INTERNATIONAL INTERCONNECTION FORUM

FOR SERVICES OVER IP

(i3 FORUM)

(www.i3forum.org)

**Source:**

**Working Group “Technology”**

**Working Group “Fight against Fraud”**

**i3 forum keyword: Voice, CLI, Interoperability, OBC**

# Technical Report

# Calling Line Identification (CLI) spoofing

# (Release 1.0) October 2020

This document provides the i3 forum’s perspective on the management of the identity of the caller (Calling Line Identification) throughout the end-to-end call path, focusing on voice services originated from fixed and mobile networks.

The scope includes both the description of Calling Line Identification (CLI) spoofing use cases and the available techniques that can be applied for preventing, detecting and mitigating CLI spoofing in the international wholesale environment.

CLI spoofing prevention and mitigation is important in order to be compliant with regulatory constraints, for revenue protection and for customer satisfaction. It does not intend to duplicate other existing specifications or documents on the same issue, but to complement these documents with the perspective of the International Carrier members of i3forum.

# Table of Contents

## Management Summary

This report provides the i3forum’s carrier perspective on the handling of Calling Line Identification (CLI) spoofing based on a joint analysis of i3forum’s Technology and Fight against Fraud Workgroups. The scope includes both the description of CLI spoofing use cases and the available techniques that can be applied for preventing, detecting and mitigating CLI spoofing in the international wholesale environment.

First an introduction is given of the problem and CLI spoofing is used in committing various fraud types, problematic to subscribers and having regulatory attention. The different aspects are addressed and what carriers looking to do, why carriers are looking into it and how the issue is being addressed today.

CLI Spoofing is creating a multi-problem statement for the Wholesale Business of IPX Carriers with the implementation of STIR/SHAKEN in countries like the USA and the foreseen rollout of call validation solutions in other countries, both answering of incoming calls by subscribers is changing as well as how traffic from IPX carriers is perceived by the terminating service providers in these countries. Playing an active role and implementing a Call Signing solution by IPX Carriers creates various opportunities for Business Value for their Wholesale Business.

The different supporting mechanisms and solution alternatives for the protection and prevention of CLI spoofing are being analyzed and evaluated in this report. The approaches fall into two different categories, the solutions for Call Validation versus the solutions for Call Fraud Detection.

The call validation solutions based on STIR/SHAKEN are most effective but require specific conditions like end-to-end support of the SIP signaling and a trusted environment for the distribution of key material. As a result, alternative solutions are being developed that are less restrictive and complex that provide similar protection and prevention for CLI spoofing.

These out-of-band solutions offer either complementary solutions for STIR/SHAKEN to cover situations like the reuse of existing TDM networks and call signing with enterprise networks, or alternative systems that are working signaling agnostic and not needing a central authentication authority. The latter look more suited for direct use between carriers to fight CLI Spoofing for international calls.

A summary table complements this report that evaluates the different technology solutions especially from a wholesale carrier perspective. A clear distinction is made between the STIR/SHAKEN solutions versus the Out-of-Band call validation solutions. It can be deduced that use of a special routing number should be avoided given the impact of the wholesale carrier business and operational practices.

The findings in this report will be used for the further evaluation of these solutions and in collaboration with other standardization initiatives like GSMA VINES to present the wholesale carrier perspective and to ensure the inter-operability of the solutions in building a critical mass in the industry to combat fraud and other abuse with CLI spoofing.

# 1. Symbols and Acronyms

| | |
|---|---|
| ATIS | Alliance for Telecommunications Industry Solutions |
| CPS | Call Placement Service |
| CLI | Calling Line Identification |
| DLT | Distributed Ledger Technology |
| EEC Code | European Electronic Communications Code |
| FAS | False Answer Supervision |
| FCC | Federal Communications Commission |
| FQDN | Fully Qualified Domain Name |
| FTC | Federal Trade Commission |
| GSM | Global System for Mobile Communications |
| GSMA | GSM Association |
| HTTP | Hypertext Transfer Protocol |
| IETF | Internet Engineering Task Force |
| IMS | IP Multimedia Subsystem |
| IPX | IP eXchange |
| IRSF | International Revenue Share Fraud |
| ISUP | ISDN User Part |
| MAP | Mobile Application Protocol |
| ML | Machine Learning |
| MNO | Mobile Network Operator |
| OBC | Origin Based Charging |
| OBR | Origin Based Rating |
| OOB | Out-of-Band |
| OSP | Originating Service Provider |
| OTT | Over-The-Top |
| PBX | Private Branch Exchange |
| PSTN | Public Switched Telephone Network |
| RCS | Rich Communication Suite |
| SEISMIC | Stopping Exploitation Inter-Network Signal Fraud by Mitigating Illegitimate Communications |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| S8HR | S8 Home-based Routing |
| SIP | Session Initiation Protocol |
| SMS | Short Message Service |
| SS7 | Signalling System 7 |
| STIR | Secure Telephone Identity Revisited |
| TDM | Time Division Multiplexing |
| TSP | Terminating Service Provider |
| TT | Trouble Ticket |
| UE | User Equipment |
| VINES | Validating INtegrity of End-to-End Signalling |
| VoIP | Voice over IP |
| VoLTE | Voice over LTE |

# 2. References

[1] IEEE, "End-to-End Detection of Caller ID Spoofing Attacks", June 2016

[2] 3forum, "Fraud classification and recommendations on dispute handling within the wholesale industry, Release 3.3 – December 2019”

[3] Andraz Oblak (Hexagon Group) “Overview of SS7 CVS call validation”

[4] Solid Specification Draft: https://github.com/solid/solid-spec

[5] FCC news item “FCC, FTC demand robocall-enabling service providers cut off covid-19-related international scammers”
https://docs.fcc.gov/public/attachments/DOC-364482A1.pdf

[6] IETF standard “STIR Out-of-Band Architecture and Use Cases”

[7] ATIS standard “Signature-Based Handling of Asserted Information Using Tokens (SHAKEN) For TDM Networks (TDM-SHAKEN)”

# 3. CLI spoofing

## 3.1. Introduction

The i3forum's Technology Workgroup focused much of its collaborative efforts in producing a document about CLI Management in 2019. This activity became a priority due to the growing trend of origination-based charging primarily in Europe but also in other regions such as West Africa, East Africa, etc. Now that A-Number, the number of the caller, impacts the cost of termination, having a clean and consistent approach to managing it is a clear priority. The international carrier community quickly identified the need for more work in this area to combat increasing inconsistencies. Without a standard approach for determining the A-number costly disputes between international carriers and service providers mounted, it was clear a document providing technical guidelines for the consistent management of CLI throughout the end-to-end call path was an important first step required by the international carrier community.

With this foundation in place the i3forum's Technology and Fight against Fraud Workgroups are now extending their focus to address the authenticity of the CLI. CLI Spoofing and the assumption of a false identity for harmful purposes towards third parties is done either by calls from a malicious caller to the callee victim or by means of a messaging service. In the latter case this refers to SMS Spoofing and the Sender ID shown to the recipient is modified to send a text message chosen by the sender. This document is focused on fraud aspects related to voice service and not messaging, so this report only deals with cases of CLI spoofing applied to voice services.

False CLI has impacted international voice connections for many years as fraudsters manipulate CLI to bypass higher termination rates (toll bypass and intra/inter-state fraud two common scenarios). More recently, regulatory agencies have created and are enforcing penalties for setting up calls with spoofed and manipulated CLI with intention to commit fraud and deceit. Consumers are inundated with unwanted robocalling and malicious marketing campaigns which sparked an intense regulatory crack-down. While regulation on national level was first implemented in North America (US and Canada), also regulation is now enacted in France and in preparation in Germany, and the next revision of the European Electronic Communications (EEC) Code is expected to include CLI spoofing which will drive the remainder of the EU in the same direction.

This regulation in each country for CLI verification is not necessarily demanding for the same technical solution and therefore a potential challenge how inter-operability of these different solutions is to be resolved for the traffic between different countries.

Addressing the authenticity of CLI is a major undertaking for the international carrier community. It represents a fundamental shift in the traditional positioning for managing CLI on carrier networks (acting just a pass through). Creating an end-to-end solution is a tremendous challenge due to the complexity of many international calls flows and volume of carriers. Not only does it require intense collaboration between the carrier community but also close cooperation with domestic operators to ensure interoperability that meets the end-users needs.

## 3.2. What are carriers looking to do?

The i3forum's Technology and Fight against Fraud Workgroups are exploring options to fight against CLI spoofing and manipulation in the international wholesale environment. While focusing on traditional voice services, the issue does also impact messaging and therefore RCS. This will be considered when exploring approaches and solutions for preventing, detecting, and mitigating CLI spoofing and manipulation.

Core to all i3forum initiatives, by pooling resources and expertise at the carrier industry level, carriers will be well positioned to find solutions that fit the unique challenges of the carrier industry, promote a common approach (avoiding siloed solutions), while potentially reducing cost and complexity. Carrier collaboration is necessary to successfully position their evolving role when it comes to safe-guarding CLI. Collaboration will also be key in uncovering the best solutions, building the necessary supporting processes and procedures, and investigating any potential commercial implications.

## 3.3. Why carriers are looking into it?

The primary benefit for working on this topic is revenue protection. Consumers have reached a breaking point where false CLI prevents them from answering their phone calls. Unanswered calls remove revenue and margin from national and international voice and messaging communications (already under tremendous pressure from natural market conditions) while taking up network resources.

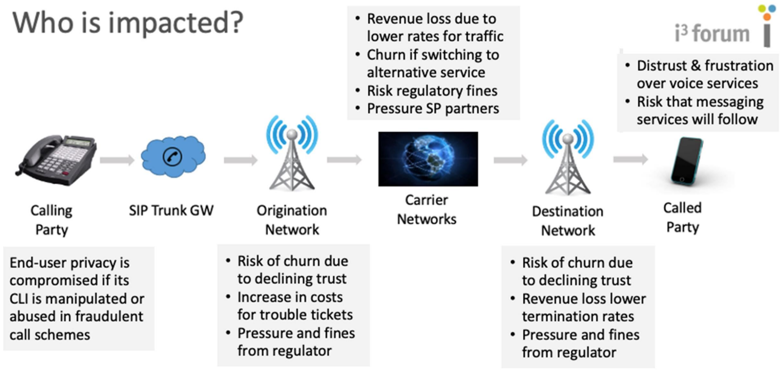
Consumer distrust for the traditional service provider offerings encourages them to switch to OTT alternatives. OTT alternative services remain a major threat to the market traditional carriers address. Non-revenue-bearing traffic streams (unanswered calls) coupled with addressable to non-addressable traffic shifts (migration to OTT), provide a major incentive for the carrier community to act.

The Origin Based Charging (OBC) principle opened the door for increased CLI manipulation in international traffic streams. Fraudsters manipulate CLI for calls terminating to OBC markets falsely masking them as intra-regional calls billed at lower rates. This CLI manipulation can remove several cents per minute of revenue and margin for traffic to many markets. Carriers and destination network operators are left with lower revenue while managing inter-operator billing disputes and other operational issues resulting from CLI manipulation.

Additionally, industry regulators impose fines when false CLI is carried by service providers. These penalties exist today in the US and Canada. The FCC has also stated that fines could be imposed to domestic and international carriers that forward or allow these fraudulent calls into the US. While the workgroup has not heard of any specific cases yet, this position could result in fines to international carriers when calls and messages with spoofed and manipulated CLI enter the US and Canada undetected and unmitigated. A first step in this direction are the recent official communications from FCC in collaboration with UST Traceback Group regarding a group of carriers facilitating robocalling with spoofed CLIs presumably.

Carriers could assist in solving the international challenges of their local service provider partners. The opportunity is to better position the carrier community with their local partners. Domestic solutions are inherently too limited, and the domestic operator may be helped by their carrier partners to extend their reach when it comes to delivering CLI validated voice and messaging services globally. By solving this problem for their local service providers, it will strengthen ties and further validate the carrier industry's value proposition.

The chart in Figure 1 outlines how various parties along a general call flow are impacted by CLI spoofing and manipulation.



