Improving CLI Validity – Solutions and Regulatory Assessment

Version 1.0

2 October 2023

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

Table of Contents

1 Introduction

In recent years, the mobile industry has seen a range of different approaches seeking to improve the validity of the Calling Line Identity (CLI) as a response to the rapidly growing threat from CLI manipulation. Identifying the best approach for improving CLI validity for a particular situation requires good understanding of the different methods available and an assessment of each.

The main objective of this GSMA white paper is to describe current CLI validation solutions and provide an assessment of each from a mobile industry perspective. This paper is provided only for the information and education of GSMA members and others. It does not seek to place any requirements on GSMA members or to recommend a particular industry approach.

This document provides a snapshot of this topic at the date of last update. Updates to this document are planned to reflect relevant regulatory and industry developments.

1.1 Abbreviations

Term	Description
ACME	Automated Certificate Management Environment
ANI	Automatic Number Identification
ATI	AnyTimeInterrogation
ATIS	Alliance for Telecommunications Industry Solutions
CDB	Central Participant Database
CIV	Caller ID Verification
CLI	Calling Line Identity
CNAP	Calling Name Presentation
CRL	Certification Revocation List
CVT	Caller Validation Treatment
DNO	Do Not Originate
IETF	Internet Engineering Task Force
IRSF	International Revenue Share Fraud
JWT	Java Web Token
NANP	North America Numbering Plan
NNI	Network to Network Interface
OBR	Origin-Based Rating
OCN	Operating Company Number
OOB	Out of Band
OSP	Originating Service Provider
PASSporT	Personal Assertion Token
PKI	Public Key Infrastructure
SP	Service Provider
SPC	Service Provider Code

Term	Description
STI	Secure Telephone Identity
STI-AS	Secure Telephone Identity – Authentication Service
STI-CA	Secure Telephone Identity – Certification Authority
STI-CPS	Secure Telephone Identity – Call Placement Server
STI-GA	Secure Telephone Identity – Governance Authority
STI-IWF	Secure Telephone Identity – Inter Working Function
STI-OOBS	Secure Telephone Identity – Out of Band Service
STI-PA	Secure Telephone Identity – Policy Administrator
STI-VS	Secure Telephone Identity – Verification Service
STIR/ SHAKEN	Secure Telephone Identity Revisited / Signature-based Handling of Asserted information using toKENs
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TSP	Terminating Service Provider
UCC	Unsolicited Commercial Communications
UNI	User Network Interface

1.2 References

Ref	Doc Number	Title
[1]	CFCA	CFCA Fraud Loss Survey Report 2021 https://cfca.org/wp-content/uploads/2021/12/CFCA-Fraud-Loss-Survey-2021-2.pdf
[2]	CIV	New ways to stop caller ID spoofing to be investigated; Warwick University; https://warwick.ac.uk/newsandevents/pressreleases/new_ways_to/
[3]	E.164	The international public telecommunication numbering plan; ITU-T. https://www.itu.int/rec/T-REC-E.164/en
[4]	ECC 338	ECC Report 338, CLI Spoofing; CEPT https://docdb.cept.org/document/28558
[5]	ARCEP 2019-0954	Décision n°2019-0954 de l'Autorité de régulation des communications électroniques et des postes en date du 11juillet 2019 modifiant la décision établissant le plan national de numérotation et ses règles de gestion https://www.arcep.fr/uploads/tx_gsavis/19-0954.pdf
[6]	ACA Code C661:2022	C661:2022 Reducing Scam Calls and Scam SMS; Australian Communications Alliance Ltd. https://www.commsalliance.com.au/Documents/all/codes/c661
[7]	BIPT	Guidelines Calling Line Identification (CLI) of 4 December 2020; Belgian Institute for Postal Services and Telecommunications (BIPT). https://www.bipt.be/operators/publication/guidelines-calling-line-identification-cli-of-4-december-2020

