Unwanted Robocalls

CHALLENGES AND SOLUTIONS

February 2020

TABLE OF CONTENTS

Abbreviations 3

Background 4

Root of the issue in VoIP environment 5

Background. 5

STIR 6

SHAKEN. 8

The position of VoLTE/RCS 10

Considerations on STIR/SHAKEN deployment. 11

Development of the ecosystem 11

Added value of policy server. 12

Network-based screening 13

Application-level screening 13

Out-of-Band method 13

Other methods 13

Challenges and Solutions of the Ecosystem 14

Conclusion. 15

References 17

ABBREVIATIONS

AI	Artificial Intelligence
AIN	Advanced Intelligent Networks
API	Application Programming Interface
ATIS	Alliance for Telecommunications Industry Solutions
CA	Certification Authority
CS	Circuit Switched
CSCF	Call Session Control Function
CVT	Call Validation Treatment
ENUM	E.164 Number to URI Mapping
FCC	Federal Communications Commission
GW	Gateway
HTTPS	Hypertext Transfer Protocol Secure
IBCF	Interconnection Border Control Function
ID	Identity
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	IP security
ISDN	Integrated Services Digital Network
JSON	JavaScript Object Notation
LTE	Long Term Evolution
MSISDN	Mobile Subscriber ISDN number
NNI	Network-Network Interface
OTT	Over-the-Top
PASSporT	Personal Assertion Token
PBX	Private Branch Exchange
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
PSX	Policy and Routing Solution
RCS	Rich Communication Services
RESTful	Representational State Transfer
RFC	Request for Comments
RTCWeb	Real-Time Communications on the Web
SBC	Session Border Controller
SHAKEN	Signature-based Handling of Asserted information using tokens
SIP	Session Initiating Protocol
SKS	Secure Key Storage
SP	Service Provider
SPS	Certificate Provisioning Service
SS7	Signaling System #7
STI-AS	Secure Telephone Identity Authentication Service
STI-CR	Secure Telephone Identity Credentials Repository
STIR	Secure Telephone Identity Revisited
STI-VS	Secure Telephone Identity Verification Service
TDM	Time Division Multiplexing
tel URI	telephone number–based URI
TLS	Transport Layer Security
TrGW	Transition Gateway
UA	User Agent
URI	Uniform Resource Identifier
VoIP	Voice over IP
VoLTE	Voice over LTE
VoWiFi	Voice over Wi-Fi
XMPP	Extensible Messaging and Presence Protocol

BACKGROUND

A robocall refers to a phone call placed through an automated dialer delivering a pre-recorded message.

In the mind of most consumers, robocalls are from telemarketers or even scammers, but they can also be used as a communications channel for public service and emergency announcements.

In addition to pre-recorded messages, advanced forms of robocalls rely on more personalized audio messages to simulate a realistic-sounding phone call. They can also be used as a solution; e.g. a voice-activated chatbot which enables users to accomplish tasks on their device hands-free.

A chatbot (also known as a chat robot, interactive agent, conversational interface or artificial conversational entity) is a solution based on artificial intelligence. It conducts a conversation via audio and text. Chatbots can also be deployed in legitimate business areas such as customer service dialog systems or information acquisition. The technical sophistication of such services vary from simple keyword scanning and database mapping to advanced natural language processing systems.

In addition to the legitimate robocalls, unwanted robocalls are a rapidly rising worldwide phenomenon. They refer to a type of unsolicited calls, or “spam”, such as unwanted advertising, other automated annoying calls and even scams. In addition to the voice calls, this category also includes automatic, unwanted spam and scam text messaging as mentioned in Ref. [1]. This phenomenon is rising concerns, as, e.g., Americans received 26.3 billion robocalls during 2018. [2]

Blacklisting is one way of preventing unwanted or illegal robocalls. The blacklist can be deployed to include an ever-increasing list of different spam callers’ telephone numbers and manage incoming calls. The respective can be implemented into a device (in either the application or integrated deeper into the chip), or as a network service. There are various solutions for blacklisting, including as a service that allows customers to define numbers they want blocked from their device, or a simple app recognizing the calling party’s telephone number blocking the unwanted ones based on its own blacklist.

A challenge of these blacklists arise when “robocallers” hide the caller ID by “spoofing” their numbers. “Spoofing” refers to faking the Caller ID, showing as a different number to the receiving party (B-Subscriber). One of the arguments against proactive robocall blacklists is that, in addition to the unwanted robocalls, they might inadvertently block allowed numbers such as automated emergency notifications. [3]

In November 2019, the US House and Senate announced a joint anti-robocalling bill that would aim to allow operators to block Robocalls in a “consistent and transparent” way and bars them from charging customers extra money for the service. The bill also gives the FCC and law enforcement more power to investigate and punish illegal robocallers.

The Federal Communications Commission (FCC) has been in a vital position in the US to bring the industry together to find a solution. The agency has issued hundreds of enforcement actions against illegal robocallers and are working with operators to block by default based on “reasonable call analytics” and implement caller ID authentication. As a result, IETF-defined STIR (Secure Telephone Identity Revisited) is considered one of the most promising technologies to combat unwanted robocalls.

Furthermore, the cooperation between the Alliance for Telecommunications Industry Solutions (ATIS) and SIP Forum resulted in SHAKEN (Signature-based Handling of Asserted information using tokens) framework, which provides a mechanism to implement STIR to authenticate calls. The solution provides SIP calls with a certificate of authenticity, which makes it easier for customers to trust that the caller ID is legitimate. The US service providers are implementing gradually the STIR/SHAKEN into their telecommunication infrastructure, the major telephony carriers leading the effort.

Combined with other methods, such as the US government’s recent legislation and the threat of substantial punishments to bad actors, STIR/SHAKEN may provide relief for the consumers. [4] Nevertheless, only time and instances from the field will prove the functionality, and provide a good indication on the additional means that could be developed as an extra layer to complement the level of trust and protection.