- Revenue loss due to lower rates for traffic
- Churn if switching to alternative service
- Risk regulatory fines
- Pressure SP partners

- Distrust & frustration over voice services
- Risk that messaging services will follow

End-user privacy is compromised if its CLI is manipulated or abused in fraudulent call schemes

- Risk of churn due to declining trust
- Increase in costs for trouble tickets
- Pressure and fines from regulator

- Risk of churn due to declining trust
- Revenue loss lower termination rates
- Pressure and fines from regulator

**Figure 1 – Impact of CLI Spoofing on the various parties in a general call flow**

## 3.4. How is the issue being addressed today?

International carriers have individually implemented a number of approaches to combat fraud within wholesale voice and messaging, however, none of these approaches are effective at verifying the authenticity of each and every CLI carried on their networks. Examples of this would be the detection by FMS systems of wrong or incorrect CLIs, CLIs that are not allowed to generate calls, abnormal traffic patterns and false CLI embedded within, fraud numbers are 'blacklisted' due to repetitive issues and these numbers were exposed to CLI spoofing or manipulation, SIM bypass testing or SMS termination monitoring flags issues to specific destinations within a limited test footprint, or dial string policies and network monitoring prevent fraudulent calls from entering their networks (ineffective as increasingly false CLIs are often compliant with regulated call formats).

One carrier community driven effort that could prove beneficial in the future is the GLF's CBAN project which looks to leverage Distributed Ledger Technology (DLT) for CLI spoofing. The project's current focus is on the wholesale voice settlement process, however, a second phase of the project is targeted towards wholesale voice fraud detection and mitigation. The workgroup believes DLT could play a role in an international CLI verification solution, however, CBAN is not addressing this use case today.

The following issues are identified with these Carrier Peripheral Approaches:

- Require constant monitoring and adjustment
- Slow to react as suspicious patterns serve as trigger
- Limited coverage with SIM Box and SMS Termination monitoring
- No visibility into validity of each incoming CLI
- False positives with whitelisting and blacklisting approaches
- Lack of alignment and continuity across the carrier industry.

Finding the right solution is one thing, more collaboration, analyzing solution alternatives, clarifying the carrier role, and implementing supporting business and operational processes is required as well like:

- Investigate commercial and business functions implications (when a solution has been identified)
  - Internal network vs. new service
  - CLI verified routing table
  - Free of charge vs. mark-up (cost of business? Should be free?)

- Supporting policies and processes (when a solution has been identified)
  - Obligations and business process to operate a solution
  - How would we use the solution?
  - Who has the responsibility to detect false CLI?
  - Who has the responsibility to act when false CLI is detected?
  - What do we do when false CLI is detected?

# 4. System environment for CLI spoofing mitigation

In the United States, the Truth in Caller ID Act prohibits anyone from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm or wrongly obtain anything of value. Anyone who is illegally spoofing can face penalties of up to $10,000 for each violation. However, modification of the caller ID is not always illegal. There are legitimate, legal uses for caller ID modification, like when an employee calls a customer from the personal mobile phone and displays the office number rather than the personal phone number or a business displays its toll-free call-back number.

In the wholesale environment, detecting and isolating CLI spoofing requires more sophistication with the increasing prevalence of SIP applications and internet evolution. In fact, it is very easy to carry out spoof CLI using any SIP client or a PBX Different from the retail world, where the carriers know the range of phone numbers that they own and they can use internal database to validate them. In the international wholesale environment, carriers are passing traffic from different sources and destinations. In the past, international wholesale carriers typically did not take actions to determine validity of CLI since carriers are in the middle of transiting traffic from the source to destination. However, the fraudsters are ramping fast due to low cost of making international calls. Therefore, international carriers need to work together to stop these fraudulent activities and preserve i3forum members' reputable company brand as ethnical and socially responsible.

Depending on the situation, modification of the CLI is not always illegal. For instance, an IP phone could be registered to a company's PBX, and the caller uses a legit company's phone number to make outbound calls to his/her client. A doctor could modify his CLI to ensure his/her patient knows it's from the doctor's office. Besides, the technical challenge in identifying CLI spoofing, there is another problem which is to identify the intention. It is very difficult to isolate and identify the validity of the CLI. However, when there is a problem, there are many solutions.

## 4.1. STIR/SHAKEN

In the United States, FCC requires carriers to implement call verification technology by the end of June 2021. The project is known as STIR/SHAKEN (Secure Telephony Identify Revisted / Signature-based Handling of Asserted information using toKENs) which allows service providers to validate the origin of the phone number. Many large telecommunication equipment vendors are implementing the STIR/SHAKEN solution to their products.

In summary, STIR/SHAKEN validation takes 3 main stages:

1. **Originating Switch or Network**

Validates the Caller-ID and applies "attestation" tag of A, B or C

In short A, B, and C are attestation levels:

- "A" for being fully responsible for the origination of the call onto the IP based network. Example: Residential customers hosted at an in-network softswitch or IMS.
- "B" for being partially responsible, but has not to establish a verified association with the number used for the call. Example: Enterprise PBX subscriber.
- "C" for having no relationship with the initiator of the call. Example: international gateways.

2. **Signing & Verification**

Calls leaving a carrier's network are signed by encrypting an identity header, and calls incoming to a carrier's network that are already signed are verified while decrypting the Identity header.

3. **Terminating Switch or Network**

Verification results (“Pass”, “Fail”, or “Not Performed”) are to be passed to SIP endpoints in the SIP Invite. The decision to complete the call is determined by termination carrier’s policy.

STIR/SHAKEN works only if all retail carriers work together to implement the solution. This implementation is required for all carriers in the United States. It was designed to allow expansion to carriers outside of the United States.

### 4.1.1. Statistical Calculation Approach

For international carriers, this solution might be difficult to implement in every country. Another method to tackle CLI-Spoofing is using mathematic algorithms to determine if a call is valid or not by looking at the calling and called party numbers.

### 4.1.2. CLI Validation via Active Test probe

This approach is in use by carriers for over 10 years. There are many service providers deployed probes around the world and charge the carriers for the service. In summary, this service might not be able to identify fraudster on the origination side, but it is capable of identifying downstream suppliers to determine if the CLI has been spoofed or passed to an illegal PBX.

## 4.2. Business Value of Call Signing for Wholesale Carriers

With the implementation of STIR/SHAKEN in countries like the USA and the foreseen rollout of call validation solutions in other countries, both answering of incoming calls by subscribers is changing as well as how traffic from IPX carriers is perceived by the terminating service providers in these countries.

This results in the following multi-problem statement for the Wholesale Business of IPX Carriers:

- **Declining call answer rates for traffic to countries like USA:** for international calls the CLI will be signed with C-level attestation at ingress nodes.
- **Mandated roll-out of STIR/SHAKEN will increase the problem:** the more customers regain trust and get used to verified calls the more chances unverified calls will be distrusted: STIR/SHAKEN is still evolving and more operators will add call validation treatments measures “scam likely” over time.
- **High cost:** for carriers with their own retail arm (typically ex-incumbents), implementing STIR/SHAKEN will mean a very substantial investment in order to be capable to label each and every initiated call from their retail customers and then send it to international termination. For pure wholesalers on the other hand, who are just transiting (already labelled) calls, it is either a low-cost CAPEX investment or no cost at all – depending on their currently used infrastructure.
- **Outbound roamers overseas calling home becomes problematic:** outbound roamers travelling outside the STIR/SHAKEN ecosystem possess caller IDs who are when not travelling “check marked – Caller Verified”. This will lead by default for the receiver of the call to distrust this particular call. Not applicable for VoLTE roaming with S8HR, see NOTE.
- **Competitive disadvantage:** if other competitive carriers are able to verify calls, these carriers become more favorable and trusted.
- **Regulatory penalties:** given the fight against abusive robocalling practices, regulatory bodies like the FCC in US are starting to impose restrictions like the recent exclusion of some IPX carriers to send traffic to the USA and fining actors of robocalling practices. See e.g. for more background the FCC news item “FCC, FTC demand robocall-enabling service providers cut off covid-19-related international scammers” [5].

NOTE This problem will disappear once VoLTE roaming S8 Home Based Routing (S8HR) is being implemented. Then the call will originate from the home carrier network and thus can be signed and verified.

Implementing a Call Signing solution by IPX Carriers creates the following Business Value for their Wholesale Business:

- **Authentic international calls bound for STIR/SHAKEN governed regions and countries will get A-level attestation:** these calls will appear as “caller verified”. This includes outbound roamers overseas making calls to their relatives and business contact at home.
- **The carrier or operator service comes more valuable:** it will improve the answer rates and gives the IPX carrier a head start and competitive advantage on this developing issue.
- **Investment protection:** in case there will be global adoption for STIR/SHAKEN, the unit cost of implementing such solution will become – most probably – significantly cheaper, than it is today and therefore will mean lower barrier for carriers to apply this solution for CLI verification.
- **Effective trace back:** every signed call can be traced back to the signer by which complaints can be pointed to the correct identity and the originator of the call becomes identifiable as well.
- **Legal significance:** STIR SHAKEN digital signatures provide non-repudiation. Who signed a call cannot falsely deny being the entity where the call entered the governed ecosystem. This digital signature is a powerful measure that has a legal basis in most of the jurisdictions and is often used a proof in a court of law.
- **Quick exclusion of entities who behave badly:** the STIR SHAKEN ecosystem provides the capability to quickly excludes misbehaving entities from the acceptance by no longer accepting calls linked to their certificates.

# 5. CLI spoofing risk analysis

## 5.1. Introduction

The Caller ID (CLI) is an identifier associated with the caller's phone number and this identifier as part of a telephone service allows the callee to see the caller's number. But this caller ID is subject to spoofing.

This means that the callee is deceived, as he is led to believe that he is called by one user rather than another. This technique of telephone fraud is widely used, causing considerable damage not only for end-users but also for telecom operators.

While spoofing CLI attacks were difficult to implement on traditional circuit switching networks, the proliferation of smartphones and VoIP and an easy access to spoofing CLI applications (there are many dedicated websites and applications, such as Spoofcard and Spooftel) allowed an average telephone subscriber to organize such attacks, with losses of billions of dollars.

Caller ID has been increasingly used to authenticate the identities of callers, or to verify their physical locations in several systems, automatic telephone banking systems, credit card activation systems, to voicemail services. Unfortunately, existing caller ID protocols do not provide real authentication and hence are untrustworthy for authenticating callers' locations or identities, because caller IDs are vulnerable to spoofing attacks [1].

Caller ID spoofing is possible because caller IDs are transmitted in plaintext with no authentication mechanisms in place. When a call is routed between different carriers, the callee's carrier will simply accept the caller ID claimed by a caller's carrier.

This happens because the entire telephone infrastructure comprises several telephone carriers with their own trusted domains, and a carrier can at most verify calls originated in its own network but not from other networks.

In addition, many VoIP carriers allow their customers to specify their own caller ID and will forward the caller ID to the callee's carrier without modifications. But an adversary can subscribe to a VoIP carrier that allows caller ID manipulation and can either use VoIP client software or a VoIP phone to claim arbitrary caller IDs.

## 5.2. Fraud Types

CLI spoofing is a malicious action that causes any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud or cause harm. This typically refers to fraud types like:

- WANGIRI
- SCAM CALLS
- ROBOCALLING
- OBC SPOOFING
- VM BRUTE FORCE
- CALL BOMBING
- BYPASS FRAUD

Please note these fraud types may be initiated either by legal service providers or by fraudsters using CLI spoofing attacks:

- Attack initiated by a legal service provider – then there is no CLI spoofing involved and as a result the CLI Spoofing solution will provide evidence that the fraudulent calls were originated by the participating entity. In such situations the CLI validation solutions will not be able to detect such fraudulent calls because the CLI is not being manipulated.

- Attack initiated by fraudsters using CLI spoofing technique – then the system will mark these calls as fraudulent ones, like “calls with unconfirmed origin” – and if the terminating provider switches on the blocking option for this type of fraud – the system will block the attack. In such cases the CLI validation fails either by an authentication failure of token with the signed CLI or the by a mismatch between the CLI received with the call and the CLI sent in parallel via an out-of-band side-path.

NOTE: More specific details about these and other fraud types considered relevant for wholesale carriers can be found in the i3forum Fraud Classification document [2]

### 5.2.1. WANGIRI

Short calls or faked missed call notification SMS messages are generated with the purpose of leaving a missed call notification on the display of customers' handsets thus prompting them to call back.
This technique is also defined as "ping call" where ping in computer jargon indicates the sending of a data which should be followed by a response by measuring the elapsed time; in this case the objective is not to calculate the response time but to obtain the response itself, which the impostor obtains either by the distraction of the victim or by the fear of the victim who thinks he has lost a business call or simply by misinformation, not knowing about this possible type of fraud. The number displayed on the callee phone is in most cases an international premium rate number and the call-back ensures financial benefit for the fraudsters.

