INTERNATIONAL INTERCONNECTION FORUM FOR SERVICES OVER IP

CLI Safe Zone: Global industry led interworking framework for trusted and authenticated CLI transfer

Release 1.0 – November 2023

I3Forum CLI Safe Zone

1. Fighting Robocall Practices

Regulators in various countries are directing national operators to implement solutions to return trust in voice calls by improving the validity and authenticity of the Calling Line Identity (CLI).

In previous years, much attention has been paid to the FCC-driven STIR/SHAKEN developments in the US, but alternate developments in many other countries around the world have either been implemented or planned, in order to protect subscribers from unwanted robocalls and other scam practices.

A critical aspect in all these solutions is the risk associated with international incoming calls. The aim of the CLI Safe Zone framework is to resolve this risk and mitigate in the most efficient way the business uncertainties for Int'l Carriers due to various regulatory requirements, solutions for both CLI protection and processes for traceback.

2. Solving Which Problem

The following Table 1 (status July/August 2023) demonstrates that the CLI protection solutions in different countries and regions are quite diverse and not inter-operable over the international interconnect.

	1. CLI Securing Solutions		2. CLI Validating Solutions		3. Roaming Status Checks		4. Call Set-up Action(s) in the Network	5. SMS Compliance
	STIR/SHAKEN Domestic	International Inbound	Numbering Plan Sanity Checks, etc.	DNO Lists	Between Domestic PLMNs	With Foreign Visited PLMNs		CLI and DNO
US	US/Canadian version	Yes	Yes	Yes	-	-	No	CLI Validation and DNO
Canada	US/Canadian version	-	Yes	-	-	-	No	-
France	French version	Planned	-	Yes	-	-	Blocking (national)	DNO
Australia	-	Yes	Industry Code C661	-	-	-	Blocking	CLI Validation and DNO
Belgium	-	-	CLI guidelines BIPT	-	-	-	Blocking	-
Latvia	-	-	CLI guidelines NRA	-	-	-	Blocking	-
Norway	-	-	Regulation and Nkom	-	-	-	Blocking	-
UK	Under study	-	CLI guidelines Ofcom	Yes	Under study	Under study	Blocking (non mobile)	MEF SMS SenderID Reg
Finland	-	-	Guidelines Traficom	-	API call	-	Blocking (national) & CLI removal	-
Poland	Under study	-	CLI guidelines UKE	-	API call	CAMEL	Blocking	-
Germany	-	-	For specific CLI ranges	-	-	CAMEL	CLI removal	-
Saudi Arabia	-	-	-	-	SS7 ATI	-	Blocking	-
Oman	-	-	-	-	SS7 SRI-SM	-	Blocking	-
China	-	-	-	-	-	-	Blocking	-
Ireland	Under study	-	CLI guidelines IREG	Yes	Under study	Under study	Blocking	MEF SMS SenderID Reg
India	-	-	CNAP under study	-	-	-	No	MEF SMS SenderID Reg
Malaysia	-	-	-	-	-	-	No	Blocking SMS containing URLs
CAN (Note)	-	-	Threshold-based rules on single A-numbers	-	-	-	Blocking	-

Status July/August 2023

Note: Andean Community (CAN) - Bolivia, Colombia, Peru and Equador, with associate members Chile, Argentina, Brazil, Paraguay and Uruguay

Source i3forum, including industry input led by Titan.ium and Xconnect

Table 1 – Overview of CLI protection solutions per July/August 2023

The four main solution approaches in the various countries can be classified as follows:

1. CLI Securing Solutions – In these solutions the CLI transfer is secured by cross-checking the CLI with a signature (STIR/SHAKEN) for voice calls between operators within a country (and between the operators in US and Canada), and for international inbound voice calls in some countries (like voice calls with trusted CLIs on dedicated separated incoming trunks).
2. CLI Validating Solutions – Here the CLI is verified against the number plan, number length, other numbering plan, blacklist checks, ingress point of the call (e.g. international) etc. Domestic calls not meeting acceptable criteria are expected to be blocked, whilst international ingress calls may be blocked, have the CLI removed or CLI marked restricted. Additionally, Do Not Originate (DNO) registries are used to block traffic with a CLI containing a number that is not used on outbound calls.
3. Roaming Status Checks – This solution is applied at the international ingress of the country where the call terminates. The domestic mobile network operators will be requested by the international gateway to provide a verification that the domestic mobile CLI received at the international gateway is assigned to a roaming customer. This can be achieved through existing SS7 methods or potentially through APIs, and optionally, verifying the status of the mobile user in the visited mobile network in the other country via CAMEL triggering.
4. Call Set-up Actions – This column shows the operator behaviour in specific countries upon receipt of a CLI that is deemed to be invalid. The call may be blocked or the CLI removed before the call is allowed to continue.
5. SMS Compliance – In some countries also the SMS messaging traffic is screened for falsified sender addresses, or in Malaysia, an additional check of the SMS user content to screen if the SMS contains vulnerable data like of robomessaging spam campaigns or an URL of a phishing attack.

National Implementation variants of the same solution approach co-exist (e.g. STIR/SHAKEN implemented in the US/Canada versus France and national variants of Mobile Roaming checks), which do not interwork due to incompatibility issues.

In many countries these solutions are complemented with call blocking policies whereas in other countries it is left to subscribers to decide whether to answer a call based on presented attestation information. Blocking policies can either be imposed by regulatory demand or agreed as part of

industry self-regulation. In the US, the regulator may instruct international gateway operators to block calls from specific international origins and transit network operators to block calls from upstream networks/customers. Failure to meet the blocking instruction can result in severe penalties imposed by the regulator.

As a result of the diversity of solutions (and their variants), and a highly unlikely global approach in standardization, trusted CLI information sent from one country is lost when the call terminates in another country.

3. Solution Limitations

Given that these solutions are solving very different problems, each solution has its specific purpose and limitation, and can complement each other:

- CLI Securing Solutions
    - Although these solutions provide technical means that a CLI cannot be manipulated (e.g. spoofed) undetected between ingress point and egress point of the solution, it does not protect against spoofed CLIs entering the solution (garbage in – garbage out).
    - As an example, If the originating STIR/SHAKEN operator is the only provider that can truly attest to the authenticity of the CLI (calling party was properly assigned the CLI and therefore confirmed they can use it), it is then unclear as to the value of other parties signing calls with lower confidence attestation levels. What evidence or data supports the claim that carriers signing calls with low level attestation prevents spoofing and SPAM (not all is per definition unwanted and illegal communications)? Also, calls signed with low attestation levels may remove traffic from an addressable green tick or trusted call market.

- CLI Validating Checks
    - CLI Validating solutions can detect occurrences of manipulated CLIs, but the accuracy is highly dependent on the accuracy and granularity of the data used for checking. More sophisticated spoofing techniques may not be detected. However, such checks can be of help to prevent spoofed CLIs entering a STIR/SHAKEN or Calling Name Presentation (CNAP) securing CLI transfer solution.
    - Bad actors can spoof legitimate or valid CLIs (origination IDs?) which would then bypass many of the traditional CLI validation checks. While this limitation does exist, many

unwanted and illegal communications utilize numbers that are invalid, unallocated, unassigned, designated for inbound only, and therefore can be detected with solid CLI validation checks and procedures.

- CNAP as considered by the India regulator in a consultation, does not address calls originated outside of India destined for Indian termination. It is limited to a national approach that addresses Indian domestic traffic only. If we extend the concept to include international traffic, there would need to be an accurate and updated global reference of names and phone numbers encompassing all worldwide voice subscribers (>7 billion). Global policies to manage consent and similar data protection and privacy concerns is another challenge (herculean challenges also considered limitations) to this approach.

- Roaming Status Checks
  - Mobile roaming status checks are needed given that incoming international calls can include domestic mobile CLIs of the country where the call is to terminate, and thus calls with a spoofed mobile CLI cannot be detected using other CLI validation checks.
  - There are legal and technical complexities or limitations to sharing subscriber status information that is required in roaming status check solutions. Legal requirements vary from country to country regarding personal data and location protection concerns. This solution would require arriving at a global policy or worldwide compromise in terms of an acceptable path forward that is approved by the NRAs, working within their jurisdictional framework.
  - Technical limitations also exist in terms of storing and transferring location status information across operator and service provider networks like when the mobile networks are of varying technology generations (SS7 is typically for 2G/3G networks, Diameter for 4G and HTTP/2 for 5G) or fixed networks without support of these SS7, Diameter or HTTP/2 roaming protocols. Alternatively, APIs or other protocols can be used by international gateways to retrieve and exchange subscriber roaming status information which may not have the same limitations.

