SHAKEN: Frequently Asked Questions

Q. What does SHAKEN stand for?

A. SHAKEN stands for Signature-based Handling of Asserted information using toKENs. It is a specification designed to mitigate unwanted robocalls by reducing the impact of caller ID spoofing. Unwanted calls are the number one source of recent complaints to the FCC. Caller ID spoofing increases the harm from these unwanted calls.

Q. Why do we often see the technology referred to as "STIR/SHAKEN"?

A. STIR (Secure Telephone Identity Revisited) is a protocol developed by the Internet Engineering Task Force (IETF) to authenticate telephone calls end-to-end. STIR is a very flexible protocol that can be implemented in many ways, including the end user installing client software, obtaining a personal "key," and proactively managing the process of keeping software current and regularly renewing keys. This is beyond the capability of most users today, but the flexibility in the protocol also allows STIR to be implemented in other ways, including within the service provider network.

Unfortunately, this flexibility can also create problems. When a protocol has too many options and independent implementations inevitably make different choices, they "won't play nice together" and a call from one service provider won't be successfully verified by a second service provider. This is where SHAKEN comes to the rescue by precisely specifying implementation details. SHAKEN specifies a "profile" of the STIR protocol; STIR defines how you *could* implement the protocol, while SHAKEN documents how you *will* implement the protocol.

Q. SHAKEN fully specifies implementation details. Is that enough to ensure full interoperability?

A. Unfortunately, no. Even with the best specifications it's still possible for developers to misinterpret important details. That's why ATIS and Neustar partnered to provide a Robocalling testbed where implementations of SHAKEN can be tested to confirm interoperability.

For more details, see: https://www.atis.org/industry-collaboration/robocalling-testbed/

Q. Who developed SHAKEN?

A. It was developed by the ATIS-SIP Forum IP-NNI Task Force. IP-NNI stands for "Internet Protocol - Network to Network Interface." SIP stands for Session Initiation Protocol. SHAKEN is based on the STIR (Secure Telephone Identity Revisited) protocol developed by the IETF (Internet Engineering Task Force) – essentially, SHAKEN defines a profile of the STIR protocol, which is why it is typically referred to as STIR/SHAKEN.

Q. How does SHAKEN work?

A. The verification system is designed to mitigate an unforeseen consequence of technology evolution that began to emerge as a problem during the late 1990s (although the origins date back much further). That's when the telecommunications industry launched a technology capable of transmitting telephone voice calls via a broadband Internet connection instead of a regular phone line and dramatically reduced the cost of making phone calls. Robocalls use VoIP because it's inexpensive. It also makes it easier for some users to enter anything they want for the caller ID of the call. That identification for the "calling number," true or false, is automatically conveyed to the called consumer.

STIR is a call-certifying protocol developed by the Internet Engineering Task Force or “IETF.” The SHAKEN framework complements the STIR protocol by providing guidance for service providers to implement STIR in carrier networks. STIR/SHAKEN allows the originating carrier to generate a digital signature that securely signals the caller's right to use a phone number to the terminating carrier. STIR/SHAKEN will offer a practical mechanism to provide verified information about the calling party as well as the origin of the call — what is known as “attestation.”

When you make a call, your phone carrier will use your identifying number to create a digital signature, or token, that will accompany the call as it is being completed. At the other end, the system verifies that nothing was tampered with, ensuring that the call came from someone with a legitimate right to use that number. Phone calls typically pass through multiple carriers as they travel from caller to recipient. Say, for instance when someone who uses AT&T calls someone who uses Verizon, the call might be routed through one or more “transit” providers. A caller’s phone provider has always known something about the origin of the call and whether the caller ID is authentic. But until now, that provider had no secure way of passing the information along to the service provider for the person being called.

SHAKEN provides a reliable way to do that, using encrypted digital signatures for each call that lets the user know that the caller ID information is accurate. The verification from SHAKEN could be displayed directly to the user or fed into a “call-blocking app” that provides a rating system that essentially identifies calls as good, questionable or likely fraudulent. The call-blocking app can then act, on behalf of the user to stop unwanted calls from getting through. In sum, SHAKEN not only gives service providers the tools needed to sign and verify calling numbers, it also makes it possible for consumers to know who is calling, before answering the call.