### 5.2.2. SCAM CALL

These are calls made by scammers who claim to work for a trusted company, but it is a scam; during the call they attempt to obtain personal information, ask to access their computer or require bank details, for obtaining money or committing identity theft (phishing). The scammer may also have a fake name or number displayed on the UE of the called, to gain his trust.

### 5.2.3. ROBOCALLING

Robocall is a telephone call where the users hear a recorded message and not a living person, which often sounds as if it was a robot. Robocalls can be legal, such as those related to political or telemarketing phone campaigns, but increasingly they are used by scammers, with the aim of obtaining financial benefit or personal information about victims. Scammers can use an auto dialer that can broadcast millions of calls within hours. Robocalls are cheap and especially difficult to track, because scammers use the spoofing caller-ID so that when a person tries to call the robo caller, he gets a disconnected number or something other than the original call source.

NOTE: The FTC rules in the US (and by similar regulations in other countries) differentiate between unwanted robocalls (also identified as nuisance calls or scams) and friendly robocalls. Friendly robocalls don’t require permission and typically include:

- Informational calls like your flight being cancelled or reminding you about an appointment.
- Calls from health care providers like a pharmacy reminding you to refill a prescription.
- Political calls as well as calls to members of a charity or prior donors.
- Calls from official and governmental agencies announcing situations of general interest (e.g. Weather conditions, etc.).

### 5.2.4. OBC SPOOFING

Telephony revenues have steadily declined over the years worldwide. With increasing competition, subscriber rates have gone down and are still falling, which results in a consequent drop in interconnection prices. Over the past 10 years, the significant increase in data transmission and the advent of OTT players have led to a further decline in the voice business. In addition, regulators in various countries are driving the reduction termination rates for the use of interconnection, which leads to a further reduction in margins. European legislation has imposed a lower termination rate for calls originated within EU. As a result, European carriers have created a paid model for fixed and mobile voice calls based on origin: the Origin Based Charging (OBC) principle or OBR (Origin Based Rating).

The OBC principle was created in Europe around 2015, to bridge the price difference between calls terminating in the EU region and calls from the EU to the rest of the world. Initially, the call origin groups were mainly non-European countries, which eventually led to the application of CLI (Caller Line Identification) techniques to be so isolated. The prices are changing too often to keep track of them. For different reasons (commercial, technical, …) not all new prices established by an operator are adopted by customers, resulting in price difference, incorrect billing and long-standing disputes.

More and more CLI spoofing and masking fraud has started to occur in order to benefit from lower rates. Since the price is based on origin, an increasing percentage of call networks without CLI has started to be forwarded, resulting in extra costs for the network forwarding the call without CLI. The target cost could be either very high, making the operator uncompetitive, or very low, allowing fraudulent calls to take advantage of these prices (arbitrage). By identifying this trend, operators internally began to detect and identify the various cases of No CLI and Invalid CLI calls, as the detection of fraud for interconnection carriers has become a necessity to avoid financial abuse.

Please be referred also to section 6.5.9 that clarifies how the STIR/SHAKEN and alike CLI protection solutions may assist to tackle inter-carrier fraud via OBC spoofing.

#### 5.2.5. VM BRUTE FORCE

Most voicemail systems will limit the number of failed passcode attempts a given caller number can make before terminating the call. However, many of them will continue to allow new caller numbers to connect and make new attempts. A brute force mechanism uses CLI spoofing to change the caller id with every attempt, trying a new combination with every call. Given the relatively small surface area of voicemail passcode options (4-6 numeric digits), this mechanism can be extremely effective.

#### 5.2.6. CALL BOMBING

Technology increasingly facilitates interpersonal attacks such as stalking, abuse, and other forms of harassment. One prominent example is in intimate partner violence (IPV), where victims report abusers utilizing apps for a range of harms, including text message “bombing” (sending hundreds or thousands of messages), spoofing phone numbers to hide the source of harassment, creating fake suggestive images to hurt a victim’s reputation, and installing spyware apps on victim devices.

These applications can also be used in combination with other types of fraud for the purpose of obtaining money or information about victims to defraud them. For example, call bombing can be used in combination with WANGIRI, to send hundreds of calls to different victims reaching their purpose in the shortest time and with the least effort.

#### 5.2.7. BYPASS FRAUD

This refers to using different call termination techniques, such as SIM boxes and hacked PBXs, to bypass the interconnection of legal calls and divert international incoming calls to avoid revenues for international call termination that operators and government agencies are entitled to.

Bypass fraud generally occurs in countries where there is a significant difference between national retail calling rates / national interconnection rates and international terminating rates, either determined by the regulator in the country or determined by a group of operators. It is also popular in countries where international gateways are government monopolized.

Please be referred also to section 6.5.9 that clarifies how the STIR/SHAKEN and alike CLI protection solutions may assist to tackle inter-carrier bypass fraud via SIM boxes and hacked PBXs.

# 6. Supporting mechanisms and solution alternatives

## 6.1. Introduction

There are different supporting mechanisms and solution alternatives for the protection and prevention of CLI spoofing. The approaches fall into two different categories, the solutions for Call Validation versus the solutions for Call Fraud Detection, as depicted in Figure 2.

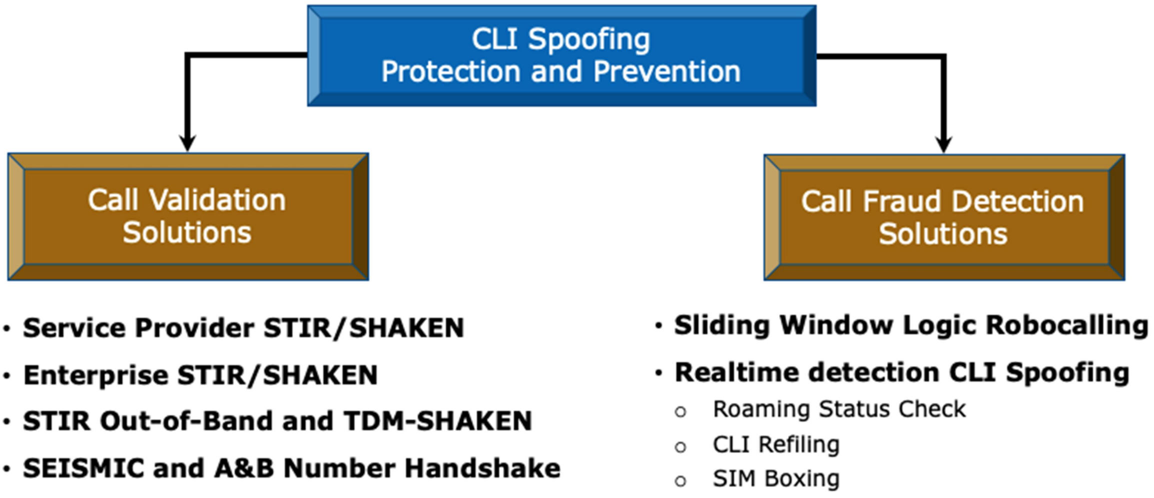

CLI Spoofing
Protection and Prevention
Call Validation Solutions
Call Fraud Detection Solutions
Service Provider STIR/SHAKEN
Enterprise STIR/SHAKEN
STIR Out-of-Band and TDM-SHAKEN
SEISMIC and A&B Number Handshake
Sliding Window Logic Robocalling
Realtime detection CLI Spoofing
Roaming Status Check
CLI Refiling
SIM Boxing

**Figure 2 – Overview of Protection and Prevention Solutions for CLI Spoofing**

The following sections provide more details of these two alternative approaches and some specifics of these solutions.

NOTE Although this report is focused on fraud aspects related to voice service and not messaging, the technical solutions may also be extended to deal with CLI spoofing applied to SMS and RCS.

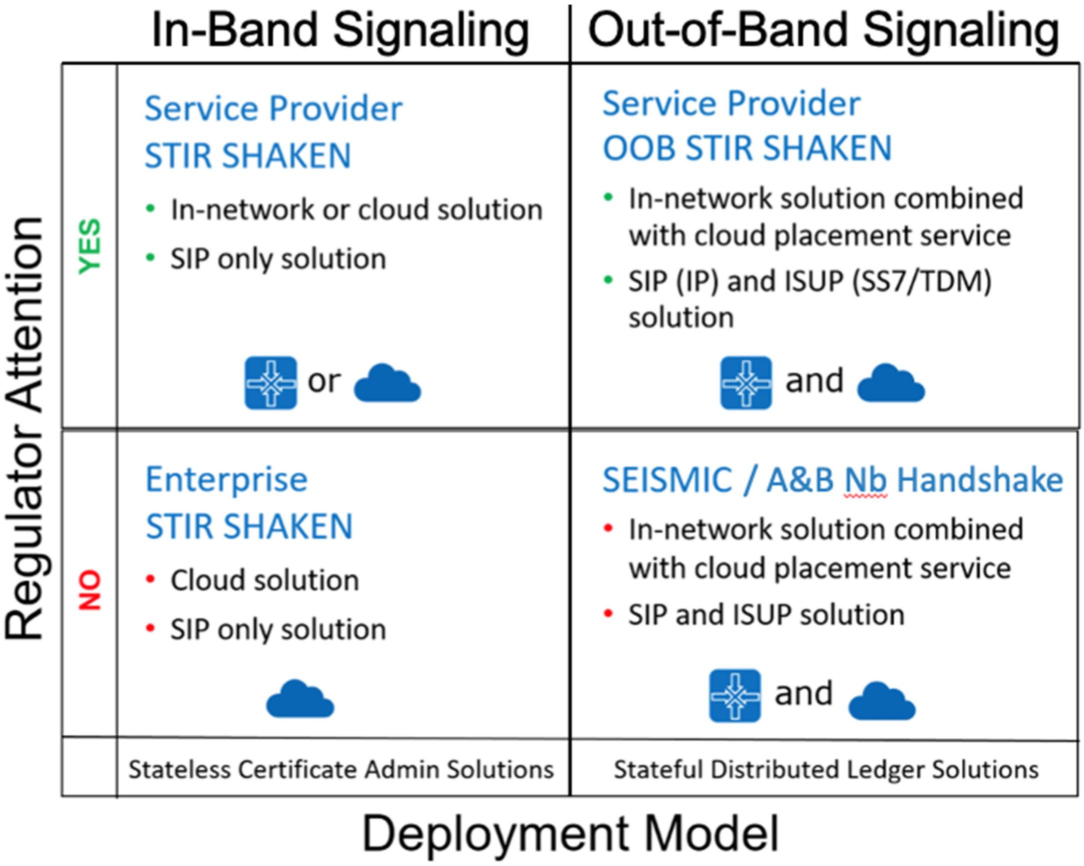
## 6.2. Call Validation Solutions

Given the need to identify and block unwanted robocalls and fraudulent calls, the Internet Engineering Task Force (IETF) defined a technology to combat unwanted robocalling: Secure Telephone Identity Revisited (STIR). Meanwhile, the Alliance for Telecommunications Industry Solutions (ATIS) and the SIP Forum joined efforts to define an industry framework for implementation of the STIR protocols: Signature-based Handling of Asserted information using toKENs (SHAKEN). Together, STIR/SHAKEN solutions are recommended to carriers and operators as a potential solution to widespread telecommunications abuses.

In parallel, leading European mobile operator groups started an anti-fraud initiative in the GSM Association (GSMA). Globally mobile operators face growing revenue losses due to various inter-network fraud types like SIM Boxing and CLI Refiling. This so-called initiative Stopping Exploitation Inter-Network Signal Fraud by Mitigating Illegitimate Communications (SEISMIC) intends to provide in real-time the terminating mobile operator with validated call set-up information via parallel secure end-to-end connections. With SEISMIC intermediate carriers will lose the ability to manipulate and intervene call setup actions to commit the various inter-network fraud types.

NOTE: To discourage such inter-network fraud types, anonymization of the A-number and/or B-number may be considered with SEISMIC and alike solutions. However, such anonymization will impact heavily and jeopardize the regular business activities and functions of international wholesale carriers. This is discussed in more detail in section 6.5.8.

It is important to consider the complete set of solutions and their mutual cohesion and inter-operability to avoid that the CLI spoofing protection solutions cannot be by-passed. The variety of Call Validation Solutions can be positioned in four different quadrants as illustrated in Figure 3.



