is accurate. In simple terms, each telephone service provider obtains a digital certificate from a certificate authority that is trusted by other telephone service providers. The certificate technology enables a called party to verify that the calling number has not been spoofed.

The originating carrier's Secure Telephone Identity Authentication Service (STI-AS) creates an encrypted Session Initiation Protocol (SIP) identity header with the following data:

- Originating caller number
- Number called
- Time stamp
- Attestation level



STIR/SHAKEN call flow from origination to termination

- Carrier signature
- Origination ID for analytics and/or traceback purposes
- Location of certificate repository
- Encryption algorithm

The SIP INVITE with the identity header is sent by the originating carrier and received by the terminating carrier. The terminating carrier makes an application programming interface (API) request to the STI Verification Service (STI-VS) to decode the identity header and perform verification of the call.

This is the high-level call flow for calls under STIR/SHAKEN:

1. Originating carrier receives calling party (customer)-initiated call
2. Originating carrier sends JavaScript Object Notification (JSON) request to the authentication service with calling party number, called party number, time stamp and carrier attestation level
3. Authentication service returns JSON request with 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 carrier
5. Terminating carrier sends JSON request with identity header to verification service
6. Verification service obtains the digital certificate with public key, decodes the identity header and verifies the originating carrier information matches digital certificate
7. Verification results are returned to terminating carrier
8. Terminating carrier completes the call to the called party

Carrier attestation

With SHAKEN/STIR, SIP headers will contain a level-of-confidence indicator from the originating service provider to signal whether the originating caller has the right to use the number via the attestation field. There are three levels of attestation:

- **Full attestation (A):** The service provider has authenticated the calling party and that they are authorized to use the calling number
- **Partial attestation (B):** The service provider has authenticated the call origin, but cannot verify that 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

As noted earlier, the originating service provider generates data in the header to facilitate traceback, identifying where the call entered its network in addition to the attestation level.

Call status display

The status of the call (verified, failed or unknown) is typically passed to users for display on their phones, or used in some other way, such as being ingested for use by the smartphone application logic or for call management (blocking) purposes

Additional STIR/SHAKEN reference information

RFC4474bis – Authenticated Identity Management in the Session Initiation Protocol (SIP) – This document is an abstract that defines a mechanism for securely identifying originators of SIP requests.

RFC 8224 – Authenticated Identity Management in the Session Initiation Protocol (SIP) – This document defines a baseline security mechanism in the SIP to cryptographically assure the identity of the end users that originate SIP requests.

RFC 8225 – PASSporT: Personal Assertion Token – This document is an abstract that defines a method for creating and validating a token that cryptographically verifies an originating identity or, more generally, a URI or telephone number representing the originator of personal communications.

RFC 8226 – Secure Telephone Identity Credentials: Certificates – This document is an abstract that describes the use of certificates in establishing authority over telephone numbers, as a component of a broader architecture for managing telephone numbers as identities in protocols like SIP.

IPNNI-2017-00037R000 – ATIS SHAKEN Signing on Egress Proposal – This document provides an architectural view of network call flows for intracarrier and intercarrier traffic

IPNNI-2018-00001R006 – Technical Report on a Framework for Display of Verified Caller ID – This technical report provides a framework for signaling verified Caller ID information from the network to a user equipment (UE) and for displaying the information on the UE in a uniform manner, independent of technology.

Learn more:

For more information about how Verizon is helping customers secure their voice networks, contact your Verizon Business Account Manager, or click here. >

verizon✓

[1] https://docs.fcc.gov/public/attachments/DOC-363399A1.docx

[2] https://www.jdsupra.com/legalnews/2019-legislative-roundup-federal-traced-68457