This document summarizes current challenges and the industry's options for enhancing the protection against unwanted robocalls as well as outlines the technology behind STIR/SHAKEN. Its purpose is to explain the current robocall landscape and technical solutions supporting the STIR/SHAKEN in order to verify the caller, minimizing unwanted robocalls and protecting consumers from fraudulent intentions from bad actors.

ROOT OF THE ISSUE IN VOIP ENVIRONMENT

The current telecommunications infrastructure is seeing a convergence of Internet and traditional telephony services. Voice over IP (VoIP) is, in fact, an increasingly popular solution to deliver voice calls in the modern networks as it packetizes the communications and delivers the calls based on packet data bearers, making communications more dynamic and flexible compared to the legacy circuit switched technology. The VoIP call can be integrated into the serving operator's infrastructure such as LTE (Long Term Evolution), which can provide native and seamless voice service for the customers. Examples of such solutions are Voice over LTE (VoLTE) and VoWiFi (Voice over Wi-Fi).

Another option is to rely on a separate, Over-the-Top (OTT) service on the application layer. These solutions are typically installed into consumer devices such as smartphones and laptops afterwards by the user. Examples of some commercial OTT solutions include Skype, Messenger and WhatsApp.

In the traditional telephony networks, the A-subscriber (calling party) and B-subscriber (called party) identity (e.g. MSISDN) is straightforward for the operator to manage, the infrastructure being circuit-switched and closed end-to-end ecosystem where the identity of the users is non-breakable. Nevertheless, the principle of open Internet facilitates the robocalls in the VoIP environment as it opens doors for external networks.

The IETF RFC 7340 [5] summarizes the issue due to interworking with different communication architectures. The communication link may include, e.g., Session Initiating Protocol (SIP), Public Switched Telephone Network (PSTN), Extensible Messaging and Presence Protocol (XMPP), and Real-Time Communications on the Web (RTCWeb), which breaks the end-to-end semantic of the communication interaction. This, in turn, has negative impact on reliable identification capabilities. In other words, the operators of such a fragmented ecosystem cannot necessarily any more ensure the real identity of the callers.

STIR

The IETF RFC 7340 [5] presents the Secure Telephone Identity Revisited (STIR) problem statement outlining challenges that have led to unauthorized robocalling and other illegitimate activities. These instances include voicemail hacking (vishing) and swatting (harassment tactic of deceiving an emergency service into sending a police and emergency service response team to another person's address), as the VoIP calls grant attackers tools to impersonate and obscure calling party numbers. The RFC 8226 [6] outlines the challenges and presents the idea behind STIR, and RFC 8224 [7] summarizes information related to respective SIP authenticated identity management.

Based on these documents, in the efforts of the system to prevent impersonation, one solution could be to implement credentials that identify the parties controlling telephone numbers. This would work for the parties to assert that they are authorized to use telephony numbers while impersonators would be unable to present such credentials. These RFCs describe credential systems for telephone numbers based on X.509 version 3 certificates.

The STIR model aims to provide means for a practical adaptation of the well-known authentication service concept. It would have two entities needing access to credentials, i.e., authentication services and verifier.

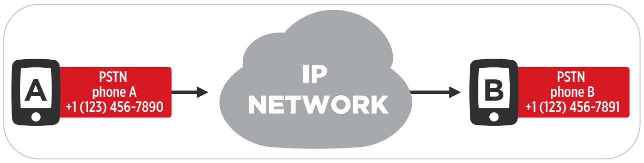
- Authentication service is operated by an entity enrolled with the certification authority;
- Verifier trusts the trust anchor of the authority; it also may access and validate the public keys associated with the certificates.

The RFC documents describe the architecture and syntax, but they do not assume specific Certification Authority (CA) or deployment environment. The purely STIR-based solution would not suffice as it lacks real operational models.

Nevertheless, the RFC 7340 document [5] describes the relevant call scenarios outlining the possibilities and challenges in the deployment of STIR:

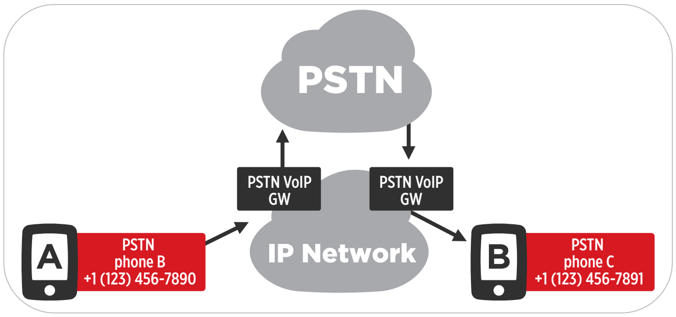
- **VoIP-to-VoIP** call: In this scenario, there is a group of service providers offering interconnected VoIP service exchange calls using SIP end-to-end and may also deliver part of the calls via circuit-switched facilities. The call is relying on SIP end-to-end. See Figure 1.

Figure 1 VoIP-to-VoIP call.



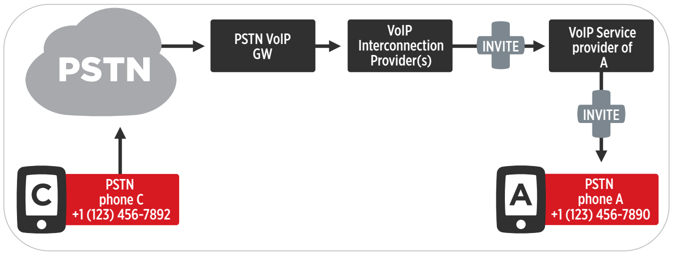
- **VoIP-PSTN-VoIP** call: Two VoIP-based service providers are not directly connected by VoIP and use Time Division Multiplexer (TDM) circuits to exchange calls, leading to the IP-PSTN-IP use case. PSTN VoIP Gateways (GW) are thus needed to interconnect the SIP call. See Figure 2.

