Transaction Network Services

One Connection – A World of Opportunities

ROBOCALL PROTECTION WHITE PAPER

3 THINGS YOU NEED TO KNOW FOR 2017

Transaction Network Services

One Connection – A World of Opportunities

Simplifying Complex Global Data Solutions

TNS addresses the evolving needs of network operators around the globe. As the industry evolves to IoT and 5G technologies, TNS leads the development of solutions to help carriers navigate a host of infrastructure complexities and maximize their network reach through the creation of unique multi-service hub solutions. From small rural operators in the US to the largest multi-national telecommunication providers, our portfolio of mobile network, identity, discovery and routing solutions enables the successful and reliable delivery of subscriber solutions around the globe, while our clearing, settlement and anti-fraud solutions protect your subscribers and bottom line.

A single connection to TNS provides connectivity to carriers around the globe and access to a suite of advanced roaming, network, database and device solutions including a powerful LTE roaming hub platform. Regardless of the challenges faced by our customers, TNS provides world-class solutions enabling the successful delivery of services to end-customers around the world. Whether launching new subscriber services, upgrading infrastructure, or migrating services, TNS delivers mission-critical solutions in a managed services model that helps minimize complexity, reduce risk, and speed to market.

Transaction Network Services - Telecom Solutions
Contact (703) 453-8300
solutions@tnsi.com

About This White Paper

Operators have been asked to provide a solution to the robocalling problem for their customers, but navigating the range of options can feel like battling a Hydra, resulting in an increasing number of questions.

- **What are the different implementation options?**
- **Will we be investing in something effective?**
- **Which of the options are long versus short-term investments?**
- **Will we find ourselves blocking important calls that our customers want to receive?**
- **How can we address caller ID spoofing?**

We will lay out three key initiatives to help you better understand the timeline and the choices available to you. The goal is to enable informed decision-making that will allow you to protect your customers from fraudulent and harassing callers, improving your relationship, decreasing customer support calls, and increasing retention.

Contents

Framing the Problem

An Overwhelming Range of Solutions

Robocalls and telemarketing calls currently represent the **number one source of consumer complaints** at the FCC[1].

In terms of both hassle and cost to consumers, over the past decade or so, robocalls have evolved into a high-impact, high-visibility problem.

According to Consumers Union, the policy and action arm of Consumer Reports, an estimated $350 million a year is lost to phone scams[2].

As a result, the FCC provided guidance on June 18, 2015, allowing operators to block problem robocallers, and the CRTC (Canadian Radio-television and Telecommunications Commission) has provided similar guidance to Service Providers in Canada[3] [4].

Operators have a range of solutions for addressing problem calls available to them, spanning from over-the-top apps for mobile phones to complex, industry-led new standards and protocols. Operators are in the spotlight, and under pressure to understand, choose from, and implement these options.

For the purposes of this paper, we will focus on three less well-understood industry solutions including: Do-Not-Originate; STIR/SHAKEN; and Analytics Server. We will walk through their meaning, expected timeline, and how they all tie together to create a layered approach to ending robocalls.