In-Band Signaling | Out-of-Band Signaling

Regulator Attention

YES

Service Provider STIR SHAKEN
- In-network or cloud solution
- SIP only solution

or

Service Provider OOB STIR SHAKEN
- In-network solution combined with cloud placement service
- SIP (IP) and ISUP (SS7/TDM) solution

and

NO

Enterprise STIR SHAKEN
- Cloud solution
- SIP only solution

SEISMIC / A&B Nb Handshake
- In-network solution combined with cloud placement service
- SIP and ISUP solution

and

Stateless Certificate Admin Solutions | Stateful Distributed Ledger Solutions

Deployment Model

**Figure 3 – Overview of Call Validation Solutions**

The four quadrants in the overview can be grouped in the following two categories:

- **Regulatory Attention:** The top half of Figure 3 shows the two quadrants that are intended to protect subscribers with solutions that national regulatory bodies demand service providers to implement. The lower two quadrants are business driven (enterprise market and carrier market) solutions, and it is left to the industry to decide to what extent these solutions are implemented.
- **Deployment Model:** The “Stateless Certificate Admin Solutions” quadrants on the left of Figure 3 refer to the STIR/SHAKEN solutions in which the CLI is signed based on certificates administered centrally in a trust relationship between actors. For these solutions there is no need to memorize any call information in the network. The “Stateful Distributed Ledger Solutions” quadrants offer an alternative manner in which CLI signing information is exchanged on a bilateral trust basis. With these information needs to be memorized in a call placement service as no signing information is received as part of the call setup messages.

The following sections provide a brief description of each solution and its working principles.

## 6.3. In-Band Signaling Call Validation Solutions

### 6.3.1. Background

This category refers to the solutions where information is supported as integral part of the call set-up information by means of a specific field or indication. In the past, solutions were developed that over time proved not working effective like:

- In C7/SS7 ISUP the indication "network verified and passed" is typically included within the Calling Party Number parameter when the originating switch has checked or included the CLI that is associated with the line or mobile user. However, this guarantee cannot be trusted if a call is received via a network trunk or if the received CLI cannot be verified.

- As a result, bad actors have learned techniques to issue calls that are transferred via C7/SS7 ISUP whereby the origin of the CLI cannot be verified.

- In SIP the same CLI identification problem has evolved over time. Although the P-Asserted-ID header was introduced to have a trustable network generated CLI next to the user generated CLI in the FROM header, fraudsters have learned techniques to issue calls that are transferred via the SIP signaling whereby the origin of the P-Asserted-ID header cannot be verified. This typically happens if a call is received via interworking situations from C7/SS7 ISUP to SIP.

STIR/SHAKEN is specified as In-Band signaling solution for the SIP protocol to solve this call validation problem by adding signing information that authenticates the CLI in the SIP signaling messages by what the terminating service provider can validate the received CLI before presenting the call to the callee. No solution is specified for C7/SS7 ISUP given the retrofitting issues with this legacy signaling protocol.

### 6.3.2. Service Provider STIR/SHAKEN

The service provider's STIR/SHAKEN solutions refer to the implementations in the SIP core networks of the all service providers in the USA, Canada and similar networks in other countries. The following simple diagram in Figure 4 illustrates the working principle of such STIR/SHAKEN solution. During call setup, the originating service provider of Alice (caller) is adding passport information to the CLI of Alice in the Identity Protected SIP INVITE message in the SIP signaling.

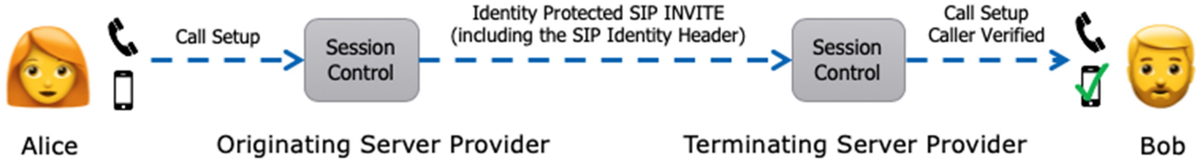

Call Setup
Session Control
Identity Protected SIP INVITE (including the SIP Identity Header)
Session Control
Call Setup Caller Verified
Alice
Originating Server Provider
Terminating Server Provider
Bob

**Figure 4 – Signing the CLI in the SIP INVITE with STIR/SHAKEN**

This enables the service providers of Alice and Bob to perform the following actions:

a. If Alice's landline or mobile is under direct control of the originating service provider, then Alice's CLI can be guaranteed. In SIP the attestation of the passport information indicates "A = Full Attestation" by which the validity of the calling number is authenticated, and the terminating service provider can inform Bob that the CLI is trusted.

b. If Alice makes a call from a phone in an enterprise PBX network, for example, then the service provider may validate the call is incoming on the trunk with the enterprise network, but it cannot validate if the CLI is associated with the phone that Alice uses. Then the passport indicates "B = Partial Attestation" which means that the validity of the CLI is partially authenticated. The terminating service provider can then inform Bob about the partial validity of the CLI.

c. If the CLI of Alice's call is received with attestation level "C = Gateway Attestation" then the terminating service provider informs Bob that the CLI is not verifiable. This applies to situations in which Alice makes a call on a network not supporting STIR/SHAKEN, or Alice is travelling abroad, and her call arrives via a foreign network.

STIR/SHAKEN enables a recipient of a call to know that the identity of the calling party is accurate. This helps to eliminate fraudulent robocalls as it provides confidence that Alice actually originated the call, not someone pretending to be Alice.

The main objective of the STIR/SHAKEN concept is to avoid manipulation of the CLI to confuse the called party or mislead billing. In the example in Figure 4, signing of the CLI only works if the SIP signaling protocol is supported end-to-end by the networks between Alice (the caller) and Bob (the person called). In other situations, an alternative but comparable solution will be to call authentication if SIP is not available end-to-end.

### 6.3.3. Enterprise STIR/SHAKEN

Because people in the USA and Canada increasingly ignore incoming unidentified calls due to the large number of robocalls, enterprises face declining success rates in reaching customers. With STIR/SHAKEN, this issue worsens as the enterprise calls are labeled with either attestation level “B”, meaning that the validity of the CLI is partially authenticated, or attestation level “C”, by which the call will be presented to Bob with the indication “Caller Unverified”, as explained in more detail before.

This problem is solved with Enterprise STIR/SHAKEN, whereby the enterprise calls are given signatures that the originating service provider agreed upon and can use to verify the authentication of the sending enterprise network. Then, the CLI of the call can proceed in SIP with attestation indication “A”, making the CLI fully trusted.

NOTE: Enterprise STIR/SHAKEN includes a per call verification of the CLI and then the call can be offered with a signed CLI in SIP in order to allow the originating SP to validate the CLI before resigning the call with a public signed CLI and with attestation value “A”.

This is different from the trunk based signing, including wholesale carrier trunk situations like SIP-T, OTT generated traffic (voice or SMS) and cloudcom SP generated traffic, whereby the incoming trunk can be validated but not the CLI of each and every individual call. Then the CLI of such calls will be signed with attestation value “B”.

## 6.4. Complexities with Service Provider STIR/SHAKEN

The implementation of STIR/SHAKEN needs the implementation of the signing of the calls in the network elements as well as a parallel infrastructure for the exchange of certificates that represent the tokens used for the cryptographic signing process. This is a complex and costly matter for implementing the network elements required for the signature of the calls.

In addition, not all service provider networks are created equal, and some do not yet support SIP. Many telecom services are delivered via legacy C7/SS7/TDM systems or the services cross networks not controlled by the SIP protocol, and the networks of enterprises may also use this non-SIP eco-system. Also, CLI validation requires global interworking between SIP-enabled systems and the CLI signing solutions in service provider networks across multiple countries.

As a result, it may take some time until a critical level is reached with enough service providers adhering to STIR/SHAKEN.

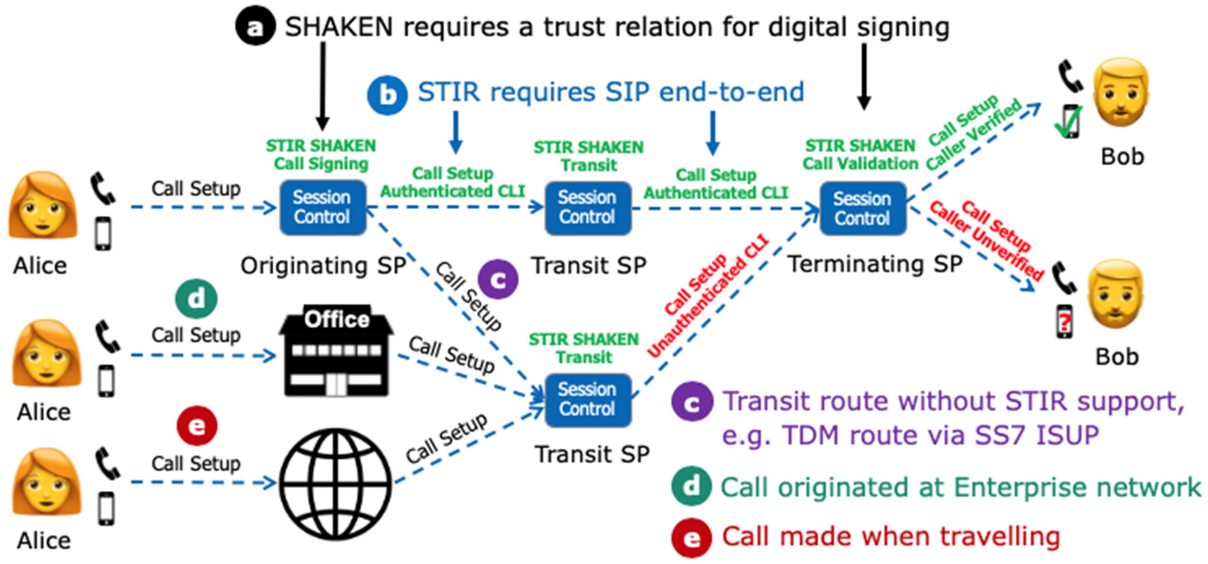

a SHAKEN requires a trust relation for digital signing
b STIR requires SIP end-to-end
STIR SHAKEN Call Signing
Call Setup Authenticated CLI
STIR SHAKEN Transit
Call Setup Authenticated CLI
STIR SHAKEN Call Validation
Call Setup Caller Verified
Bob
Alice
Call Setup
Session Control
Session Control
Session Control
Originating SP
Transit SP
Terminating SP
Call Setup Caller Unverified
Bob
c
Call Setup
d
Call Setup
Office
Call Setup
Alice
STIR SHAKEN Transit
Session Control
Call Setup Unauthenticated CLI
e
Call Setup
Call Setup
Transit SP
Alice
c Transit route without STIR support, e.g. TDM route via SS7 ISUP
d Call originated at Enterprise network
e Call made when travelling

**Figure 5 – Complexities with the working of STIR/SHAKEN**

Figure 5 shows the typical complexities that are present with the working of STIR/SHAKEN:

a. **SHAKEN requires a trust relation for digital signing**
The protection of the Call Setup requires that the terminating service provider can trust the digital signature added by the originating service provider. This involves a key retrieval as directed by the signature in each call whereby the central SHAKEN certificate management infrastructure is not involved in the real-time key exchange.

b. **STIR requires SIP end-to-end**
The additional passport information in the identity protected SIP INVITE message is only specified for the SIP protocol and requires support end-to-end including support by intermediate nodes. In non-SIP scenarios the implementation of alternative solutions like Out-of-Band (aka side path) SHAKEN may be required, see for further details section 6.5.

c. **Transit route without STIR support, e.g. TDM route via C7/SS7 ISUP**
When calls are routed via network parts without STIR support of the SIP protocol, then the call will proceed without the additional passport information. As a consequence, this information will be missing on receipt of the call setup by the terminating service provider. Hence, the call will be offered to Bob with the indication “Caller Unverified”.

d. **Call originated at Enterprise network**
If originating service providers receive calls from enterprise networks without passport information via intermediate carriers, then the individual CLI information cannot be authenticated. As a result, the terminating service provider will present the call to Bob with the indication “Caller Unverified”. SHAKEN standards body is evaluating a variety of scalable techniques to support A attestation for these enterprise scenarios.

e. **Call made when travelling**
When making calls during travelling, the serving network may not be in a position to authenticate the CLI of the caller and existing STIR/SHAKEN solutions don’t work internationally. As a result, the terminating service provider will present the call to Bob with the indication “Caller Unverified”.

The next sections outline the mitigation call validation solutions for the above mentioned issues c, d and e.