- Call Set-up Actions in the Network
  - CLI removal policies can impact legitimate Enterprise DID and Call Center traffic due to the removal or blocking of domestic non-mobile CLI found in these international calls.

Without a proper right of use function to identify and allow authentic, safe, international enterprise and call center traffic utilizing domestic CLI, these services could be permanently disrupted.

- SMS Compliance
    - Mobile operators may already have implemented Home Routing and SMS Firewalls but still SMS fraud and manipulated SMS is a growing concern in the industry. This is also partly caused as commercial senders of SMS very often do not follow strict rules for their embedded URLs by what the innocent receiver of the SMS is not able to easily distinct real addresses from false addresses.

In additional to the solutions in Table 1, strong customer vetting processes and traffic analytics are useful additional tools to assist with Know Your Customer and Know Your Traffic solutions and requirements. One limitation to traffic analytics is its inability to pinpoint spoofing. Analytics (today) do not provide proof that the calling party either has the right, or not, to use the CLI. There are also many false positives associated to traffic monitoring and analytic solutions. Second layer human oversight is required to follow-up and confirm many cases that carrier systems flag as 'potentially' unwanted and illegal communications. Advanced AI could provide an opportunity to further fine-tune present data analytic approaches. However, global coordination is a question given intellectual property considerations and the commercial nature of these implementations.

4. CLI Safe Zone Solution Potential

The different solution strategies in countries and regions to restore CLI trust (e.g STIR/SHAKEN or blocking suspicious calls) create business risks for the Int'l Carriers:

1. Decreasing call/answer rates for international calls, especially in countries where solutions are being implemented to protect subscribers against vulnerable calls, as in such situations international calls are offered to subscribers with a low attestation value or without CLI. This makes the subscribers less willing to answer any incoming international call.
2. To implement a wide range of solutions to comply to the varying national regulation frameworks for the termination of international calls and in support of traceback repercussion actions.

The concept of the CLI Safe Zone framework is an industry led initiative between the Int'l Carriers in the i3Forum to provide a path toward inter-

operability between the different national CLI trust initiatives in order to restore trusted and authenticated CLI transfer for international calls.

Figure 1 sketches the position and the concept of i3Forum's CLI Safe Zone framework acting between a domestic originating network in Country A and a domestic termination network in Country B. These networks can either be fixed networks, mobile networks or a mix thereof.

Figure 1 – Concept of i3Forum's CLI Safe Zone framework

The CLI Safe Zone as industry led interworking framework by the Int'l Carriers in the i3Forum is to provide an interworking framework between different CLI protection solutions in various domestic countries and to provide the following three key capabilities:

1. At the originating side (the CLI Safe Zone ingress) to validate the CLI entering the CLI Safe Zone with checks depending on the situation in the domestic originating network like:
    - In case of STIR/SHAKEN a validation check of the CLI similar as a terminating carrier in the domestic originating network to retrieve the attestation value of the CLI to be mapped to normalized CLI trust level in the CLI Safe Zone.
    - If the trust of traffic is differentiated via trunk separation to use the incoming trunk identity to assess the appropriate attestation value of the CLI, but not an option if the traffic can be received from different originating carriers.

    Optionally, see also the considerations in section **Error! Reference source not found.** below, additional CLI sanity checks may be implemented before a call is entering the CLI Safe Zone:

    - In other situations, numbering plan consistency checks and other sanity checks of the CLI to screen for malicious calls with detectable manipulated CLIs.
    - Also some basic screening of the CLI may be performed in cases where the CLI refers to the numbering plan of the domestic terminating network in country B like for calls made

by a mobile user roaming in a visited mobile network within country A.