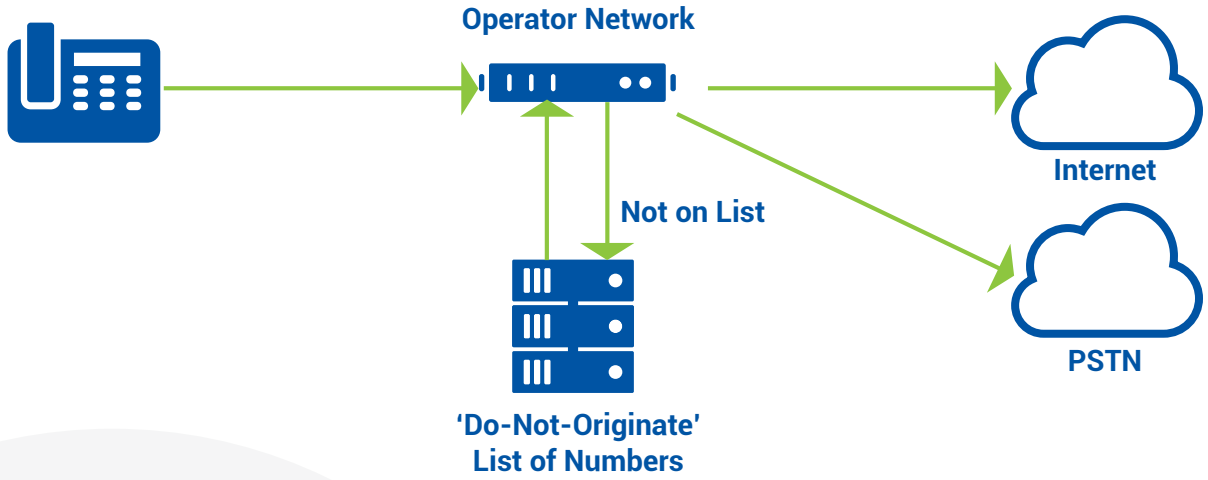
1 https://www.fcc.gov/news-events/blog/2016/07/22/cutting-robocalls
2 http://consumersunion.org/end-robocalls/
3 https://www.fcc.gov/document/fcc-strengthens-consumer-protections-against-unwanted-calls-and-texts
4 http://news.gc.ca/web/article-en.do?nid=1148039

1. Do-Not-Originate (DNO)

ALSO KNOWN AS 'NETWORK-DIRECTED CALL BLOCKING'

Overview

VoIP permits both legitimate and illegitimate caller name and number spoofing. Do-Not-Originate (DNO) involves the management of an outbound-calling blacklist consisting of the telephone numbers of financial institutions, government agencies, the 911 Do Not Call list, etc. used solely to receive inbound calls. This DNO list will be checked by VoIP gateways as they process outbound calls.



The goal is to block origination of calls from numbers that should never originate phone calls. These numbers belong to entities such as the IRS, often used in caller ID spoofing, usually with the intent to defraud. DNO could potentially allow the carrier to block any call that is using a non-allocated North American Numbering Plan NPA-NXX number, as well. On September 30, 2016, the FCC provided clarification that numbers added to the DNO list may be blocked by gateways[5].

5 https://apps.fcc.gov/edocs_public/attachmatch/DA-16-1121A1.pdf

At the end of October 2016, members of the Robocall Strike Force presented the FCC with the results of a DNO trial. **A 90% reduction in IRS scam calls was reported[6].**

While implementation of DNO is straightforward from a technical perspective, the challenges lie in the creation, maintenance, and security of the list server.

Once established, future additions to the list will have to be authenticated.

The authority for provisioning of this service will have to be established.

Finally, similar telephone numbers will not be included in the database and may still be used for fraudulent purposes.

Example: The IRS uses the number 800-829-1040 to receive tax help questions from individuals. Though this number may be added to the DNO registry because it doesn't originate calls, this addition does not preclude a similar number, possibly also ending in "1040", from being used to impersonate the IRS and defraud consumers.

New Necessary Services

DNO Registry

Roles

DNO Registry Service Provider

Timeline

DNO has an implementation goal of the **end of 2017**

6 https://www.onthewire.io/carriers-plan-to-implement-do-not-originate-list-to-defeat-robocalls/

2. STIR/SHAKEN

Authentication and Verification

Whereas **DNO** is designed to prevent the origination of calls from telephone numbers that should not be making outbound calls, **STIR/SHAKEN** addresses identity authentication for calls traversing the SIP network, in order to mitigate caller ID spoofing.

STIR can be used both to **validate origination in real time** and to **perform a traceback**, after a call is complete.