## 6.5. Out-of-Band Signaling Call Validation Solutions

### 6.5.1. Background

This category refers to call validation solutions whereby call details are transferred in a secure manner via a side-path (i.e. out-of-band) in parallel to the call set-up signaling information transferred in the SIP protocol or the C7/SS7 ISUP protocol or alike. The information transfer via the side-path is either to provide an alternative call validation mechanism to STIR/SHAKEN or to overcome the risk that the PASSport information is lost due to reasons like:

- Not all call segments in today's telecom networks are controlled by SIP like the TDM route c in Figure 5. Legacy network technology is still widely used, and the STIR/SHAKEN information will be lost when reaching one of these segments.

- SIP implementation may remove the identity token from the SIP header either because the SIP implementation needs to be upgraded of by filtering actions on the network edge to normalize or secure the information transfer via the SIP signaling.

- Some SIP networks use the UDP layer in the IP protocol stack instead of the TCP layer. Since UDP doesn't provide flow control and retransmission, packet fragmentation and packet loss is a serious problem with UDP by what the identity token may be lost or corrupted through what the call can no longer be verified by the STIR/SHAKEN call validation server.

Although telecom networks are gradually evolving toward SIP, and the total replacement of all remaining legacy technology is costly, complex and a multi-year undertaking to complete. Such a long delay does not meet the legal requirements in the US and Canada for alleviating nuisance and scam calls with the implementation of STIR / SHAKEN via end-to-end SIP support.

A similar inter-operator interworking problem applies to the handling of international calls. When arriving in a STIR/SHAKEN domain the validity of the call cannot be determined, so the call will be given the level "C = Gateway Attestation" by the ingress node of the transit service provider. As a result, the call will be presented to Bob with the indication "Caller Unverified".

Solutions for the treatment of international calls are still under consideration. Figure 6 shows a possible mitigation if the sending foreign operator is able to authenticate the CLI and is given a signing certificate by the either the certificate repository or the transit operator in the recipient STIR/SHAKEN domain.

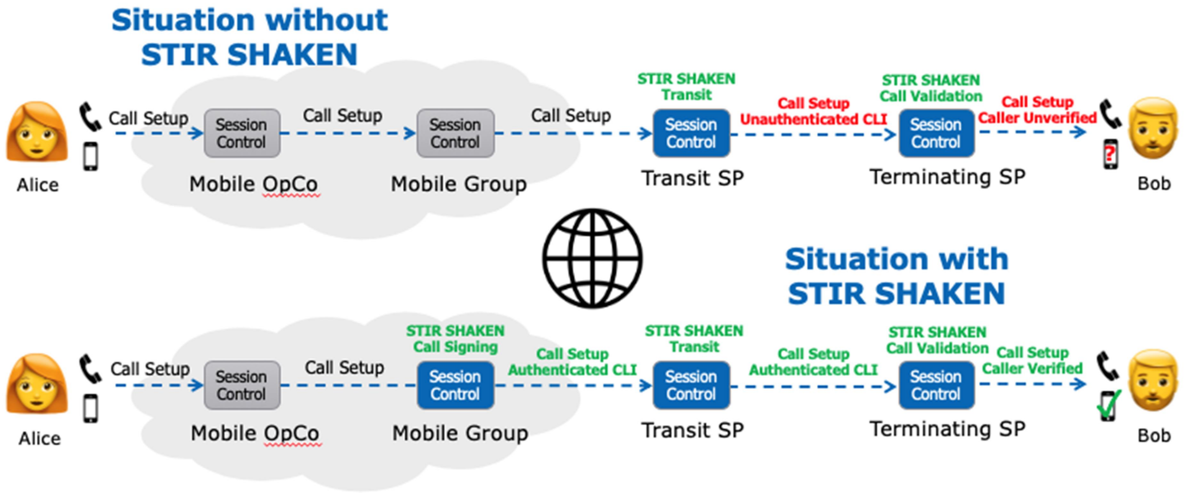


**Figure 6 – Handling of international calls without and with STIR/SHAKEN**

Hence, the compelling advantages are offered with using the out-of-band authentication methods:

- It does not matter what kind of network segments (IP and/or TDM) are used to route the call.
- There are no concerns about whether any of the network equipment or software along the call path by which the STIR authentication information in SIP is lost.
- There are no problems with tokens being corrupted by packet loss or fragmentation.
- Since the identity tokens are secured, there are no security or privacy concerns since the tokens can only be read by the terminating service provider and are of no value to intermediate actors.
- The same SHAKEN infrastructure can equally and seamlessly be applied for the OOB SHAKEN solutions as being used for STIR/SHAKEN.

With regard to the implementation costs of STIR/SHAKEN deployments for international carriers (see item 8 in the evaluation table in section 7), various approaches may be envisaged like:

- **Low** – For pure wholesaler deployments the minimum will be to transit already labeled calls as low-cost CAPEX or no cost at all solution. This would presume that the originating operator is enabled for signing the call that can be validated by the terminating operator. This would imply that there is a trusted relationship between originating operator and terminating operator with any involvement of the international carrier in this STIR/SHAKEN signing and validation process except for transiting the signing information with the CLI.

- **Medium** – A somewhat more expensive investment would imply an active role of the international carrier in the STIR/SHAKEN signing and validation process between originating operator and terminating operator like verification of the received CLI signed information and possibly resigning of the CLI to interwork between the STIR/SHAKEN domain with the originating operator and the STIR/SHAKEN domain with the terminating operator.

- **High** – A comprehensive investment would apply if the originating operator outsources the STIR/SHAKEN signing process to its international carrier(s) and similarly, if the terminating operator outsources the STIR/SHAKEN validation process to its international carrier(s). This would imply more service logic and processes to be supported by the international carrier for providing such hosting STIR/SHAKEN service deployment services.

  NOTE: One risk associated to a low investment approach is creating a perception that the international carrier is a non-participant in the CLI verification process. Similar to legacy positioning with regard to CLI 'we just pass along what we receive' this could be viewed by the broader industry as not doing enough to combat CLI spoofing and associated frauds. In addition, it will be more difficult to investigate cases of CLI spoofing and manipulations (or defend one own's handling of CLI) without having access to the secured signing information of labeled calls.

The subsequent sections outline different solution variants for out-of-band call validation.

### 6.5.2. Call Placement Service (CPS)

The CPS function is an essential element as part the Out-of-Band Signaling Validation Solutions for the storage and exchange of call details via a side-path solution. There are various manners how this CPS function can be implemented and organized:

- **STIR/SHAKEN –** In countries like the USA and Canada with a STIR/SHAKEN infrastructure, the working of the CPS function is documented in IETF and ATIS standards as described in section 6.5.3:
  - The CPS function in the IETF standard "STIR Out-of-Band Architecture and Use Cases" [6] is working as an extension of the SHAKEN key management infrastructure

introducing significant complexities for new entrants and the standards body is still working on a scalable approach.

- A simple private CPS implementation is documented in the ATIS standard "Signature-Based Handling of Asserted Information Using Tokens (SHAKEN) For TDM Networks (TDM-SHAKEN)" [7].

- **SEISMIC –** As outlined in section 6.5.4, SEISMIC is typically foreseen as a distributed ledger infrastructure for inter-network deployment based on open web standards for Solid [4] with individual Solid pods per service provider. These Solid pods can e.g. be accessed with TLS sessions via the existing IPX network and addressed with FQDN types like "cps.mcc204.mnc08.3gppnetwork.org".

- **Coordination Organization –** As part of the proprietary A&B Number Handshake solution described in section 6.5.5, the exchange of E.164 number ranges and IP addresses via the coordination organization.

- **Existing SS7 Infrastructure –** Re-use of procedures used in regular roaming situations as part of the SS7 CVS call validation solution [3] as referenced in section 6.5.7.

### 6.5.3. Service Provider Out-of-Band STIR/SHAKEN

Service provider out-of-band (OOB) STIR/SHAKEN adds a parallel infrastructure to enable the transfer of the signature information for network instances where the transfer of passport information via SIP (IP) cannot be guaranteed end-to-end or where the SIP protocol is not supported. The latter typically applies to existing PSTN networks with C7/SS7 ISUP trunks that are likely to remain in service for quite some time before SIP-only networks fully replace them.

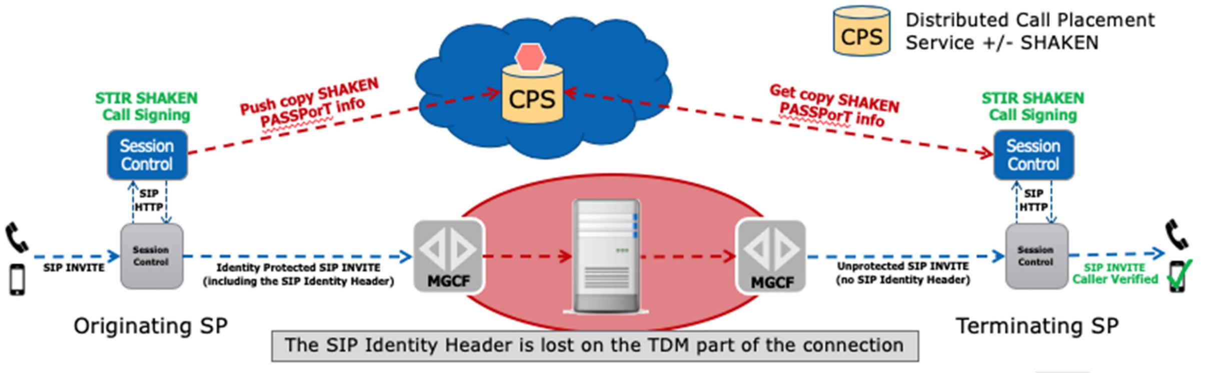

CPS
Distributed Call Placement Service +/- SHAKEN
STIR SHAKEN Call Signing
Push copy SHAKEN PASSPorT info
CPS
Get copy SHAKEN PASSPorT info
STIR SHAKEN Call Signing
Session Control
Session Control
SIP HTTP
SIP HTTP
SIP INVITE
Session Control
Identity Protected SIP INVITE (including the SIP Identity Header)
MGCF
MGCF
Unprotected SIP INVITE (no SIP Identity Header)
Session Control
SIP INVITE Caller Verified
Originating SP
Terminating SP
The SIP Identity Header is lost on the TDM part of the connection

**Figure 7 – Working principle of OOB STIR/SHAKEN**

Figure 7 sketches the working of OOB STIR/SHAKEN in the situation where the call, started via the SIP signaling, is routed via a transit TDM (C7/SS7 ISUP) network whereby the signed information of the SIP Identity Header is lost. The parallel path ensures that a copy of the SHAKEN passport information can be retrieved via a distributed Call Placement Service (CPS) by the terminating service provider. With this addition Bob (the called party) can still see the CLI of Alice (the calling party) with the indication "Caller Verified".

NOTE: There are several models under development for the operations of such CPS infrastructures like proprietary offerings and the definition of standardized frameworks in GSMA and ATIS.

Other scenarios (not visualized in Figure 7) may include network parts at the originating service provider side and/or terminating service provider side not supporting the in-band transfer of the signature information via SIP (IP).

In case there is no entry found in CPS or in case of disruption, calls can proceed although CLIs of such calls cannot be validated by the terminating service provider and the CLIs will be presented to the callees accordingly.

Since the information exchange via CPS is only for the transfer of the SHAKEN PASSPorT info, there is no added value here for the Trouble Ticketing (TT) operational care processes.

Detailed solution descriptions can be found in the following IETF and ATIS standards:

- **IETF standard "STIR Out-of-Band Architecture and Use Cases" [6]**

  This concept is based on the STIR/SHAKEN setup whereby the CPS has a public interface for sending and receiving PASSporTs. Anyone can send PASSporTs to the CPS using an HTTP POST, and anyone can retrieve PASSporTs from the CPS using an HTTP GET. This is why the OSP encrypts the PASSporT using the TSP's public key. The TSP then uses their private key to decrypt the PASSporT. Therefore, only the TSP can read the PASSporTs. However, this introduces the following complexities that makes the solution overly expensive, more time consuming, extra labor intensive and failure prone like:

  - Encryption is a delicate and cumbersome process needing an additional process for the exchange and regular update of keys among all carriers.
  - As the signing process needs the TSP's public key for encryption, before sending the call the OSP needs to know the TSP including LNP correction.
  - If calls are becoming forwarded, the CLI cannot be validated because the TSP is unable to read the PASSporT of the diverted call as the TSP does not have access to the private key of the SP that forwarded the call.