Figure 2 VoIP-PSTN-VoIP call.



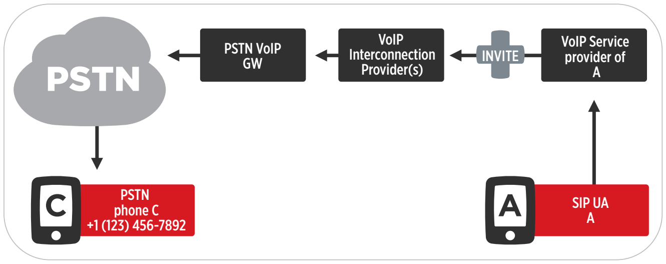
- **PSTN-to-VoIP** call: The originating call traverses the PSTN and enters the Internet via a PSTN/VoIP gateway. One or a set of VoIP interconnection providers are involved in this scenario. See Figure 3.

Figure 3 PSTN-to-VoIP call.



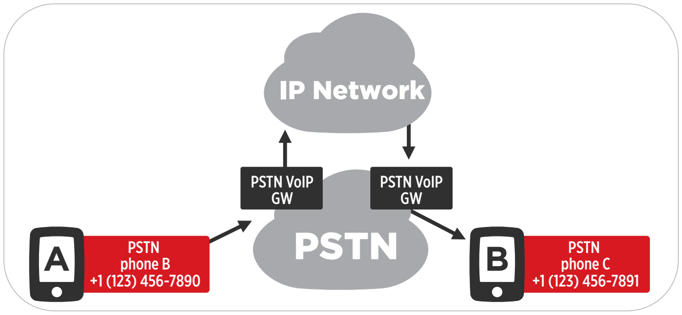
- **VoIP-to-PSTN** call: The originating call's E.164 number is translated to a SIP URI and an IP address. The originating call traverses VoIP provider, which adds call origin identification information and forwards the call to PSTN/VoIP gateway. See Figure 4.

Figure 4 VoIP-to-PSTN call



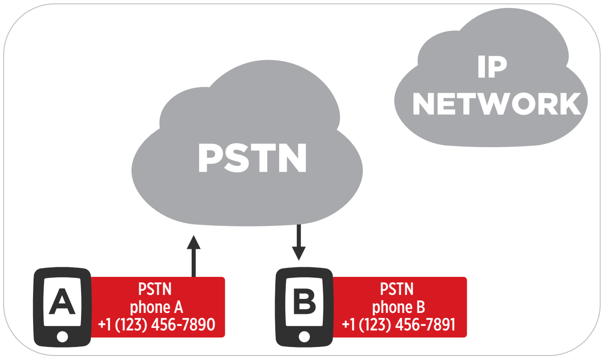
PSTN-VoIP-PSTN call: Both A and B subscriber have PSTN terminals while interconnection between the two circuit-switched parts of the PSTN is accomplished via an IP network. A subscriber's operator uses a PSTN-to-VoIP gateway to route the call via an IP network to a gateway to break out into the PSTN again. See Figure 5.

Figure 5 PSTN-VoIP-PSTN call.


IP Network
PSTN VoIP GW
PSTN VoIP GW
PSTN
A
PSTN phone B +1 (123) 456-7890
B
PSTN phone C +1 (123) 456-7891

- **PSTN-to-PSTN** call: This scenario represents the legacy case, which may also allow the use of out-of-band IP connectivity at the originating and terminating carrier to validate the call information. See Figure 6.

Figure 6 Legacy call within PSTN.


IP NETWORK
PSTN
A
PSTN phone A +1 (123) 456-7890
B
PSTN phone B +1 (123) 456-7891

From the models depicted in Figure 1 - Figure 6, the end-to-end SIP call of Figure 1 provides the highest level of confidence in the attestation efforts, and thus the most efficient shielding against number spoofing as the originator of the call can be authenticated within the infrastructure.

The SIP has the From-header field, which can be used for user-supplied identity. The IETF RFC 3261 [8] aimed to provide a secure origin for SIP requests as an extension to SIP. The respective intermediate solution is the P-Asserted-Identity header as described in IETF RFC 3325 [9], and is deployed widely.

Nevertheless, and being a challenge in the cases 2-6 of the respective Figures, it is limited to closed trusted networks where end-user devices cannot alter or inspect SIP messages and offers no cryptographic validation. As P-Asserted-Identity is used increasingly across multiple networks, it cannot offer protection against identity spoofing by intermediaries or entities that allow untrusted entities, leading to the possibility for SIP spam. This problem statement is described in IETF RFC 5039. [10]

In addition, other solutions have been under active discussions at IETF, which is summarized in IETF RFC 4474. [11] Most importantly, the document considers the Certificate Authority concept as a feasible solution. Nevertheless, the ideal solution is still to be explored.

As summarized in [5], SIP mimics the structures of the telephone network and uses telephone numbers as identifiers. Telephone numbers in the From-header field value of a SIP request may appear as the user part of a SIP URI or in an independent tel URI (referring to resources identified by telephone numbers). Nevertheless, the certificate designated by the Identity-Info header field as specified, corresponds only to the domain portion of a SIP URI in the From header field. IETF RFC 4474 [11] does not have any provision to identify the assignee of a telephone number.

The SIP Identity mechanism provides thus no assurance that a number has been assigned to any specific carrier. For a tel URI, moreover, it is unclear in IETF RFC 4474 [11] what entity should hold a corresponding certificate. A caller may not want to reveal the identity of its service provider to the called party and may thus prefer tel URIs in the From header field.