STIR/SHAKEN is more complex than DNO, so, in addition to providing a high-level summary, we will also provide a more detailed explanation for those interested in a deeper understanding. We will then review open questions from a policy and implementation standpoint.

Perhaps most important to note from the outset is that STIR may only be used to authenticate and validate origination of the call for U.S. domestic calls, and is applicable for SIP-to-SIP calls only. STIR is not applicable for TDM, nor will it work if the network path of the call traverses a legacy network, as opposed to an uninterrupted SIP-to-SIP call.

Terminology

STIR: Secure Telephone Identity Revisited - defines a signature to verify the calling number, and specifies how it will be transported in SIP "on the wire".

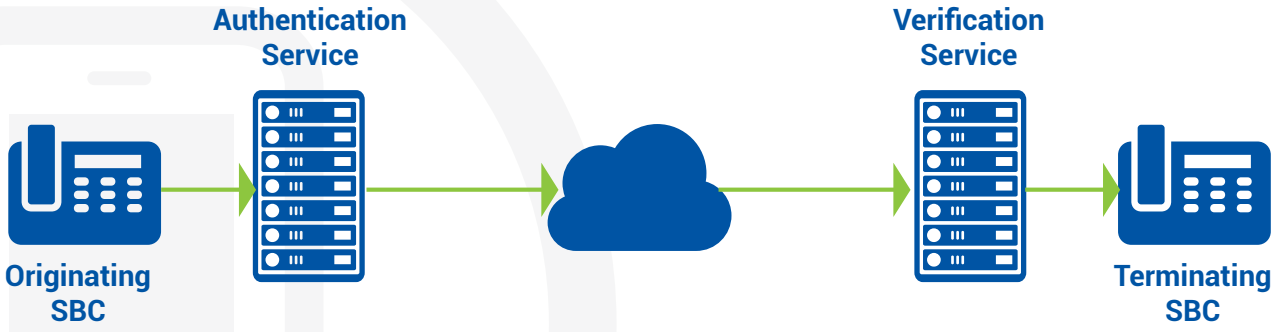
SHAKEN: Signature-based Handling of Asserted information using toKENs - the framework document developed to provide an implementation profile for Service Providers implementing STIR.

Together, **STIR** and **SHAKEN** represent the SIP protocol changes, signature standard, and interoperability framework. STIR was developed by members of the IETF, and the SHAKEN framework was the work of the joint ATIS SIP Forum Task Force.

Overview

The goal of the initiative is to deliver what is referred to as a "secure identity attestation mechanism" for SIP calls. Updates and enhancements to the current SIP protocol will allow **identity information to be passed by an Authentication service via the SIP identity header to a Validation service**, where it is checked before the call is completed.

The information contained in the SIP header will allow regulatory agencies to identify who made the identity assertion via a mechanism called a **'traceback'.**