- **ATIS standard "Signature-Based Handling of Asserted Information Using Tokens (SHAKEN) For TDM Networks (TDM-SHAKEN)" [7]**

  TDM-SHAKEN simplifies the CPS implementation model without the encryption complexities by use of a private CPS accessed only by approved community members to lower the cost for implementation, shortening the time for introduction and limiting the operational effort.

### 6.5.4. Stopping Exploitation Inter-Network Signal Fraud by Mitigating Illegitimate Communications (SEISMIC)

SEISMIC refers to an initiative within the GSMA that aims to eliminate various fraud types between operators on their interconnections. It provides a distributed global infrastructure for secured end-to-end delivery of validated call set-up information in real-time. SEISMIC makes sure that the terminating mobile operator can detect fraudulent incoming calls and decide to let the call proceed, block the call, and determine any further actions for the call.

The following Figure 8 shows a possible implementation of SEISMIC whereby the original B-number is replaced by a SEISMIC Routing Number (SRN) for routing the call to the terminating service provider. The SRN routing is similar as the existing practices routing calls to roaming mobile users.

NOTE: The use a specific routing number ensures that most popular inter-network fraud types like IRSF shortstopping and SIM Box are not possible anymore because the actual premium number or destination is not visible during the routing process. However, the same SEISMIC concept can also be deployed by keeping the B-number untouched to simplify the implementation effort and avoiding any impact with existing IPX services.

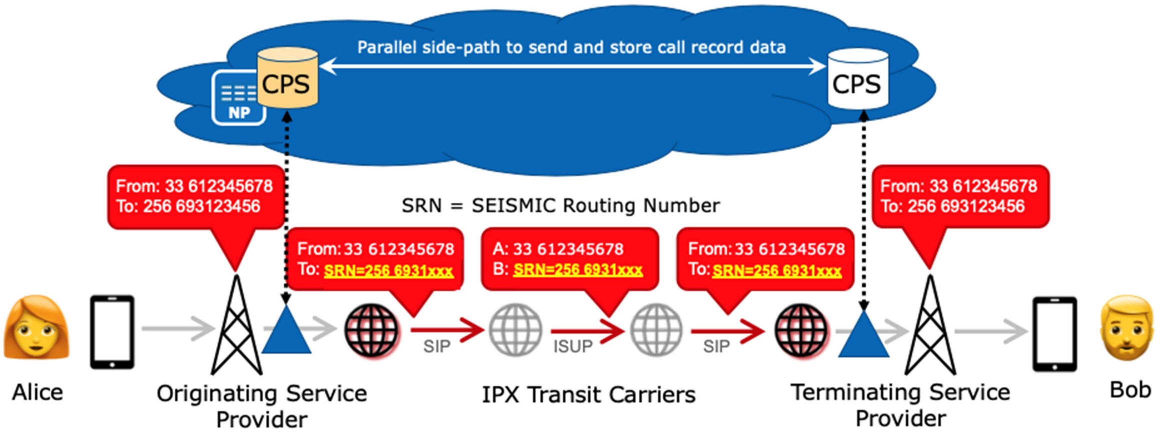


**Figure 8 – Potential working principle of SEISMIC**

The schema above shows the workflow whereby the received B-number is temporarily replaced by the SRN (SEISMIC Routing Number) for the routing of the call between originating service provider and terminating service provider. This is following the same MSRN (Mobile Subscriber Routing Number) routing principle used between MNOs for the delivery of calls to roaming users abroad. The temporarily hiding of the B-number protects inter-network calls against fraud type like IRSF Shortstopping and the secured transfer of the call record data via the parallel CPS side-path provides the additional protection against SIM Boxing fraud and CLI Refiling. However, the hiding of the B-number implies that calls will fail if either the SEISMIC service is interrupted, or calls are erroneously delivered to networks not supporting SEISMIC.

A lightweight deployment mode of SEISMIC would by routing on the B-number, thus no use of the SRN. Then incoming calls can proceed independently of the SEISMIC call record although CLIs of such calls cannot be validated by the terminating service provider and the CLIs will be presented to the callees accordingly. However, this would make the solution somewhat less effective for the originally intended protection against inter-network fraud.

NOTE: The standardization of SEISMIC is on hold given the evaluation in the GSMA VINES group to ensure the inter-operability of the CLI Spoofing validation solutions for building a critical mass.

The SEISMIC concept complements STIR/SHAKEN on a number of its fundamental limitations:

- SEISMIC is not bound to SIP (IP) because SEISMIC works independently of the signaling type and so suited for the many C7/SS7 ISUP (TDM) networks that are still abundantly in use within national networks and for the handling of international traffic.
- SEISMIC doesn't prerequisite an end-to-end support capability via the SIP (IP) signaling as it offers the ability to interwork between SIP networks that are working with and without STIR/SHAKEN.
- SEISMIC doesn't rely on a central certificate management authority as with SHAKEN, but the trust relationship in SEISMIC works on a bilateral basis between networks via a distributed ledger making SEISMIC suitable to work between global networks that have no mutual trust relationship.
- The call record data via CPS can provide additional or an alternative working for classic CDRs and be used for Billing and Trouble Ticketing (TT) operational care processes.

### 6.5.5. A&B Number Handshake

This solution is already in use between service providers to eliminate (mitigate) the industry risks connected with international voice fraud and can also deal with SMS and RCS. The A&B Number

Handshake solution provides protection to all participants in a telco transaction: end customers, operators and carriers.

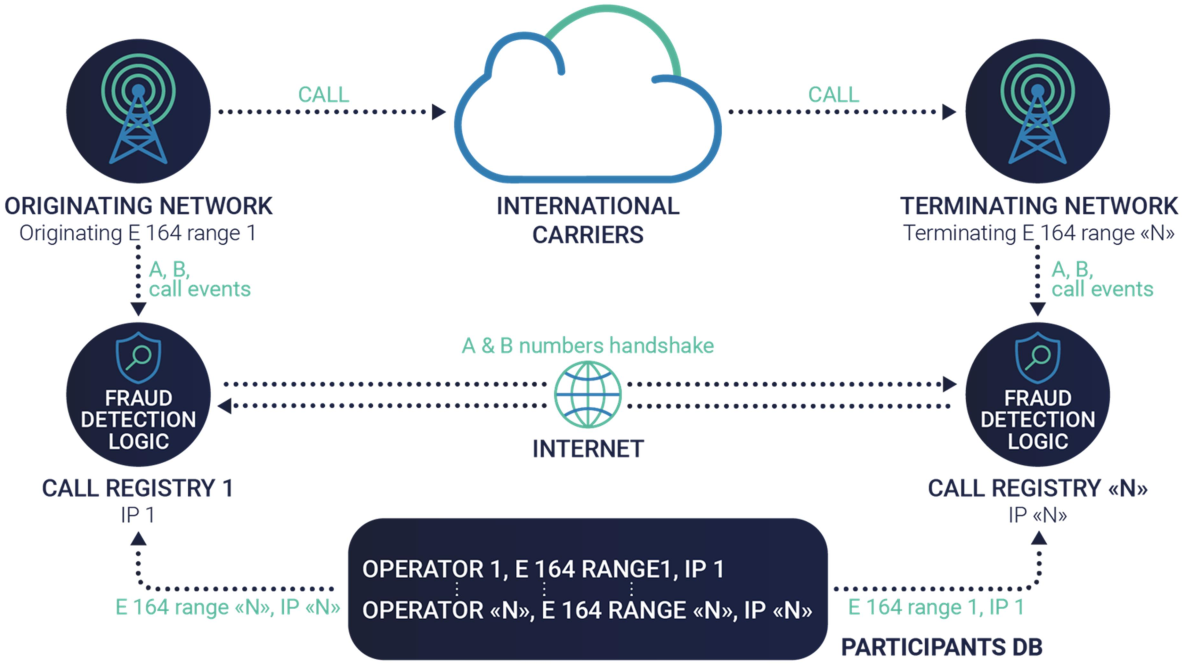


**Figure 9 – Working principle of A&B Number Handshake**

The originating operator stores the set including A-number, B-number and timestamp into his database (Call Registry Originating) when passing the outbound call to the IPX carrier. The terminating operator stores an identical set including A-number, B-number and timestamp into his database (Call Registry Terminating) on receipt of the inbound call from an IPX carrier. The call registries handshake (via the out-of-band parallel HTTP side-path) to determine the validity of the call details.

The solution requires, that before operators can participate in the system, they submit to the coordinating organization the E.164 number ranges that they operate. At the same time, they provision with the coordinating organization the IP address of the local call registry that they are operating. This information submitted by each carrier is then made available by the coordinating organization to all networks participating in the A-B Number Handshake system to facilitate routing between registries.

NOTE At this point of time these operational arrangements are coordinated by Lanck Telecom among its participating customers. Depending on the market acceptance of the solution, in future these arrangements might be coordinated via organizations like the GSMA or else.

Any enrolled entities are presumed trusted and can distribute data elements to one another through interfaces between their local registries. As the local tables distributed by the coordinating entity contain mapping between telephone numbers and the IP of registries, the tables themselves can be used to check that the proper originator of a call is provisioning a record.

A network element in the originating side may use a variety of protocols (like RADIUS, SIP and CAMEL), to provision a record at its local call registry. The registry then routes the call record to the terminating side by looking up the called party number in a local table (populated from the information distributed by the coordinating organization). When the terminating side needs to interact with the originating side, it uses its own local table to find the originating registry. These local call registries then coordinate via HTTP as call signaling events occur, providing feedback to the network on call handling.

The solution can block fraudulent calls in real time or allows for an “Alerting Mode only” working with no blockage. In the alerting mode operators will have, in real time, all necessary information to continue their activities transparently – open trouble ticket (TT), change routing, open disputes etc. But all TTs and disputes will have a documental confirmation (logs from Call Registry). ın case of multiple simultaneous calls to the same B-number, the Call Registry on the terminating side will verify each A&B number pair. The system can alert/block calls with an unverified A&B number pair. No false positives.

NOTE: The A&B Number Handshake logic allows for the call to be terminated in any case, even when the out-of-band equipment is not accessible. In such case, the operators are notified that the out-of-band equipment is not accessible and there is no verification done.

The A&B Number Handshake implies validation of call details both at the start of the call and at the end. With the “end validation” phase call stretching fraud cases can be detected. With the “start validation” false answer fraud cases can be detected.

### 6.5.6. Combination of STIR/SHAKEN and SEISMIC

SEISMIC and alike solutions provide a supplementary inter-network solution for call validation. In the context of national or regional STIR/SHAKEN domains, SEISMIC may be envisaged to offer the potential capability for bridging calls between the separate STIR/SHAKEN domains in different countries and regions. This is shown in Figure 10 and provides a similar working as Out-of-Band STIR/SHAKEN.

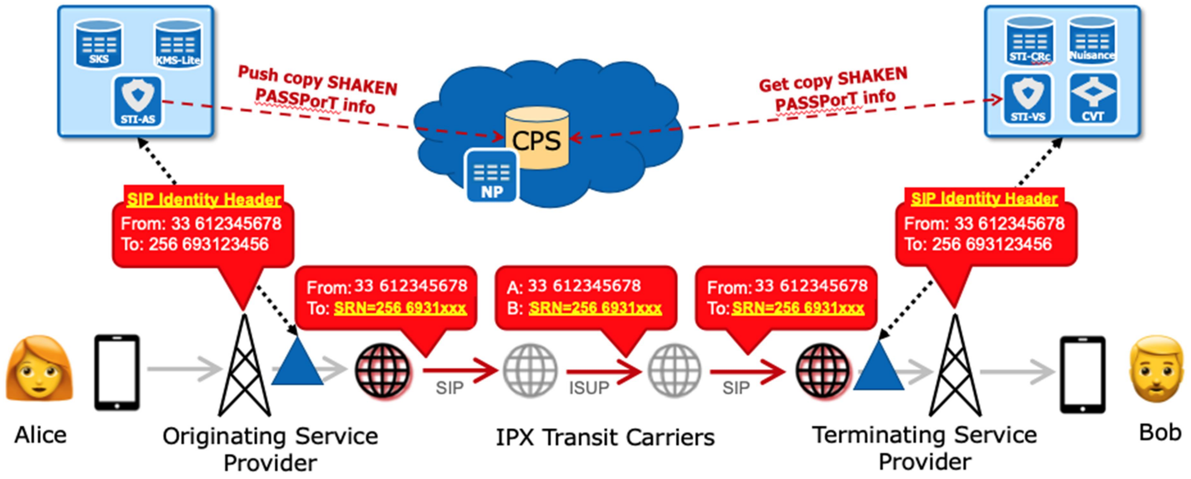


**Figure 10 – Bridging potential with SEISMIC between STIR/SHAKEN domains**

### 6.5.7. Side-Path Solution Alternatives

The OOB SHAKEN, SEISMIC and A&B Number Handshake solutions assume a side-path working on secure HTTP connections between the CPS call registries and the Solid Pods with SEISMIC (see for the Solid Specification for more details [4]), respectively, so based on today’s implementation practices with IT protocols over either the IPX intranet for data services or the open public internet.