This lack of authority gives rise to a whole class of SIP Identity problems when dealing with telephone numbers. Therefore, the pure STIR-based solution does not provide sufficient means to combat against unwanted robocalls.

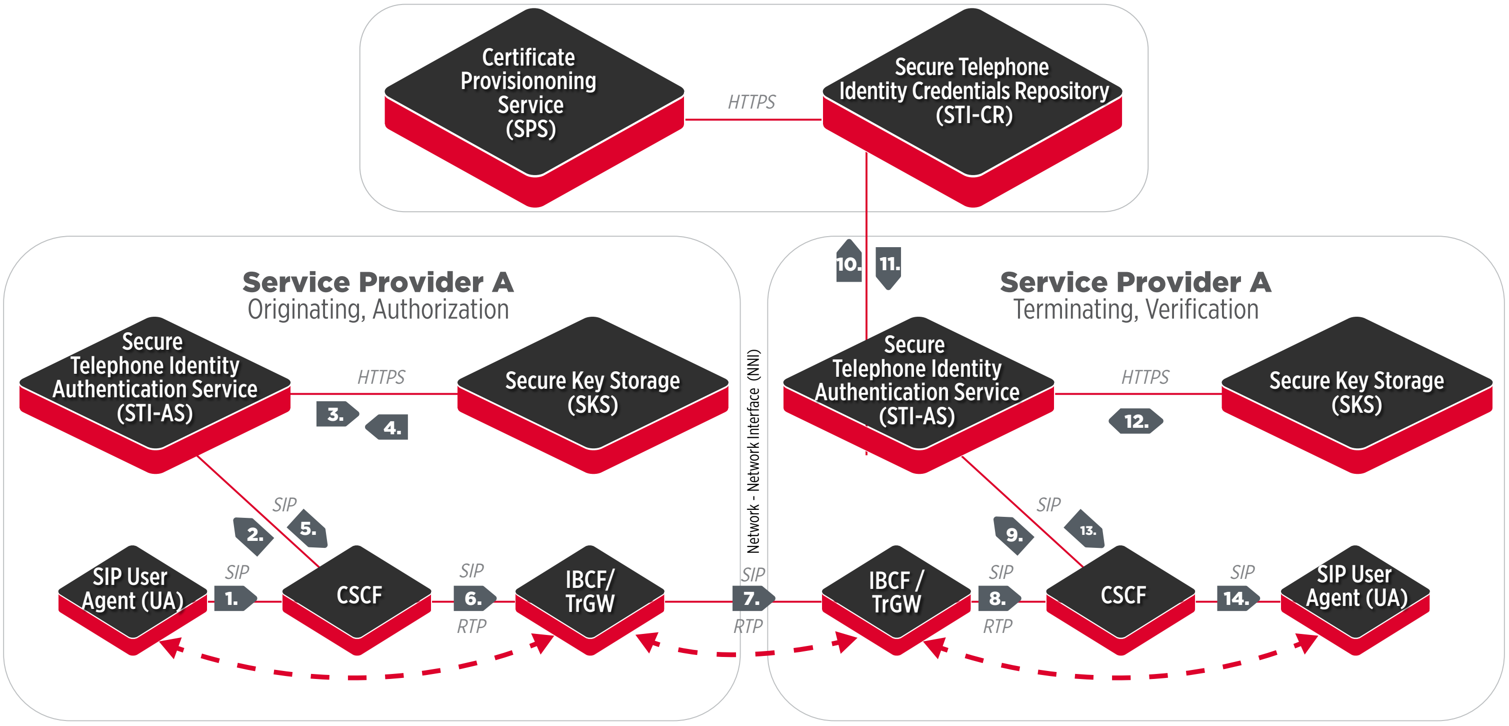
SHAKEN

To solve the issues detailed in the STIR documentation [5], the IETF has been actively working on the extension of PASSporT (Personal Assertion Token).

The respective work item is called SHAKEN (Signature-based Handling of Asserted information using tokens), and the related IETF draft documentation can be found in Ref. [12]

The aim of the SHAKEN is to extend PASSporT, which refers to a token object that conveys cryptographically signed information about the participants involved in communications, to include information defined as part of the SHAKEN specification from the Alliance for Telecommunications Industry Solutions (ATIS) and the SIP Forum IP-NNI Joint Task Force. It is assumed that the extensions provide an adequate level of confidence in the originating identity, including originating communications with and without STIR information.

Figure 7 The architectural model and signaling flow of SHAKEN as interpreted from [13].


Certificate Provisiononing Service (SPS)
HTTPS
Secure Telephone Identity Credentials Repository (STI-CR)
10.
11.
Service Provider A
Originating, Authorization
Secure Telephone Identity Authentication Service (STI-AS)
HTTPS
Secure Key Storage (SKS)
3.
4.
SIP
2.
5.
SIP User Agent (UA)
SIP
1.
CSCF
SIP
6.
RTP
IBCF/ TrGW
Network - Network Interface (NNI)
SIP
7.
RTP
Service Provider A
Terminating, Verification
Secure Telephone Identity Authentication Service (STI-AS)
HTTPS
12.
Secure Key Storage (SKS)
SIP
9.
13.
IBCF / TrGW
SIP
8.
RTP
CSCF
SIP
14.
SIP User Agent (UA)

The SHAKEN [13] specification defines a framework for using STIR protocols and for managing the deployment of Secure Telephone Identity (STI) technologies. Its purpose is to provide end-to-end cryptographic authentication and verification of the telephony and other relevant information in IP-based voice network. The framework includes PASSporT as defined in Ref. [14] (IETF RFC 8225), SIP Authenticated Identity Management as defined in Ref. [15] (IETF RFC 8224) and the STIR certificate framework as defined in Ref. [6] (IETF RFC 8226), and they serve for implementing the cryptographic validation of an authorized originator of telephone calls using SIP. The framework tackles a multitude of scenarios combining VoIP and TDM/SS7 originated traffic. SHAKEN thus complements the STIR, as indicated in Table 2, which summarizes the key aspects of STIR and SHAKEN.