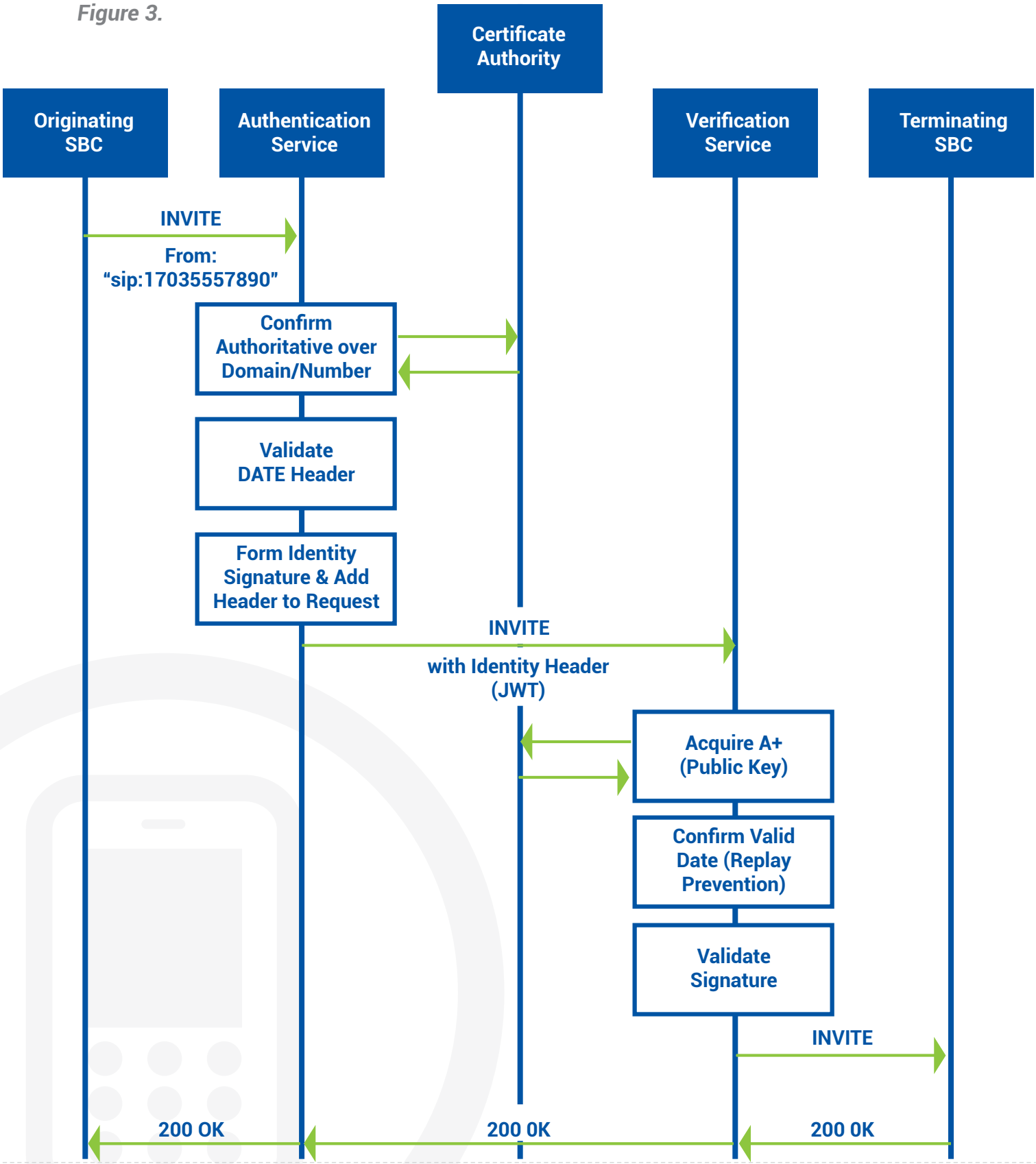


How It Works

The Authentication Service creates a public/private key-pair, then sends a Certificate Signing Request (CSR) to the Certificate Authority (CA), also known as a PKI Trust Anchor. Once its identity is verified by the CA and the CSR is signed using the private key, the Authentication Service is able to generate a JSON web token into the SIP header and send a SIP INVITE. The Authentication is now able to sign multiple requests.

The subsequent process is described in Figure 3.

Figure 3.


Certificate Authority
Originating SBC
Authentication Service
Verification Service
Terminating SBC
INVITE
From:
"sip:17035557890"
Confirm Authoritative over Domain/Number
Validate DATE Header
Form Identity Signature & Add Header to Request
INVITE
with Identity Header (JWT)
Acquire A+ (Public Key)
Confirm Valid Date (Replay Prevention)
Validate Signature
INVITE
200 OK
200 OK
200 OK

With STIR, the SIP protocol is enhanced to validate claims of E.164 numbers, or SIP URIs and their corresponding E.164 numbers.

The IETF has chosen PASSporT as the token mechanism used to sign originating identity, due to its independence of any signaling call logic, allowing for flexibility of implementation.