SHAKEN also provides digital signatures for businesses that are allowed to “spoof” telephone numbers, known as “partial attestation.” Although this does not provide as much information as full attestation, where you know the caller has the right to use the number displayed, but it is still valuable for call-blocking apps and to help identify, and stop, illegal callers.

However, SHAKEN is not a silver bullet solution to the problem of unwanted calls.

It won't block any phone calls – including robocalls. The network is designed to complete calls. Consumers eventually are expected to see an as-yet-undetermined signal that will identify calls that have been verified, a feature intended to help guide decisions about whether to pick up. The system also is expected to enhance the accuracy of companies that provide call-blocking apps for consumers. They already try to block robocalls by looking for calling patterns to identify calls from suspicious numbers, but with reliable caller ID information, this will be far more effective.

SHAKEN is designed to be a flexible solution, with industry-led governance that can adapt to address new scams as they arise. An industry-led governance structure will allow SHAKEN to quickly work toward mitigating new problem calls without cumbersome regulatory measures.

An important point is that the phone network is essentially facing the same problem that email once faced. Many of us remember a time when our email account was littered with spam, to the point that it was feared users might abandon email altogether. Filters and other anti-spam techniques have brought the email problem under control, even though they have not eliminated email spam. SHAKEN will help us have the same success in mitigating the current problems with the phone network.

Q. When will SHAKEN be up and running? When will I stop getting these calls?

Fraud calls won't vanish overnight. But the phone system has fewer points of entry and fewer paths to monitor than the wide-open spaces of the Internet. Knowing when incoming Caller ID correctly identifies the caller, and that a malicious party can be more easily identified, could finally cut off the scammers.

Seeing the value in the SHAKEN solution, in November 2018, FCC Chairman Ajit Pai said in a statement that he demanded that the phone industry adopt a robust call authentication system to combat illegal caller ID spoofing and launch that system no later than the end of 2019. This system was successfully launched on December 16, 2019 and authorized service providers are now registering to participate.

Q. What is the industry doing to fix the problem?

A. The Secure Telephone Identity Governance Authority (STI-GA), which operates under the auspices of ATIS, is a critical body helping the industry achieve success in mitigating the problem of unwanted robocalling. The STI-GA is defining the rules governing the certificate management infrastructure to ensure effective use and security of SHAKEN certificates. The STI-GA issued a request for proposals for a Secure Telephone Identity Policy Administrator or "STI-PA," to apply and enforce the STIR and SHAKEN rules. On May 30, 2019, the STI-GA announced the selection of iconectiv as the U.S. STI Policy Administrator (STI-PA), a critical role in advancing industry efforts to mitigate illegal robocalling. As the STI-PA, iconectiv will apply and enforce the rules as defined by the STI-GA to set the SHAKEN framework into action in the network. The STI-PA will apply and enforce mechanisms designed to ensure that STI certificates are only available to authorized service providers based on rules defined by the STI-GA. As the STI-PA, iconectiv will also ensure that STI Certification Authorities perform all security functions specified to maintain the integrity of the SHAKEN framework. The STI-PA and STI-CAs were operational on December 16, 2019, and available for authorized service providers to participate in the SHAKEN ecosystem.

Q. What will the user see when SHAKEN is deployed? Will they see a "green checkmark" or "red X"? If they don't see anything, how will they regain confidence in the phone network?

A. It is currently up to individual service providers to decide how/if they would like to communicate the information SHAKEN provides to their customers. The IP-NNI Task Force is debating the optimum strategy for what to display to the end user, based on SHAKEN verification. However, independent of what is displayed to the end user, SHAKEN will enhance the effectiveness of call-blocking apps and government enforcement actions, both of which will reduce the negative impact of unwanted calls. Over time, these will help consumers regain confidence in the phone network.

Q. How much will it cost to solve this problem?

A. Individual service providers bear the costs of operationalizing SHAKEN. ATIS cannot comment further on this, as it is up to the individual service providers.