As indicated in the Ref. [13], the following draft IETF documents form the foundation summarizing the current understanding of the STIR/SHAKEN architecture deployment scenarios: 1) Draft-ietf-stir-rfc4474bis; and 2) Draft-ietf-stir-passport. These documents describe protocol level tools compatible with the SIP for providing digital signatures to the Caller ID or telephone number of the calling party. One of the key questions is related to the means the signing provider has to assert that their customer can legitimately use the number that appears as Caller ID. For this assessment, signer-specific policy is applied. It could be potentially used, e.g. the following principles as mentioned in Ref. [13]:

- The number was assigned to this customer by the signing service provider;
- This number is one of a range of numbers assigned to an enterprise or wholesale customer;
- The signing service provider has ascertained that the customer is authorized to use a number;
- The number is not permanently assigned to an individual customer, but the signing provider can track the use of the number by a customer for certain calls or during a certain timeframe.

As an additional aspect, the service provider's reputation may be directly dependent on how rigorous they have been in making this assertion.

As soon as the originating telephony service provider receives the SIP INVITE from the A-subscriber, there are thus three levels defined for the assessment result of the reliability of the calling number:

A: Full Attestation. The service provider authenticates and authorizes the A-subscriber. This case is valid, e.g., when the A-subscriber is customer and registered within the service provider's infrastructure (e.g., softswitch or SBC, Session Border Controller).

B: Partial Attestation. This case refers to the situation when the service provider can authenticate the A-subscriber but cannot perform authorization for using the telephone number. This case is valid, e.g. in enterprise PBX environment.

C: Gateway Attestation. This case refers to the situation in which the service provider can authenticate from where the call is originated but is not able to authenticate the call source. An example of this situation is the call received from an international gateway.

Table 1 summarizes the key roles of the elements presented in Figure 7, as interpreted from Ref. [13]. This attestation level is included in the SIP header, along with A- and B-subscriber IDs, timestamp and origination ID, as a result of the service provider's inquiry to the authentication service.

Upon the receiving service provider of the B-subscriber, the SIP INVITE, accompanied by the above-mentioned header info, is sent to a verification service which, in turn, obtains the originating service provider's digital certificate (which is found at the public repository), as a basis for verification procedure for the certificate chain of trust.

The SIP identity header contains the abovementioned data, which is decoded in base64 URL format. The complete SIP Identity header contains parameters for the encryption algorithm, SHAKEN extension, and PASSporT token type indicators, as well as a JSON web token. The latter comprises of base64 URL JSON encoded header and payload, and a signature. [16]

After the verification procedure, the verification service provides the results to the service provider of the B-subscriber (e.g., within the softswitch or SBC).

Table 1 the main elements of SHAKEN architecture.

FLOW	ELEMENT	DESCRIPTION
1	SIP-UA	The network of the originating caller's service provider (SP) A authenticates the SIP User Agent. If under the same management control, the serving SP can identify the initiating SIP UA.
1, 2, 5, 6	CSCF	IMS Call Session Control Function is part of the IMS and has the role of registrar and router. The originating CSCF routes the call to the egress IBCF, after the additional signaling via STI-AS and SKS (3, 4, 5).
6, 7	IBCF / TrGW	Interconnection Border Control Function / Transition Gateway interconnects networks. The Network-Network Interface (NNI) routes the INVITE through a standard inter-domain routing configuration.
3, 4, 5	STI-AS	Secure Telephone Identity Authentication Service performs the authentication within the originating SP. It determines, based on SP-specific means, the legitimacy of the telephone number identity of the INVITE. After receiving the private key from SKS, the STI-AS signs the INVITE and adds an Identity Header field as described in the draft-ietf-stir-rfc4474bis using the Caller ID in the P-Asserted-Identity header field. After this, the STI-AS passes the INVITE back to the CSCF of the SP A.
3, 4	SKS	Secure Key Storage responds, providing the private key.
9-13	STI-VS	Secure Telephone Identity Verification Service. (9) The terminating CSCF initiates a terminating trigger to the STI-VS for the INVITE. (10) The terminating SP B STI-VS uses the INFO parameter information in the Identity header field per draft-ietfstir-rfc4474bis to determine the STI-CR Uniform Resource Identifier (URI) and makes an HTTPS request to the STI-CR. (11) The STI-VS validates the certificate and extracts the public key. It constructs the draft-ietf-stir-rfc4474bis format and uses the public key to verify the signature in the Identity header field, which validates the Caller ID used when signing the INVITE on the originating service provider STI-AS. (12) The service provider could have an optional CVT (Call Validation Treatment) within its own network, or also 3rd party could implement it elsewhere. (13) Depending on the result of the STI validation, the STI-VS determines if the call setup progresses with an appropriate indicator. The SIP INVITE is passed then back to the terminating CSCF, which continues to set up the call to the terminating SIP UA if appropriate.

THE POSITION OF VOLTE/RCS

The support of robocall/spam messaging filtering via IMS – which also serves VoLTE (Voice over LTE) and RCS (Rich Communication Services) – has benefits as the infrastructure is growing, and the respective SIP signaling can be used, e.g. by applying additional PKI/certificate concept as described in STIR documentation [5].

The additional benefit of such an approach is that the integrated prevention solution could promote further the adaptation of VoLTE/RCS also beyond the robocall prevention.

Nevertheless, the adaptation of public key infrastructure (PKI) / Certificate Authority (CA) concept into the VoIP / VoLTE / RCS environment, including the overall telephony ecosystem, still needs further assessment as the IETF specifications arise.