The PASSporT extension permits for Attestation ("attest"), indicating the level of attestation a Service Provider can provide about a caller's legitimacy, and carries an Originating Identifier ("origid"), indicating the originating trunk, node, or customer as a mechanism for call tracebacks.

The Authentication Service adds a JWT (JSON Web Token) identity header to the request. This token is made up of a Javascript Object Signing and Encryption (JOSE) header, JWS (JSON Web Signature) payload, and JWS signature added to the SIP INVITE request. (CSeq, Call ID, Contact, Message body, and ID-info will be removed.)

An accurate time stamp is essential to prevention of replay schemes, which try to use the signature to forge calls from a number.

If the signature can be verified, the Verification Service passes the call to the UAS (User Agent Server).

Levels of Attestation

Full meets 3 criteria: 1) the signing provider is responsible for the origination of the call onto the network; 2) they have a direct, authenticated relationship with the customer, allowing them to identify the customer, if needed; 3) and they have established a verified association with the telephone number used for the call.

Partial meets 2 of the 3 criteria: 1) the signing provider is responsible for the origination of the call onto the network; 2) they have a direct, authenticated relationship with the customer, allowing them to identify the customer, if needed; but they are not able to establish a verified association with the telephone number used for the call.

Gateway attestation does not meet these criteria, but signal that they acted as the entry point of the call onto the network. They affirm no relationship with the initiator of the call (e.g., an international gateway), but may sign for traceback purposes, without verifying the identity of the customer or telephone number[7].

Tracebacks

A **historic traceback** involves the use of the information transmitted via the SIP header to determine the originating provider of the call. Level of detail is dependent upon level of attestation, as previously discussed. Requests may be initiated either by a regulatory body or by a Service Provider either on its own or on behalf of a number of customer complaints. Policy around tracebacks and repercussions for violations are still being determined, but it is generally understood that the entity that acts as the Authentication Service is ultimately responsible, if the information provided in the SIP header is not correct. **Prospective tracebacks** may also be used to log future calling behavior of a telephone number.

Sources of Origination

STIR will be applicable for ATA, DSLAM, VoLTE, and DOCSIS-originated calls. ATAs, used for landline SIP, use cryptographic authentication between the ATA and the SIP registrar. DOCSIS and VoLTE involve registration at the DOCSIS adapter and VoLTE device level. DOCSIS operators will be required to address the ability for neighbors to spoof one another, as the access network is shared media. DSLAM does not share this concern, as the line identifies the user[8]. IPPBX will be able to set its own policy, and enable authentication and validation via their provider or as part of their Service Provider's business subscriber Application Server[9].

7 http://www.sipforum.org/component/option,com_docman/task,doc_view/gid,821/Itemid,261/
8 https://s2erc.georgetown.edu/sites/s2erc/files/files/upload/stir_status_and_analysis.pdf
9 http://www.sipforum.org/component/option,com_docman/task,doc_view/gid,821/Itemid,261/

No ID Header

If the **signature is not present or fails validation,** the Verification Service's response will depend on the preferences of the Service Provider. They may decline the call with a modified From field; they may blackhole the INVITE; or they may send back a 438 response code. They may also choose to pass the call through to the UAC with a warning of some kind. Underlying all of these options is yet another possibility: a Service Provider may choose not to sign its calls; **use of the mechanism STIR provides is optional.**

Legitimate Spoofing

There are several instances where an **entity may give permission to the Authentication Service for a related party to provide their calling name and number** to another party to use. For example, a customer service representative may use an enterprise's caller name and number, rather than their own. An enterprise may permit a third party to make calls on their behalf. In these cases, policy will be required around the process for permission to be granted by the enterprise to the in-house representative or the third party and passed to the Authentication Service. This can be additionally complicated by the fact that the enterprise and the third party may use different Service Providers.