Q. Who is making these calls? From where do they originate?

A. The bulk of the unwanted robocalls calls are from international sources. In some cases, the calls use Voice over Internet Protocol (VoIP) for inexpensive direct international connections. In others, the calls use the Internet to initiate the call from a U.S.-based IP-PBX, and as a result, even if the call agents are in another country, the calls effectively enter the PSTN network within the United States. In this case, SHAKEN, even when it is only applied domestically, can begin to have an impact on illegal robocalls.

And although the international VoIP calls won't have end-to-end SHAKEN initially, they will be signed at the gateway where they enter the U.S. network. This will help call-blocking apps identify sources of illegal calls and help enforcement agencies identify the source of illegal calls and shut them down.

Q. How will SHAKEN affect call-blocking apps already in use?

A. Call blocking and analytics apps will remain important in combatting illegal robocalls and empowering consumers to manage the legitimate calls they may or may not want to answer. SHAKEN conveys trusted information to these apps about the authenticity of the caller ID and the origin of the call. By providing the analytics companies with more accurate information on which to base their call-filtering decisions, SHAKEN will increase the accuracy and reliability of existing call-blocking apps.

Q. Will SHAKEN work with legacy (TDM/ISUP) networks?

A. Generally speaking, no – SHAKEN will not work with legacy TDM/ISUP networks. In specific scenarios, SHAKEN may be able to provide some value for legacy networks that use IP-based interconnection, but this will be limited. To realize the full value of SHAKEN, networks must be SIP-based and use IP-based interconnection.

Q. Will SHAKEN work for international calls?

A. Not initially. The STI-GA is defining an infrastructure for calls that originate and terminate in the U.S. However, ATIS has published a Technical Report (TR) that describes how the SHAKEN protocol can be extended to international calls once other countries adopt SHAKEN. The current TR focuses on countries with similar regulatory contexts, such as the U.S. and Canada, but can be extended to include all countries when required.

For now, besides the U.S., Canada is the only other country that has started implementing SHAKEN. However, many countries are carefully monitoring SHAKEN deployment to assess its impact on illegal calls, and ATIS continues to brief international regulators on progress. There is general recognition that as SHAKEN begins to reduce unwanted calls in the U.S., it is likely that the focus of the scammers will shift to target countries that haven't yet deployed SHAKEN.

Q. If SHAKEN won't work for international calls initially, won't that defeat the purpose, since the bulk of problem calls are from international sources?

A. The bulk of the unwanted robocalls calls are from international sources but in many cases the calls use the Internet to initiate the call from a U.S.-based IP-PBX, and effectively originate on the PSTN as domestic calls. For these calls, SHAKEN will have an immediate impact. International VoIP calls won't have end-to-end SHAKEN initially, but they will be signed at the gateway where they enter the U.S. network. This will help call-blocking apps identify sources of illegal calls and help enforcement agencies identify the source of illegal calls and shut them down. As SHAKEN is deployed internationally, the effectiveness will increase.

Q. How do I participate in SHAKEN?

A. Participation in the SHAKEN ecosystem is currently limited to service providers and those wishing to act as Certificate Authorities (CAs). Qualified service providers and CAs should go to the STI-PA site at: https://authenticate.iconectiv.com/. To determine if your company is a qualified service provider, please review the Service Provider Code Token Access Policy.

Q. Can service providers in the U.S. commonwealths and territories take part in the STI-GA SHAKEN ecosystem?

A. Yes, a service provider based in the commonwealths of Puerto Rico or the Northern Marianas, or the territories of American Samoa, Guam and the U.S Virgin Islands may participate in the STI-GA STIR/SHAKEN ecosystem. Generally, as long as a service provider meets the requirements of the SPC token Access Policy, it may register for authorization with the STI-PA.

Q. How do I become a SHAKEN Certification Authority?

A. Qualified Certification Authorities can register to join the SHAKEN ecosystem today by visiting the STI-PA site at: https://authenticate.iconectiv.com/certification-authority-authenticate.