Ref	Doc Number	Title
[8]	Latvia	Numerācijas krāpniecības novēršanas noteikumi (Numbering Fraud Prevention Rules); Public Utilities Commission Latvia. https://likumi.lv/ta/id/335934-numeracijas-krapniecibas-noversanas-noteikumi
[9]	Norway	Regulations on electronic communications networks and electronic communications services (ekom regulations); Nkom. https://lovdata.no/dokument/SF/forskrift/2004-02-16-401
[10]	Ofcom UK	Guidance on the provision of Calling Line Identification facilities and other related services. https://www.ofcom.org.uk/__data/assets/pdf_file/0021/247503/CLI-guidance-annex.pdf
[11]	TKMG	German Telecommunications Modernisation Act (TKMG), 23 June 2021 (German only) https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1858.pdf%27%5D__1683545909352
[12]	China	Law Against Telecom and Online Fraud [反电信网络诈骗法 http://www.npc.gov.cn/npc/c30834/202209/faadac81d2e94aa0bd7574efc9862cd0.shtml
[13]	India	Consultation Paper on Introduction of Calling Name Presentation (CNAP) in Telecommunication Networks" 2022 https://www.trai.gov.in/sites/default/files/CP_29112022.pdf
[14]	i3forum	Presentation at ITW 2023; Restoring Public Trust in International Communications; An Industry Call to Action https://i3forum.org/wp-content/uploads/2023/08/i3forum-Restore-Trust-in-Intl-Communications-August-23.pdf
[15]	Ireland	Combatting scam calls and texts. Consultation on network-based interventions to reduce the harm from Nuisance Communications. Comreg, June 2023 https://www.comreg.ie/media/2023/06/Consultation.pdf
[16]	Finland 1	Recommendation to Telecommunications operators on Detecting and preventing Caller ID spoofing. Traficom, May 2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/EN%20Recommendation%20to%20Telecommunications%20Operators%20on%20Detecting%20and%20Preventing%20Caller%20ID%20Spoofing.pdf
[17]	Finland 2	Traficom and Finnish telecommunications operators join forces to help customers by stopping caller ID spoofing. June 2022 https://www.traficom.fi/en/news/traficom-and-finnish-telecommunications-operators-join-forces-help-customers-stopping-caller
[18]	ECC	Draft ECC Recommendation (23)03; Further to ECC Report 338 - Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers https://cept.org/files/9522/Draft%20ECC%20Recommendation%20(23)03_v1.docx

2 Problem Description

2.1 Definitions and Background

Calling Line Identity, Caller ID or CLI is a number by which inbound calls made to individuals or businesses can be identified by their origin number. CLI spoofing refers to manipulation of the IP address, CLI or automatic number identification (ANI) to hide someone's true origination or identity. Common CLI spoofing scenarios involve spamming, phishing, robocalls and one-ring scams.

CLI spoofing is a prevalent source of damage to organisations and individuals. CLI manipulation may also lead to considerable social and organisational damage when state and emergency agency numbers are manipulated. The individual victims or targets of CLI fraudsters may become victims of monetary fraud, unsolicited content exposure, and personal information and identity theft. Destination network operators suffer from revenue loss, inter-operator billing disputes and customer distrust.

The 2021 Communications Fraud Control Association (CFCA) Fraud Loss Survey [1] reported CLI spoofing as the top fraud issue. Although estimates of financial loss are difficult to calculate, the CFCA-reported figure of $2.63 billion of telecom yearly revenue loss (and growing) is an indication of the scale of the problem.

2.2 Fragmentation

Many different approaches are followed in different countries around the world to fight illegal robocalls and other scam calls. These approaches include number registries with block lists that operators may use to validate the CLI during call setup as well as technical signalling controls to authenticate, secure and validate the CLI from caller to called. In parallel, various processes are used, sometimes based on regulatory enforcement, for traceback, reconciliation, and fault investigation, to identity and eliminate sources of abusive traffic.

This growing sprawl of solutions is counterproductive as a way to solve the problem of CLI spoofing for international calls:

- The solutions in different countries are not compatible with each other, which makes it difficult to build a global strategy against CLI spoofing.
- National campaigns against illegal robocalls are hindered if abusers can bypass the national protection solutions with international calls.
- Operators will be hesitant to invest in protection solutions if this fragmentation continues.

3 Problem and Solution Focus

3.1 Overview of Different Approaches

An overview of different approaches is provided in [14].