New Necessary Services

Authorization and Verification Services
Certificate Authority (CA)
Governance Authority

Roles

STIR requires introduction of new entities along the chain of trust. If the root authentication for a call comes from a foreign CA, for example, the call cannot be trusted at the root level. It's for this reason that STIR can only address domestic calls.

The role of trusted root CA (PKI Trust Anchor) and Governance functions may be performed by the FCC, or multiple entities qualified to issue certificates. The FCC could ask a body such as ATIS to determine the CA or CAs. STIR will likely be rolled out initially using Service Provider-managed certificates. The important issue is trust.

The Authentication and Verification Services could be performed by large Service Providers, but are more likely to be performed by a trusted third party for most Service Providers.

Questions

Many questions are still unanswered.

- **Who issues certificates?**
- **How do we validate that those issuing certificates can be trusted?**
- **How secure is the computer storing the private key?**
- **How are certificate recipients validated?**
- **What happens after call validation?**
- **How is the public educated about initiating a traceback?**
- **Where will post-call reporting take place?**
- **How are tracebacks enforced?**
- **Can a private key be intercepted and misused?**
- **How are keys revoked? What happens when a number is ported?**
- **What's the TTL for a certificate and can it be extended via a hack?**
- **How are third parties making legitimate calls on behalf of an enterprise authorized to spoof their caller name and number?**
- **What do operators have to buy and deploy? When will it be available? How much will it cost?**
- **How, if at all, do we recover costs of implementing a strategy?**
- **What will our liability be if we block a good call? Or authenticate a bad call?**

Timeline

The FCC provides a detailed timeline in the Robocall Strike Force readout dated October 26, 2016. https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf

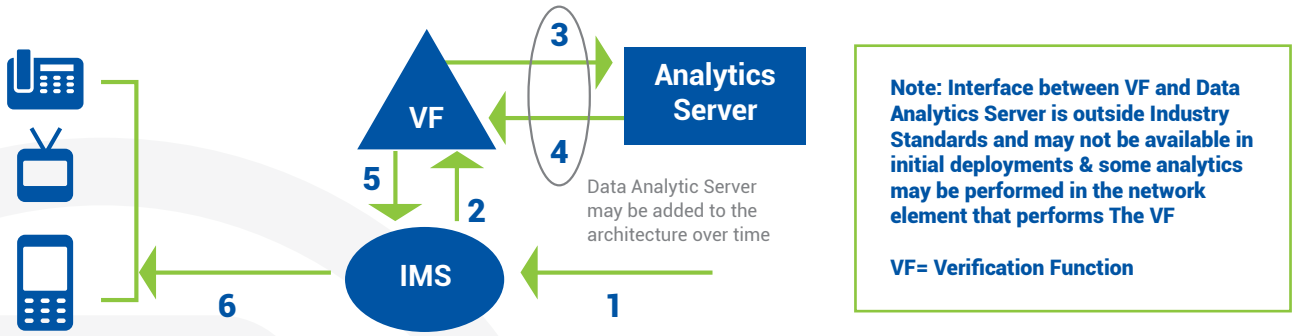
3. Analytics Server

Overview

Once fully deployed, Do-Not-Originate and STIR/SHAKEN will provide crucial layers of protection. Among industry experts engaged in analysis of the issue, however, consensus is clear: a layered approach requiring access to an Analytics Server at the Verification point is also required.

Per the FCC's October 2016 Robocall Strike Force readout[10], the ATIS/SIP Forum's October 2016 Mitigation Techniques for Unwanted Robocalls: Updates on ATIS and Other Key Industry Initiatives[11], and the CRTC's November 2016 Compliance and Enforcement and Telecom Regulatory Policy CRTC 2016-442[12], real-time analysis of calling data to determine telephone number reputations will provide that additional layer that permits detection of calls the other initiatives do not address, such as circuit-switched originations and IP gateways across which international and wholesale traffic traverse.