Some of the topics the industry would need to research further include the following:

- There are several options left for practical deployment; what is the minimum set of mandatory functionalities, and how well such variety would fit into the practical interoperability scenarios such as roaming cases as robocalls can be assumed to be generated worldwide?
- Even the benefits of shielding can be assumed to outperform the increased signaling caused by STIR/SHAKEN, how much the PASSporT signaling payload/tokenization would affect the current networks in terms of performance, capacity, or cost?
- Would there be any potential situations when the SIP header size causes a bottleneck for embedding STIR/SHAKEN-related and other additional information for perhaps some other additional services relying on SIP signaling, and how to minimize the impact of such situations?

In general, the VoLTE and RCS, based on IMS architecture, provide with integrated benefits for the prevention of robocalls and spam robotexting. The IMS core and the interfaces with the interconnected elements and networks (such as LTE and 5G radio and core networks, roaming networks and chatbot servers) can be shielded properly. IMS protects the contents against eavesdropping and manipulation on a hop-by-hop basis, and each interface can be shielded by applying the appropriate industry's security standards such as IPsec, TLS, etc.

Relying on IMS core, the end-to-end communications within VoLTE and RCS networks thus provide means to combat against unwanted robocalls and spam robotexts within the same ecosystem but whenever the end-to-end chain of trust is broken, i.e., when there are other systems interconnecting each other, the confidence of the correct attestation varies.

Table 2 Key principles of STIR and SHAKEN industry standards. [17]

STIR	SHAKEN
IETF STIR defines core protocols and technologies for SIP and certificate usage for applying digital signatures to validate the telephone identity of the calling party.	ATIS/SIP Forum SHAKEN defines the industry framework for using STIR technology.

CONSIDERATIONS ON STIR/SHAKEN DEPLOYMENT

DEVELOPMENT OF THE ECOSYSTEM

The STIR/SHAKEN is considered an efficient way to combat the unwanted robocalls.

It can be assumed that along with practical experiences, the initial deployments can be further enhanced to provide more efficient shielding against bad actors. Such items may include the further developed principles of the attestation and means to prove the origin of the call. This could be based on, e.g. a reputation score which evolves and gets more reliable as the call history develops.

In essence, STIR works in an IP environment to validate SIP calls in real-time, or to trace calls afterwards. The accompanying gateway may sign its identity for such traceability without need to verify calling number. Nevertheless, it is not necessarily possible to verify calls from outside the SIP network. By default, only domestic SIP calls can thus be traced, while the tracing of the TDM-based calls is more challenging.

As noted in [17], even with the deployment of the STIR/SHAKEN framework, traffic from CS originations and IP Gateways, including international and wholesale actors, will continue being an issue for robocalling and illegal spoofing. Thus, deployment of other mitigation techniques to complement the STIR/SHAKEN solution in a form of layered approach may be desired.

As summarized in [18], it can be assumed that a single solution such as STIR/SHAKEN will not suffice to combat against unwanted robocalls even in an all-IP environment, but a layered approach will continue to provide benefits as bad actors keep changing tactics quickly. The STIR/SHAKEN works for authenticating and thus proving that a call has not been spoofed, but it does not determine caller intent. This means that bad actors may continue making unwanted calls by registering telephone numbers, which, as long as registered, are authentically theirs, as indicated in Ref. [18].

This leaves a threat model in which bad actors may register a block of (legitimate) numbers to use those for unwanted (illegal) robocalls. This can happen at a fast pace by utilizing those numbers quickly, and continuing the cycle by abandoning them and obtaining a new block of telephone numbers to start the process again.

As concluded in [18], it is beneficial to assess the intent of a call by real-time analytics layer, which is in practice a multi-protocol analytics server to assert the traffic basing on, e.g., VoIP, TDM, ENUM, SIP, AIN and RESTful API. Various companies are using the layer in current ecosystem.

As a conclusion for the near-term opportunities and challenges, STIR/SHAKEN authentication standard provides logical means to tackle the challenges of unwanted robocalls in IP environment, minimizing the possibilities of bad actors to spoof and perform other robocall tactics. Nevertheless, as the development of more mature all-IP infrastructure and its coverage takes time, additional layers of protection seem justified to complement the efforts, including an analytics layer.

ADDED VALUE OF POLICY SERVER

A specific policy server can provide additional value in the trust chain for monitoring and evaluating the level of confidence of the legitimacy of the calls. Such a policy server could compare some pre-defined information on, e.g. the location of the originating call compared to the destination, and the amount of such calls during a certain period. This would help further in capturing, e.g. massive, unsolicited campaigns originated from certain locations.

As summarized in [19], the Session Border Controller (SBC) and Policy and Routing (PSX) are commercial examples of platforms that can be applied complementing in the efforts of the caller authentication and verification. In this type of deployment of STIR/SHAKEN solution, the SBC can generate and pass the identity header and respective signature to an authentication server via the policy server, which, in turn, receives verification of the signature and passes it to the SBC. Depending of the result of the verification, the SBC may reject or continue with the call.

As another example of product types, Ref. [20] indicates there are additional policies that can be applied into the STIR/SHAKEN solution such as:

- Robocalling fraud triggers (action can be decided automatically for the calls from a number exceeding threshold such as the amount of call attempts per time period);
- Reputation service (crowdsourcing to build databases of robocall caller IDs and to prevent calls from poor reputation sources);
- Blacklisting to prevent neighbor-spoofing (the protection against robocalls with a fake caller ID reminding the receiving party's number, with the aim of the receiver being more likely to answer a call from such a number);
- Customer-maintained blacklists (API and respective web portal that authenticates subscribers who can then enter a request to block calls to their number from a specific calling number);
- Shield database of high-risk numbers (vendor-maintained database for high-risk numbers).