3.2 Solution Limitations

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

- Although CLI integrity solutions provide a technical means to ensure that a CLI cannot be manipulated (e.g., spoofed) without detection between the ingress point and egress point of the solution, it still may cause issues if the CLI was already spoofed before entering (garbage in – garbage out).

- CLI validation solutions can detect occurrences of manipulated CLIs, but the accuracy is dependent on the accuracy and precision of the data used for checking. More sophisticated spoofing techniques may not be detectable. However, such checks can be of help to prevent spoofed CLIs from entering a STIR/SHAKEN or Calling Name Presentation (CNAP) secure CLI transfer solution.

- Roaming status checks are needed given that incoming international calls from outbound roamers will include domestic CLIs, and thus spoofed calls cannot be detected with the CLI validation checks alone. The mobile roaming status check is needed to refine the result of a CLI validation check by checking if the incoming call from an international carrier is from an outbound roamer in another country.

4 Different Solution Approaches

Several nationally focussed approaches have been deployed in different countries. These include Do Not Originate lists, managed blocklists, and regulations on compliance with ITU-T Recommendation E.164 [3]. The **Do Not Originate** lists are used to record telephone numbers that are reserved for inbound calls. This means that incoming calls cannot have CLI assigned to the DNO lists. Often such lists include state services and emergency agencies, as well as banks and other high security phone numbers. **Managed Blocklists** are sometimes maintained at national level to filter out malicious phone numbers. A number can be blocklisted if it is known for making unwanted or spam calls. Calls from blocklisted numbers will be blocked or sent directly to voicemail, either by the recipient's phone carrier or a third-party app. **E.164** is an international standard (ITU-T Recommendation), titled "The International Public Telecommunication Numbering Plan" that defines a numbering plan for the worldwide public switched telephone network (PSTN) and some other data networks. E.164 defines a general format for international telephone numbers.

See also CEPT ECC Report 338 "CLI Spoofing" [4].

4.1 Approaches Based on a Unified Technological Framework.

4.1.1 United States of America

In 2019, the US Congress passed the "Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act" ("TRACED Act"), which went into effect the end of that year. The TRACED Act directed the Federal Communications Commission (FCC) to require the industry to develop caller-ID authentication procedures and to issue rules to protect subscribers from receiving unwanted calls or texts using unauthenticated Caller IDs.

To implement the TRACED Act, the FCC has issued several rulings, leading to the following:

- Creation of the Robocall Mitigation Database– Voice service providers in the US must register a declaration in the database that they either fully implement the STIR/SHAKEN framework or document their reasonable procedures to mitigate unwanted calls. As of September 18, 2021, US-based voice service providers can no longer accept calls directly from other US service providers not listed in the database.

- All voice service providers in the US were required to fully implement STIR/SHAKEN by June 30, 2021. This included an exemption for small service providers with fewer than 100,000 subscriber lines, originally until June 30, 2023. This deadline was later shortened to June 20, 2022. The order also included an ongoing exemption for small, non-IP providers.

- Since June 30, 2023, international gateway providers have been required to register with the Robocall Mitigation Database and to implement SHAKEN/STIR if seeking to terminate calls with North American Numbering Plan (NANP) CLIs in the US. Voice service providers in the US will be prohibited from accepting NANP CLI calls from gateways not registered with the database.

From the end of 2023, intermediate providers will be required to register in the Robocall Mitigation Database, apply SHAKEN/STIR authentication to calls that were not authenticated by the originating provider, and to apply “Know your Customer” vetting to upstream providers.

4.1.2 Canada

The solution in Canada is also based on the ATIS standards and is very similar to the solution implemented in the US. This similarity helped in the implementation of a cross-border working arrangement with the STIR/SHAKEN deployments in the US.

4.1.3 France

France’s Electronic Communications, Postal and Print media distribution Regulatory Authority (ARCEP) has implemented several standard regulations to combat CLI spoofing (E.164 + managed blocklists). Furthermore, decision *2019-0954* [5] refers to work on "STIR/SHAKEN" (see section 0) protocols as likely to form the basis of a long-term solution to meet the growing need for caller ID number authentication. To test it, ARCEP has already introduced specific ranges (for geographic, mobile and non-geographic numbers) that are dedicated to authenticated numbers.