Figure 5. **- FCC and ATIS/SIP Forum documents reference the following diagram:**



"Even with the deployment of the STIR/SHAKEN framework, traffic from CS originations and IP Gateways (International & Wholesale) will be an issue for robocalling, therefore deployment of other mitigation techniques in a layered approach is required."

Martin Dolly, AT&T, Mitigation Techniques for Unwanted Robocalls: Updates on ATIS and Other Key Industry Initiatives, October 12, 2016

10 https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf
11 https://www.atis.org/01_news_events/webinar-pptslides/robocallslides_final.pdf
12 http://crtc.gc.ca/eng/archive/2016/2016-442.htm

Value of Real-time Analysis

Today, it is possible to detect caller ID spoofing and other malicious and nuisance robocalling behavior based on real-time network data analytics; in other words, **the Analytics Server functionality described in the October 2016 FCC Robocall Strike Force report is available now.**

STIR/SHAKEN and DNO will eventually remove some of the burden borne by the Analytics Server today, but will not render this crucial component unnecessary.

Whereas blacklist solutions sit outside the network and depend on collection of data about historical behavior of a telephone number, with no ability to determine when to remove numbers from the list, real-time analytics examine calling behavior and make determinations as the behavior is occurring. Because bad actors move from number to number in a short period of time, and will evolve and adapt to evade new detection mechanisms, the ability to make decisions about a telephone number's reputation based on calling behavior will continue to provide **an essential layer of consumer protection.**

Additionally, this functionality is not dependent on business inputs and participation, as DNO is, nor is it limited to domestic SIP-to-SIP calls, as STIR/SHAKEN is. Further, whereas STIR does not address caller intent, the Analytics Server function can infer intent from analysis of calling patterns.

Access to an Analytics Server is available for **all types of Service Providers across all networks, whether VoIP or TDM**, via ENUM, SIP, AIN, or RESTful API. As a result, a key component of proposed standards **can be implemented well in advance of the deployment of other layers of protection.**

Roles

Analytics Server

Timeline

Available now

Conclusion

As we move through 2017, Service Providers have a range of options for addressing robocalls. When deciding which to implement, it is important to guard against selections that offer only limited or short-term solutions.

A Do-Not-Originate (DNO) registry, STIR/SHAKEN, and an Analytics Server have industry consensus behind them. The effectiveness of these solutions will, of course, correspond directly with how widely they are adopted.

Though technical implementation decisions around these services have been thoroughly documented, there remain many open questions around policy and costs. The time for Service Providers to weigh in on those questions is now.

In addition, several new roles will have to be filled including: DNO registry provider; Authentication and Validation Service providers for STIR/SHAKEN; one or more STIR Certificate Authorities; a STIR Governance Authority to follow up on tracebacks and address issues that may arise with errant certificates or authentications; and finally, the Analytics Server function, providing real-time reputational data.

In terms of timeframes, DNO has a goal of the end of 2017 for implementation; STIR/SHAKEN is being rolled out over the next several years; and Analytics Server functionality is available today. Providers who wish to offer protection to their customers can implement this part of the solution immediately.

TNS is able to support DNO registry services, Authentication and Verification services to support STIR, and is already partnered with leading Service Providers as their Analytics Server, with our Call Guardian product.

TNS Call Guardian offers:

- Reasonably-priced, flexible, easy integration
- Carrier-grade service and support
- Ability to integrate with AIN, SIP, ENUM, or API delivery of data within the call flow
- Real-time analytics based on a learning algorithm, with insight into the calling behavior of ~500M North American telephone numbers
- Co-located or cloud-based resolution
- Subscriber white and blacklists, and more

To find out more about how TNS can help you with a wide range of telecom solutions:

USA +1 703 453 8300 **Europe** +44 (0)114 292 0200 **Asia Pacific** +61 2 9959 0800

solutions@tnsi.com **www.tnsi.com**

US MARCH 2017