Alternative solutions can also be envisaged like SS7 CVS call validation [3]. In this regard SS7 as complimentary technology can be used for the call validation actions considering the presence of the global SS7 infrastructure for mobile roaming and the reuse of the already SS7 roaming procedures with MAP or CAMEL:

- MAP ProvideRoamingNumber with original B-number – the existing mobile roaming procedure is used to store both the called number and calling number (CLI) in the registry in advance of the call set-up. Then the call is routed on the original B-number and the receiving operator may the double-check the call set-up details with the information stored in the registry.

- MAP ProvideRoamingNumber using routing number – the existing mobile roaming procedure is used to store both the called number and calling number (CLI) in the registry in advance of the call set-up. In addition, the terminating network returns a temporary routing number (i.e. similar as the MSRN for calls to roaming users). Then this routing number is used to route the call and the receiving operator will retrieve the original B-number and may the double-check the call set-up details with the information stored in the registry.

- CAMEL verification with InitialDP – the call is routed on the original B-number and CAMEL is used by the terminating network to verify the call set-up details stored in the registry.

However, the use of SS7 (and Diameter) introduces risks because the SS7 network is sensitive to both eavesdropping and spoofing. This will require careful consideration and comprehensive firewalling to avoid that content of the registry becomes compromised.

### 6.5.8. Impact A-number and B-number Anonymization

With these side-path solutions, implementation models can be considered whereby a temporary routing number is used for the routing of the call across the IPX domain to protect against inter-carrier fraud types like IRSF shortstopping and SIM boxing.

Some fraud types may include A-number and B-number manipulation tactics and such manipulations complicate end-to-end back tracing actions and CDR comparison checks. With the side-path methods such B-number validation helps in CLI Spoofing cases where also the B-number may be manipulated and is also evaluated in section 7 as some of the solutions take a wider approach than CLI authentication only. In this context it is recognized that one of the weaknesses of stir/shaken is that it only looks at the origination of the calls and not the termination.

Although the use of temporary routing numbers is a known practice for delivering calls to roaming mobile subscribers, see 2nd bullet in section 6.5.7 above, the anonymization of the B-number for call routing also introduces complications that need careful consideration (and resolution) as this may heavily impact the core activities of IPX providers and Wholesale Carriers as well as impacting operators running national wholesale activities:

- **Traffic Routing (Voice & SMS)**
  - Wholesale Carriers work on greater granularity than operators (to the last digit)
  - Identifying accurately the actual terminating and originating number is key to implement the right routing like:
    - The same B-number may be terminated through a different route depending on the A-number
    - Subranges are terminated through a different route
  - Troubleshooting - No details on the specific A-number and B-number involved in an event will prevent troubleshooting and it will be impossible to reproduce an event

- **DID – Cloud Number business (Voice & SMS)**
  - The allocation of DIDs (e.g. Reverse charging numbers) is done on very small ranges or even number by number
  - Each of these numbers requires thus a different route as they are allocated to different businesses like:
    - 10 numbers are allocated to Enterprise A and 10 others to Enterprise B
  - There is no repository of these allocations and these are dynamic

- **Legal Intercept**
    - This is a Legal obligation in most countries.
    - It is required that the Wholesale Carrier is able to intercept very well-defined calls, for a given A- or B-number.
- **Analytics and Machine Learning**
    - These techniques require details and granular data to be effective and efficient.
    - Analytics and Machine Learning (ML) are used in the Fraud Prevention domain but also in other business areas to improve efficiency and the service level provided to the operators like:
        - Fraud, CLI spoofing, False Answer Supervision (FAS), Origin-Based-Pricing, etc.
- **Number Portability**
    - NP is regularly updated (e.g. Hourly) → the accuracy is key and any mismatch would have a routing/financial impact on the whole chain
    - NP databases are country-wide, not specific for each and every network operator → these may not be 'sharable' outside of the country.
- **Outage of CPS infrastructure or delay in anonymization process for the termination party**
    - Failure for carriers to meet service obligations
    - Weak point that could be attacked by government actors (cyberwarfare) and organized criminals (extortion)
    - Damage to telco reputations
    - Revenue loss for all parties involved in the transaction flow
- **Trouble Ticketing**
    - Use of a temporary routing number may complicate trouble shooting as the B-number (and A-number) is quite crucial for searching
    - More complicated processes will be needed for cross-referencing between data records with the temporary routing number and with the B-number.

Similar considerations apply to the anonymization of the A-number during routing to avoid interference with MTR regulation based on A-number and need for legal intercept support for wholesale carriers.

As a result, A-number and B-number anonymization has the following consequences:

- The impact for IPX Providers / Wholesale Carriers is heavy and would jeopardize their **core activities** on different domains and well as other services provided to Operators globally
- There is also an impact for **operators running national wholesale** activities
- The need for **Number Portability** resolution is far from being easy and is not addressed in the current scheme.

#### 6.5.9. Tackling Interconnect Bypass Scenarios

Although this report focuses mostly on CLI spoofing solutions, these can help also to prevent OBC spoofing as in section 5.2.4, as well as bypass fraud via SIM boxes and hacked PBXs with fraudulent re-routing of traffic (e.g. interconnect bypass via SIM boxes and hacked PBXs) as in section 5.2.7.

- **Bypass fraud via SIM boxes**

  In such situations the incoming international call is transformed into a local mobile call whereby the call is reinitiated with the CLI associated with the SIM card. So, in such situations the CLI is replaced by a local mobile number that originates from the SIM within the SIM box. As a result, the owner of the SIM box pays a retail mobile fee (likely unlimited minutes with a mobile flat fee subscription) instead of a wholesale termination fee if the call would have been terminated in the normal manner with the original international CLI.

If the sending operator is using in-line STIR/SHAKEN, the SIP PASSporT header may be lost in transit or removed by the fraudulent carrier. Although in such situations detection will still be difficult, with STIR/SHAKEN the terminating operator will present these call as "caller unverified" based on the attestation C value, by what the call seizure rate will decline for these calls making this fraud less lucrative.

In case the fraudulent carrier would include a SIP PASSporT header for the CLI associated with the SIM, then the payload of the PASSporT header needs to be signed and would require that the fraudulent carrier has a certificate for signing. As this certificate is unique for that carrier, on detection of the abuse the malicious carrier can be traced back and made responsible for the fraud. This is different from today where the identity of the manipulating carrier is normally hidden. However, abusive signing CLIs with attestation level A is conflicting with how STIR/SHAKEN guarantees the validity of the CLI, by what the certificate of the fraudulent carrier can be withdrawn to stop the abuse and possibly put more traffic at risk.

With the side-path transfer with solutions like Out-of-Band STIR/SHAKEN, SEISMIC and A&B Number handshake, then the receiving operator may check the CPS for existence of a PASSporT entry for a call to the B-number in the given timeslot. If so, the terminating operator may block the fraudulent call or let the call proceed with the CLI corrected based on the content of the PASSporT entry.

As in such cases the PASSporT information is send via the side-path, there is no possibility to falsify the inline call signaling information. And for the side-path the same conditions apply to any carrier involved in the side-path that would resign the PASSporT information.

- **Bypass fraud via hacked PBXs**

  It may be noted that this situation can be somewhat more diverse as PBX hacking may not always involve CLI Spoofing and calls may be either diverted via the hacked PBX or locally generated by the PBX. However, when CLI Spoofing is involved the same prevention potentials apply as for bypass fraud via SIM boxes.

## 6.6. Call Fraud Detection Solutions

Fraud due to CLI spoofing cannot be fully mitigated with a purely industry and standards driven approach. Reaching a critical mass of one single solution may be impossible, but at this point all parties understand that there will be no single solution and that interoperability amongst the different solutions will be the key to success. And this is achievable in case the solutions are built considering this need for interoperability and it is however is still envisaged but it needs to be understood that this will take time.

For this reason, call fraud detection solutions will coexist and will complement the standards driven approach. The following sections describe the potential approaches for the detection and prevention of Robocalling and CLI Spoofing in real-time.

### 6.6.1. Real-time Robocall Detection and Prevention

Robocalls often have a clear signature that can be picked up the analyzing in CDRs and more preferably, in real-time, based on signaling information like:

- **Perpetrator:** A-party
- **When:** During day and evening

- **Call Release:** B-party (in connected phase)
- **Filter:** One-to-many ingress
- **Number nature:** real B-numbers, fake/unallocated A-numbers, manipulated A-numbers (although it is not always the case)

Based on the traffic characteristics above, a one-to-many filter “gauge” can be applied to incoming calls matching the pattern. By doing so, a sliding window technique can prevent spikes of robocalls.

To increase the accuracy of such technique additional logic is crucial:

1. A blacklist and a whitelist shall exist to be applied to feed the logic with number (range)s from where the behavior is already known. These may be call numbers which are not robocalls but happen to have a similar signature or calls of known Robocallers.
2. Industry data should enhance the decision making. If CLIs are clearly wrong, e.g. to not match the (international) dialing plan, then the call may, signed or not, be dropped. Industry provided hotlists of Robocallers may assist as well in filling the blacklist.
3. One can make better decisions based on historical call data. Such analytics increase the chances of identifying a true-positive Robocaller.

### 6.6.2. Real-time CLI Spoofing Detection and Prevention

While industry standards such as STIR/SHAKEN and initiatives as SEISMIC will be key in fighting CLI spoofing, prevention and detection measures will continue to play a major role as well. From an operator perspective preventing CLI spoofing of its own subscriber base (or on national or regional level if such initiative exists) can be accomplished by applying a roaming status check on the subscriber, e.g. by a MAP AnyTimeInterrogation message or a check on the operators’ or carriers signaling firewall.

More complex is tackling CLI spoofing for the purpose of CLI refiling fraud and SIM boxing fraud. In such instances, the perpetrator is not the caller or the called number, but the fraud is rather occurring in transit.

The detection of CLI refiling calls starts with sanity checks about the validity of the CLI in order to verify if the manipulated CLI is correct according to the numbering plan and actual use. The typical sanity checks are on information like:

- Allocated A-party?
- Valid Type-of-Number format A-number?
- Minimum/maximum length A-number?
- Number portability status A-number?
- A-number not on blacklist?

In addition, these fraud cases can be tackled with probability based real-time decision making based on analytics. Historical traffic data, preferably unbiased, provides insights in the probability that certain calls are CLI-spoofed. For example, if an operator or carrier suddenly loses incoming calls from certain origins, then B-parties that were dialed from such origin historically could reveal CLI refiling by analyzing the A-parties from where calls those same B-parties arrive.

The outcome of such analysis could be a scoring mechanism where, based on probability, different measures might be taken as outlined in Figure 11 below:

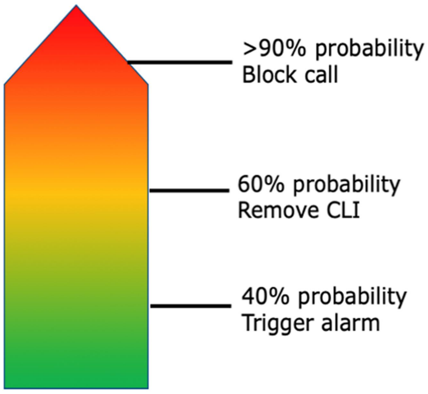


**Figure 11 – Probability based decision making for CLI Refiling**

With probability-based decision making a 0.9 probability might result in baldly blocking a call while a 0.6 probability would result removing the CLI to protect the customer.