NETWORK-BASED SCREENING

As an example of other commercial solutions, Nomorobo is a network-based service, without need for setting up a device. It is based on a blacklist of phone numbers reported to the Federal Trade Commission (FTC) as Do Not Call violators, and numbers that consumers indicate are connected to robocallers. Nomorobo works on VoIP telephone service for cable and Internet provider customers. When someone calls the number of the subscriber, Nomorobo rings simultaneously on the aimed home phone and the Nomorobo servers. If the service IDs the incoming number as a robocaller, it ends the call after one ring. [3]

APPLICATION-LEVEL SCREENING

There are some ideas on the "pre-evaluation entity". There have been applications with artificial intelligence which makes conversation with the robocallers (such as explained in Ref. [21].

Google aims to develop further the pre-screening idea as described in Ref. [22] by providing a virtual assistant to screen the caller first, to connect the legitimate calls or to reject the spam calls. These are transparent solutions network-wise as they are in application level or integrated into the devise such as Google's "Call Screen" feature, which the Pixel 3 smartphone supports.

OUT-OF-BAND METHOD

One of the most concrete additions on top of the STIR is the possibility to deliver certificates from sources that are not connected to end-to-end SIP chain. This means that instead of SIP-capable transmission, the certificates could be delivered for the process via alternative routes such as the Internet. [23]

This work item is included in the further development by IETF. As the item is still under construction, there is no formal RFC yet available. As soon as it's ready, this scenario would assist further in the assessment of the originating calls. More specifically, for these cases where telephone calls do not use Internet signaling protocols, or use them for only part of their signaling path, Ref. [23] summarizes the respective use cases requiring the delivery of the PASSporT objects outside of the signaling path; Example of such delivery could take place via the Internet as shown in Figure 6 while the actual call is established via the traditional route.

For further information, the Ref. [23] defines respective architectures and semantics.

OTHER METHODS

One way to combat unwanted robocalls is crowdsourcing to report the problematic sources. This method can also provide preliminary (most probable) information about the type of robocall, e.g. if it is about intention to engage the called party to discussions by offering free-of-charge gifts (leading to potentially hard-to unsubscribe, expensive services or products), or other fraudulent intention to steal the called party's bank account information.

In the future, as a stand-alone solution or in combination with the crowdsourcing methodologies, real-time Artificial Intelligence (AI) and Machine Learning (ML) solutions could be applied gradually into the set of prevention tools of unwanted robocalls, as indicated in [18]. Due to the dynamics of the unwanted robocall intentions, the fully automatized machine learning technologies combined with optimized algorithms could be utilized to take advantage of big data originated from the network addresses to identify the changing identities of robocallers more efficiently than is possible manually. This methodology could be based on the assessment of call patterns directly from the network.

One of the potential future ideas would be to extend the STIR/SHAKEN concept further to integrate also blockchain principles to protect the transactions, although the pros and cons of such ideas are yet to be evaluated. As an example, even MNOs typically prefer avoiding increased signaling and network element modifications (e.g., extensions to HLR/HSS is normally avoided), the blockchain could potentially add value justifying the benefits over the impact on the signaling load.

CHALLENGES AND SOLUTIONS OF THE ECOSYSTEM

The STIR/SHAKEN is designed to help industry and users to fight against unwanted robocalls, but it is not considered to be a “silver bullet” as such. While it is not adapted too widely by US and international stakeholders, there will remain uncertainties about the origin of the calls.

The challenges in the deployment of STIR/SHAKEN include investment. The FCC has clearly informed the need for the STIR/SHAKEN. FCC Chairman Ajit Paij summoned major phone companies to implement SHAKEN/STIR caller ID authentication standards by the end of 2019. [24] The practical deployment can be assumed thus to be gradual, starting with the major US operators. Global interoperability will be an important item in the evolution of the ecosystem to fully benefit the users. Ensuring the interoperability requires active cooperation between the stakeholders on a global level.

The impact on the network needs to be understood well to avoid creating unnecessary bottlenecks due to problems such as increased signaling load of the embedded STIR/SHAKEN messages and tokens. This requires cooperation and joint testing of the solution, and adjustments as per findings.

The impact to the end-users should be positive. The “pre-digested” indication of the legitimacy of the source, in an easy-to-understand format on the display of the device will make for a clear Caller ID. Nevertheless, uncertainties will remain when any part of the call is routed outside of the SIP environment.

As the industry comes up with solutions, bad actors will work to invent new methods to circumvent them such as pretending to be legitimate parties within the ecosystem.

Therefore, the more comprehensive solution may benefit from the layered approach combining STIR/SHAKEN with other methods such as traffic analytics. There are already commercial network analytics solutions such as those presented in Ref. [20].

CONCLUSION

As the prevention of robocalls is not yet widely or globally established, there is still room for new, enhanced ideas for respective protection. The challenge of such adaptation on the network side is that it would need global acceptance and deployment to be efficient, as well as combining legacy and new technologies. There are obviously many issues to be solved as service providers prepare to provide a fully interoperable ecosystem. The main issue with the initial deployment of the STIR/SHAKEN is that all the countries would need to implement it to be valuable. Yet currently, mainly North America is active in the implementation of STIR/SHAKEN.

It can be argued that STIR/SHAKEN as it stands today may not provide sufficient shielding against unwanted robocalls, particularly during the initial phase and while still not compliant with complete end-to-end all-IP concept. Thus, the implementation of multiple layers of shielding would be beneficial for optimizing the protection, including different forms of analytics, while the solutions mature and are developed further along with advances in areas such as Artificial Intelligence and Machine Learning.

Even the STIR/SHAKEN framework does not completely solve the issue of unwanted robocalls yet, but it gives needed and timely protection against bad actors.

ABOUT THE GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com.