2. Within the CLI Safe Zone between Int'l Carriers to provide an end-to-end secure transfer in combination with reliable post-call traceback capabilities between the carriers serving the domestic network in country A and the domestic network in country B:
    - During call setup, supporting a data integrity protection solution whereby the CLI cannot be modified or changed unnoticeable like for inter-carrier fraud and other irregularities during forwarding of the call by an intermediate Int'l Carrier, and if modified, the identity of the Int'l Carrier will be known that made the change and becoming liable for the integrity of the CLI.
    - Post call, support of traceback and processes for reconciliation based on CLI authentication information of the liable Int'l Carrier associated with each individual call instance.
    - Surrounding governance and policy actions to keep the CLI Safe Zone secure and reliable performed by i3Forum as industry body that will surveil membership of the CLI Safe Zone and abandon fraudulent carriers from the system. This will imply that trusted international carriers would become members of a group of carriers who define and agree on a set of criteria, monitor compliance of those criteria and enforce these criteria to pass traffic in a secure manner. If a carrier in the group subsequently fails to meet the criteria, it will no longer be able to participate in the end-to-end secure transfer and traceback capabilities. Likely such a fraudulent carrier will also be disconnected by domestic networks.

      NOTE This will imply that trusted international carriers would become members of a group of carriers who have agreed to meet a set of criteria so as to be able to pass traffic in a secure manner. If a carrier in the group subsequently fails to meet the criteria, it will no longer be able to participate in the end-to-end secure transfer and traceback capabilities. Likely such fraudulent carriers will by disconnected by domestic networks.

3. At the terminating side (the CLI Safe Zone egress) to forward the CLI with associated CLI trust actions depending on the situation in the domestic terminating network and the received attestation value set by the preceding and identifiable Int'l Carrier in the CLI Safe Zone liable for the CLI like:

- In case of STIR/SHAKEN setting of the attestation level of the CLI as received as part of the call setup from the preceding Int'l Carrier in the CLI Safe Zone.
- If the trust of traffic is differentiated via trunk separation, to select the appropriate outgoing trunk in accordance with the received trust value of the CLI.

Optionally, see also the considerations in section **Error! Reference source not found.** below, additional CLI sanity checks may be implemented before a call is leaving the CLI Safe Zone:

- For calls received with a CLI of a mobile subscriber, a complimentary mobile roaming status check to verify whether the mobile subscriber is roaming in a foreign mobile network, or not.
- Complimentary numbering plan consistency checks and other sanity checks of the CLI to screen for malicious calls with detectable manipulated CLIs.
- Depending on the regulatory demands in the domestic country B with a malicious or untrusted CLI, specific call treatment actions like dropping the call setup instance, or removing the CLI field from the call set, or else.

5. Mission of the CLI Safe Zone

An important question to consider for both regulators and i3Forum is to agree on the mission of the CLI Safe Zone as there are potential conflicts of interest:

- Originating side (the CLI Safe Zone ingress)

  It seems self-evident that knowledge about the trust of a CLI in country A of origin is an important asset for the functioning of the CLI Safe Zone.

  However, it may be queried if additional sanity checks of the CLI at the originating side are a responsibility of the Int'l Carriers, or not. Since the accuracy of such sanity checks is no 100% guarantee that the CLI is not manipulated, the only certainty what is received by incoming call setup at ingress side at country A and translated as CLI trust information to the egress side at country B of the CLI Safe Zone.

- Within the CLI Safe Zone (in between Int'l Carriers)

Known CLI trust information (like derived from STIR/SHAKEN attestation values, traffic routed over dedicated trunks, or else) at the CLI Safe Zone ingress point in country A is to be interworked and transferred to the terminating side of the CLI Safe Zone egress point in country B.

- Terminating side (the CLI Safe Zone egress)

  Idem, it seems self-evident that the CLI trust information transferred over the CLI Safe Zone is to be mapped to any CLI protection mechanism implemented and regulated in the terminating country B.

  However, it may be queried if additional sanity checks of the CLI at the terminating side are a responsibility of the Int'l Carriers, or not. It should be considered that CLI Sanity Checks and Mobile Status Checks are depending on the regulatory demands, privacy legislation and jurisdiction in the terminating country B.