# 7. Evaluation of solution alternatives

The following table summarizes the capabilities supported by the different solutions.

| | STIR/SHAKEN Solutions | | Out-of-Band Call Validation Solutions | |
|---|---|---|---|---|
| | **In-line** | **Out-of-Band** | **Routing on B-nb** | **Routing on RN** |
| **1. Standardized Solutions** | STIR/SHAKEN | OOB STIR / TDM SHAKEN | SEISMIC Simple | SEISMIC Sophisticated |
| • **Standards Availability** | Yes | Final drafts | In progress | In progress |
| • **Product Ready Status** | Yes | Proof of Concept | Proof of Concept | Proof of Concept |
| • **Commercially Available** | Already Deployed | Existing for piloting in US | 2022+ | 2022+ |
| **2. Commercially Available Proprietary Solutions** | | | A&B Number Handshake and SS7 CVS Call Validation | SS7 CVS Call Validation using MSRN for routing |
| • **Product Ready Status** | | | Yes | Yes |
| • **Commercially Available** | | | Already Deployed | Already Deployed |
| **3. Verification Capability** | | | | |
| • **Verification A-number** | Yes<br>secured CLI included in SIP | Yes<br>secured CLI transferred via CPS | Yes<br>secured CLI transferred via CPS | Yes<br>secured CLI transferred via CPS |
| • **Verification B-number** | Yes<br>secured B-nr included in SIP | Yes<br>secured B-nr transferred via CPS | Yes<br>secured B-nb transferred via CPS | Yes<br>secured B-nb transferred via CPS |
| **4. CLI Spoofing Prevention/Detection** | | | | |
| • **WANGIRI** | Yes<br>The secured CLI in the SIP PASSporT header can't be spoofed | Yes<br>If CLI in call setup and secured CLI via CPS don't match | Yes<br>If CLI in call setup and secured CLI via CPS don't match | Yes<br>If CLI in call setup and secured CLI via CPS don't match |
| • **SPAM CALLS** | Yes<br>The secured CLI in the SIP PASSporT header can't be spoofed | Yes<br>If CLI in call setup and secured CLI via CPS don't match | Yes<br>If CLI in call setup and secured CLI via CPS don't match | Yes<br>If CLI in call setup and secured CLI via CPS don't match |
| • **ROBOCALLING** | Yes<br>The secured CLI in the SIP PASSporT header can't be spoofed | Yes<br>If CLI in call setup and secured CLI via CPS don't match | Yes<br>If CLI in call setup and secured CLI via CPS don't match | Yes<br>If CLI in call setup and secured CLI via CPS don't match |
| • **OBC SPOOFING** | Yes<br>The secured CLI in the SIP PASSporT header can't be spoofed | Yes<br>If CLI in call setup and secured CLI via CPS don't match | Yes<br>If CLI in call setup and secured CLI via CPS don't match | Yes<br>If CLI in call setup and secured CLI via CPS don't match |
| • **VM BRUTE FORCE** | Yes<br>The secured CLI in the SIP PASSporT header can't be spoofed | Yes<br>If CLI in call setup and secured CLI via CPS don't match | Yes<br>If CLI in call setup and secured CLI via CPS don't match | Yes<br>If CLI in call setup and secured CLI via CPS don't match |

| | STIR/SHAKEN Solutions | | Out-of-Band Call Validation Solutions | |
|---|---|---|---|---|
| | In-line | Out-of-Band | Routing on B-nb | Routing on RN |
| • CALL BOMBING | Yes<br>The secured CLI in the SIP PASSporT header can't be spoofed | Yes<br>If CLI in call setup and secured CLI via CPS don't match | Yes<br>If CLI in call setup and secured CLI via CPS don't match | Yes<br>If CLI in call setup and secured CLI via CPS don't match |
| • BYPASS FRAUD | Yes<br>The secured CLI in the SIP PASSporT header can't be spoofed | Yes<br>If CLI in call setup and secured CLI via CPS don't match | Yes<br>If CLI in call setup and secured CLI via CPS don't match | |
| **5. Signaling Support Capability** | | | | |
| • Valid for ISUP | No<br>needs end-to-end SIP support | Yes<br>signaling agnostic path via CPS | Yes<br>signaling agnostic path via CPS | Yes<br>signaling agnostic path via CPS |
| • Valid for SIP | Yes<br>needs end-to-end SIP support | Yes<br>signaling agnostic path via CPS | Yes / No (SS7 CVS)<br>signaling agnostic path via CPS | No<br>signaling agnostic path via CPS |
| • Valid for mix SIP / ISUP | No<br>Needs end-to-end SIP support | Yes<br>signaling agnostic path via CPS | Yes / No (SS7 CVS)<br>signaling agnostic path via CPS | No<br>signaling agnostic path via CPS |
| **6. Service Availability** | | | | |
| • Call continuation if call context is missing | Yes<br>Call presented with CLI unverified indication if PASSporT is missing | Yes<br>Call presented with CLI unverified indication if PASSporT is missing | Yes<br>Call presented with CLI unverified indication if CPS is unavailable | No<br>Call cannot be established if B-nb is not retrievable via CPS context |
| **7. System Architecture** | | | | |
| • Centralized architecture | Yes | Yes | No | No |
| • Central authentication authority required | Yes | Yes | No | No |
| • Specific external infrastructure required | Yes<br>automated key mngt exchange needs SHAKEN framework | Yes<br>Parallel CPS infrastructure and SHAKEN framework | Yes<br>Parallel CPS infrastructure | Yes<br>Parallel CPS infrastructure |
| **8. Business impact on carriers** | | | | |
| • Routing Services | No<br>No change, B-nb used for routing | No<br>No change, B-nb used for routing | No<br>No change, B-nb used for routing | Yes<br>Routing Number used for routing |
| • Signing and Validation logic | Low / Medium / High<br>See for more details section 6.5.1 | Low / Medium / High<br>See for more details section 6.5.1 | Small / Medium investment<br>Only parallel CPS infra needed with reuse existing routing practices | Medium investment<br>More complex solution with B-nb replacement by routing number |
| • Migration to IP | Expensive and complex<br>Long winding implementation to decommission all TDM trunks | Small investment<br>Only parallel CPS infra needed and allows reuse existing TDM | Small investment<br>Only parallel CPS infra needed and allows reuse existing TDM | Small investment<br>Only parallel CPS infra needed and allows reuse existing TDM |
| • New business opportunity | Yes<br>If operators will outsource PKI function to carrier | Yes<br>If operators will outsource PKI function to carrier | Yes<br>If operators will outsource PKI function to carrier | Yes<br>If operators will outsource PKI function to carrier |
| **9. Impact on Trouble Ticketing** | No<br>B-nb transferred as is and CLI can't be spoofed | No<br>B-nb transferred as is and CLI via CPS can't be spoofed | No<br>B-nb transferred as is and CLI via CPS can't be spoofed | Yes<br>B-nb replaced by Routing Number and CLI via CPS can't be spoofed |

# 8. Recommendations for Wholesale Carriers and IPX Providers

This chapter first outlines the generic set of guidelines that typically refer to the business and operational interests of wholesale carriers and IPX providers. Subsequently guidelines are provided for the solution strategy as attributes for the selection process of the CLI Spoofing solutions as sketched in this report.

## 8.1. Generic Guidelines

1. The industry is not served with proprietary solutions because fighting CLI Spoofing practices will be best served with general adoption of standardized solutions given the critical mass that will be needed which requires mutual trust and openness of the technical practices.
2. No anonymization of data like with the use of routing numbers and pointers because the wholesale carriers and IPX providers need visibility of the actual data for the execution of their services.
3. Solutions like STIR/SHAKEN are acceptable that entail encryption of information that is used by the sender and receiver for the end-to-end authentication and validation of the CLI information.

## 8.2. Solution Strategy

1. STIR/SHAKEN is considered the most favorable long-term approach because it has the least impact on the business and activities of the wholesale carriers and IPX providers. It combines end-to-end authentication and validation of the CLI signing process together with A-number visibility as is.
2. It is recognized that STIR/SHAKEN will not be the single solution to resolve the problem of CLI Spoofing due to different regulatory regimes, maturity of the problem, and the variety of dominant fraud types in different regions.
3. Surrounding solutions may be considered that are seamless inter-operable with STIR/SHAKEN implementations in countries or regions to grow the critical mass of the CLI Spoofing eco-system.
4. The international carrier community can leverage the STIR/SHAKEN experience of North American operators working with each other and their respective regulatory agencies on adoption and implementation challenges over the past few years.
5. The STIR/SHAKEN – OOB model and the STIR/SHAKEN Enterprise model could be necessary to create meaningful coverage as legacy TDM networks will likely remain in many markets slow to transition to IP and legitimate Enterprise calls should be fully trusted.
6. It is recognized that the STIR/SHAKEN type of solutions solve the problem of CLI Spoofing but are not protecting against other types of inter-carrier fraud.

# 9. Document History

| Version | Date | Description | Editor |
|---|---|---|---|
| Draft | 11 March 2020 | Document structure | Gregory Koch (Koch Consultancy) |
| Draft | 12 May 2020 | Initial content as input for i3forum Technology WG call 14 May | Filippo Cauci (Sparkle) e.a. |
| Draft_04 | 30 May 2020 | Update for discussion at i3forum Technology WG call 3 June | Filippo Cauci (Sparkle) e.a. |
| Draft_05 | 11 June 2020 | Update discussed i3forum Technology WG call 3 June and merged with evaluation by i3forum Fight against Fraud WG | Pieter Veenstra (NetNumber) e.a. |
| Draft_06 | 16 June 2020 | Comprehensive review of draft_05 | Jens Johann (Deutsche Telekom) |
| Draft_07 | 16 June 2020 | Additions to section 6 | Pieter Veenstra (NetNumber) |
| Draft_08 | 29 June 2020 | New baseline based 3forum Fight against Fraud WG call on June 24th and of the i3forum Technology WG call on June 25th | Pieter Veenstra (NetNumber) e.a. |
| Draft_09 | 10 July 2020 | Update based on comments via email review | Pieter Veenstra (NetNumber) e.a. |
| Draft_10 | 17 July 2020 | Input for i3forum Fight against Fraud WG on July 20th and of the i3forum Technology WG on July 21th | Pieter Veenstra (NetNumber) e.a. |
| Draft_11 | 27 July 2020 | Preparation final draft based on i3forum Fight against Fraud WG call on July 20th and i3forum Technology WG call on July 21th | Pieter Veenstra (NetNumber) e.a. |
| Draft_12 | 31 July 2020 | Early draft preparation for sharing with GSMA VINES based on consolidation of draft_11 | Katia Gonzalez (BICS), Filippo Cauci (Sparkle), Tamas Marothy (i3F) and Pieter Veenstra (NetNumber) |
| Draft_13 | 11 Sept 2020 | Updated draft with:<br>• Proposed additions based on comments by Sergey per email August 28th<br>• Write-up of recommendations in chapter 8 based on discussion Katia, Filippo, Greg Tamas and Pieter in review call July 31st<br>• Proposed handling of comments by Greg in email August 18th and refinements by Katia in email Sept 2nd | Pieter Veenstra (NetNumber) e.a. |
| Draft 14 | 28 Sept 2020 | Updated draft with refinements as per i3forum Fight against Fraud WG call on Sept 21st:<br>• Item 6 added in section 8.2 as suggested by Katia that Stir/Shaken solutions don't cover all forms of inter-carrier fraud<br>• Updates in rows 1 and 2 with refined times for already operational solutions<br>• Confirmation of comment handling for this release of the report by Sergey in his email of Sept 22nd | Pieter Veenstra (NetNumber) e.a. |
| Draft 15 | 1 Oct 2020 | In 6.5.1 added a clarification and reference to | Greg Koch (i3forum) |

| Version | Date | Description | Editor |
|---|---|---|---|
| | | the item in the evaluation table following the i3forum Technology WG on Sept 29th | and Pieter Veenstra (NetNumber) |
| Finaldraft | 14 Oct 2020 | Preparation final draft with following changes:<br>• Handling of comments by GSMA VINES as by Chris and multiple rewordings of legal manipulation of CLI cases as per Michael<br>• Refinement of item 4 in evaluation table in section 7 by Jens | Chris Drake (iconectiv), Jens Johann (Deutsche Telekom), Michael Coupland (Bell CA) and Pieter Veenstra (NetNumber) |
| Final | 26 Oct 2020 | This includes the final review during the call of the i3F Technology Group on Oct 26th:<br>• A few simple rewordings based the line-by-line review on the changes in the finaldraft<br>• The addition of the section 6.5.9 “Tackling Interconnect Bypass Scenarios” that clarifies how the STIR/SHAKEN and alike solutions may be assistant to tackle inter-carrier fraud plus cross-references to this new section in 5.2.4 and 5.2.7. | Pieter Veenstra (NetNumber) |