Follow the GSMA on Twitter: @GSMA_NA.

ABOUT THE GSMA NORTH AMERICA TEAM

Headquartered in Atlanta, Georgia, GSMA North America represents and leads mobile network operators in the United States, Canada, Greenland and the Caribbean. Working alongside some of the mobile industry's most influential companies, GSMA North America aims to increase the region's commercial opportunities and develop a collaborative and socially responsible and ecosystem. In this mission, GSMA North America convenes several leading annual industry events, provides regulatory expertise and technical knowledge to support network optimization.

Document Editor
Jyrki Penttinen
Senior Technology Manager, North America
jpenttinen@gsma.com

For further information, please visit:
https://www.gsma.com/northamerica

REFERENCES

1. FCC, "FCC FACT SHEET, Wireless Messaging Service Declaratory Ruling; Declaratory Ruling - WT Docket No. 08-7," Federal Communications Commission, November 21, 2018.

2. B. Fung, "Report: Americans got 26.3 billion robocalls last year, up 46 percent from 2017," The Washington Post, 29 01 2019. [Online]. Available: https://www.washingtonpost.com/technology/2019/01/29/report-americans-got-billion-robocalls-last-year-up-percent/. [Accessed 04 02 2019].

3. Consumer Reports, "Phone Companies Can Filter Out Robocalls, They Just Aren't Doing It," [Online]. Available: https://www.consumerreports.org/consumerist/phone-companies-can-filter-out-robocalls-they-just-arent-doing-it/.

4. Federal Trade Commission, "Who's reporting robocalls?," FTC, 29 July 2019. [Online]. Available: https://www.consumer.ftc.gov/blog/2019/07/whos-reporting-robocalls. [Accessed 05 November 2019].

5. IETF, "RFC 7340," [Online]. Available: https://tools.ietf.org/html/rfc7340.

6. IETF, "RFC 8226," [Online]. Available: https://tools.ietf.org/html/rfc8226.

7. IETF, "Authenticated Identity Management in the Session Initiation Protocol (SIP)," 02 2018. [Online]. Available: https://tools.ietf.org/html/rfc8224. [Accessed 03 12 2018].

8. IETF, "SIP: Session Initiation Protocol," 06 2002. [Online]. Available: https://tools.ietf.org/html/rfc3261. [Accessed 03 12 2018].

9. IETF, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," 11 2002. [Online]. Available: https://tools.ietf.org/html/rfc3325. [Accessed 03 12 2018].

10. IETF, "The Session Initiation Protocol (SIP) and Spam," 01 2008. [Online]. Available: https://tools.ietf.org/html/rfc5039. [Accessed 03 12 2018].

11. IETF, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," 08 2006. [Online]. Available: https://tools.ietf.org/html/rfc4474. [Accessed 03 12 2018].

12. IETF, "PASSporT SHAKEN Extension (SHAKEN)," 17 10 2017. [Online]. Available: https://tools.ietf.org/html/draft-ietf-stir-passport-shaken-04. [Accessed 03 12 2018].

13. ATIS, "Signature-based handling of asserted information using toKENs (SHAKEN)," ATIS/SIP Forum NNI Task Group, 01 01 2017. [Online]. Available: https://access.atis.org/apps/group_public/. [Accessed 03 12 2018].

14. IETF, "PASSporT: Personal Assertion Token," 02 2018. [Online]. Available: https://tools.ietf.org/html/rfc8225. [Accessed 03 12 2018].

15. IETF, "Authenticated Identity Management in the Session Initiation Protocol (SIP)," 02 2018. [Online]. Available: https://tools.ietf.org/html/rfc8224. [Accessed 03 12 2018].

16. "Understanding STIR/SHAKEN," TransNexus, 2019. [Online]. Available: https://transnexus.com/whitepapers/understanding-stir-shaken/. [Accessed 13 02 2019].

17. ATIS, "Mitigation Techniques for Unwanted Robocalls: Updates on ATIS and Other Key Industry Initiatives," ATIS, October 12, 2016.

18. Transaction Network Services, "Beyond STIR/SHAKEN: Carriers Need a Multi-Layered Approach," 03 01 2019. [Online]. Available: https://tnsi.com/blogpost/beyond-stir-shaken-carriers-must-have-a-multi-layered-approach-to-robocalls/. [Accessed 07 02 2019].

19. Ribbon, "SBC and PSX for Caller Authentication and Verification," Ribbon, [Online]. Available: https://ribboncommunications.com/solutions/service-provider-solutions/security-analytics/stir-shaken. [Accessed 07 02 2019].

20. TransNexus, "Robocall prevention," [Online]. Available: https://transnexus.com/robocall-prevention/. [Accessed 12 03 2019].

21. Tech Times, "This AI Bot Will Prank Telemarketers By Talking To Them Until They Catch On," 01 02 2016. [Online]. Available: https://www.techtimes.com/articles/129723/20160201/ai-bot-will-prank-telemarketers-talking-until-catch.htm . [Accessed 03 12 2018].

22. NBC News, "Google wants to help screen those incessant robocalls," 10 10 2018. [Online]. Available: https://www.nbcnews.com/tech/tech-news/google-wants-help-screen-those-incessant-robocalls-n918766. [Accessed 03 12 2018].

23. IETF, "STIR Out-of-Band Architecture and Use Cases," IETF, 11 03 2019. [Online]. Available: https://tools.ietf.org/html/draft-ietf-stir-oob-04. [Accessed 12 04 2019].

24. G. Guthrie, "FCC calls on the telecom industry to speed up implementation of Caller ID spoofing protection," 14 May 2019. [Online]. Available: FCC Chairman Ajit Pait summoned major phone companies to implement SHAKEN/STIR caller ID authentication standards by the end of 2019.. [Accessed 7 August 2019].