Consequently, it is proposed to define the working of the CLI Safe Zone based on the principle of the mapping of known CLI trust information in country A and to be interworked to CLI trust information in country B. Additional checks on the ingress side in country A and on the egress side in country B are left to the legal requirements and service requests of the network operator in the respective domestic countries A and B.

In addition, in the begin the primary goal of the CLI Safe Zone is to improve the trust of international calls in terminating countries with a CLI protection solution implemented. Although the callee in country B may not be helped with a trustable CLI, traceback to ingress side of the CLI Safe Zone will be supported, and optionally, suspicious calls may with additional CLI sanity checks and/or Mobile Status checks, see above.

When both sides have a CLI protection solution implemented, the overall working of the eco-system will further improve:

- A direct effect to the callee in the terminating network by receiving calls with an attestation information for trustable CLIs and not hindered and confused by calls with spoofed CLIs.
- For the caller in the originating network the advantages that its call is more likely being answered and no confusion at the callee as the CLI can no longer be manipulated.
- The traceback capability will improve with details about the originating operator network where the call started and the root of the CLI.

6. Legislation and Regulatory Aspects

The following aspects relate to the demands and concerns in the field of legislation and regulation:

- Noting strict data protection and privacy legislation in the various countries, use of a central network resource for routing and call setup information transfer is not currently being considered as part of the CLI Safe Zone because it would introduce security and privacy risks, would raise political concerns, and potentially creates a honeypot for intruders.
- Specific regulations in different countries may give rise to conflicts of interest with stricter CLI trust rules and may also not be resolved by the CLI Safe Zone. If the regulations in the sending country A would require omitting the CLI for calls to some countries, such calls may fail if the regulations in the receiving country B require that incoming international calls must be blocked with an empty CLI field.

7. Summary

This industry led initiative by the i3Forum as a neutral, not for profit body, to orchestrate and acting as a watchdog with support from the regulatory authorities around the world is aimed to mitigate the limited international jurisdiction of the global problem.

This initiative is to accelerate the adoption by the international communications industry given the diversity of mechanisms promoted by domestic regulatory bodies without disrupting the existing open business model and existing technical interconnects by this industry led initiative facilitated by the i3Forum.

The working of the CLI Safe Zone will be based on CLI trust information in country A mapped to CLI trust information in country B. Additional checks on the ingress side and on the egress side are left to the legal requirements and service requests in the domestic countries A and B.

APPENDIX

1. References

US FCC-CIRC2205-01 (approved May 2022) that mandates the specific conditions and technical means operators need to follow for international inbound voice call

France STIR/SHAKEN regulation French Law n° 2020-901 "Naegelen" specifies that the Calling Line Identity (CLI) must be authenticated by the CSPs before continuing any call

Australia ACA Code C661:2022 Reducing Scam Calls and Scam SMS; Australian Communications Alliance Ltd.

Belgium Guidelines Calling Line Identification (CLI) of 4 December 2020; Belgian Institute for Postal Services and Telecommunications (BIPT).

Latvia Numerācijas krāpniecības novēršanas noteikumi (Numbering Fraud Prevention Rules); Public Utilities Commission Latvia.

Norway Regulations on electronic communications networks and electronic communications services (ekom regulations); Nkom.

UK Guidance on the provision of Calling Line Identification facilities and other related services

Finland Traficom, Recommendation To Telecommunications Operators On Detecting And Preventing Caller Id Spoofing

Germany Telekommunikationsgesetz (TKG) 2021 - §120 Rufnummernübermittlung

China Law Against Telecom and Online Fraud [反电信网络诈骗法

India Consultation Paper on Introduction of Calling Name Presentation (CNAP) in Telecommunication Networks" 2022

Singapore Notification Of Proposed Direction Under Section 31 Of The Telecommunications Act 1999 ("Act"): Implementation Of Measures To Address Spoofed Calls

Europe ECC Report 338, CLI Spoofing; CEPT https://docdb.cept.org/document/28558

CEPT ECC Report 338, CLI Spoofing

i3Forum Presentation at ITW 2023; Restoring Public Trust in International Communications; An Industry Call to Action