A further addition to the act, active from 24 July 2020, specifies that operators should block calls that have a French CLI but have been routed through interconnection with an operator that normally does not provide telecommunication services to end users in Europe. Moreover, the act requires all operators to deploy some method of call authentication within 36 months. ARCEP organises workshops and seminars on the planned STIR/SHAKEN framework in France.

The latest decisions made by the MAN (Mécanisme d’Authentification des Numéros) working group chaired by ARCEP are as follows:

- STIR/SHAKEN has been selected as the preferred solution approach in France despite some initial reservations, because it is commercially available and relatively

feasible for the integration. The initial date for STIR/SHAKEN implementation was set for July 24, 2023. However, the MAN working group recognises that this technology will not be able to deal with all CLI manipulation cases and requires further development. Additional enhancements will be required post 2023.

- Cross-border: The MAN working group and French authorities recognise that CLI spoofing is a problem that requires cross-border cooperation. The need for cross-border validation of CLI"s is implicitly acknowledged, but there are no specific proposals in this area at present.

4.2 Approaches Based on Universal Specified Call Handling Procedures.

4.2.1 United Kingdom

The UK telecoms operator, Ofcom, updated its guidance [10] on the provision of Calling Line Identification in November 2022. The guidance describes how to comply with the updated 'General Conditions of Entitlement' (GCs) of the Telecommunications Act. This includes:

- making use of information that identifies numbers which should not be used as CLI, such as
  - Ofcom's numbering allocation information; and
  - the Do Not Originate (DNO) list.
- identifying calls originating abroad that do not have valid CLI and blocking them;
- identifying and blocking calls from abroad spoofing UK CLI; and
- prohibiting the use of 09 non-geographic numbers as CLI.

The updated requirements apply from May 2023

NICC (the UK's interconnect standards organisation) has published three documents covering CLI, as follows:

- NICC ND1016 – Requirements on Communications Providers in relation to Customer Line Identification display services and other related services
- NICC ND1439 – Guidance for implementing NS1016 in SIP networks.
- NICC ND1447 – Guidance on blocking of inbound international calls with UK Network Number as CLI

4.2.2 Poland

On 15 November 2022, the Polish Council of Ministers adopted a draft law on electronic communications, which will implement Directive (EU) 2018/1972 establishing the European Electronic Communications Code. The new regulations extend to conventional telecommunication businesses but also to operators of the over-the-top services. Already implemented methods of CLI validation include:

- Roaming status checks – this solution applies to terminating calls when the CLI of a mobile user is checked against its roaming status. The status is checked between

national operators and using CAMEL to verify the status of the mobile user in the outbound visited mobile network.

- Standard practices including managed blocklists and compliance with the ITU-T recommendation E.164.

4.2.3 Germany

The German Telecommunications Act 2021 (TKMG) [11] implemented a new solution for CLI validation:

- Roaming status check where all terminating calls are checked for consistency of the CLI with the roaming status. The status is checked using CAMEL (sometimes referred to as CAMEL triggering) to verify the status of the mobile user in the outbound visited mobile network.
- Additionally, Germany implements a series of standard practices: DNO for emergency and high security numbers (e.g., 112, banks); ITU-T Recommendation E.164 and managed blocklist.
- All providers of publicly available telecommunications services involved in the connection must ensure that a nationally significant number in the German number range is only displayed as the caller's number if the connection is transferred from the public German telephone network.

4.2.4 Saudi Arabia

Saudi Arabia uses a national roaming status check based on SS7 MAP AnyTimeInterrogation (ATI) request. All terminating calls will be screened, with a roaming status check request sent directly towards the operator that owns the A- number, using a SS7 ATI request and response. The chosen solution requires a direct connection between operators rather than a central solution.

The ATI response may disclose more subscriber information than necessary. An SS7 firewall at the queried operator can be used to intercept the response message to only allow the necessary information to be shared.

4.2.5 Oman

Oman uses a national roaming check status based on the SS7 MAP SendRouting Information -Short Message (SRI-SM) request. All terminating calls will be screened, with roaming status check request sent directly towards the operator that owns the A-number, using a SS7 SRI-SM request and response. The chosen solution requires states a direct connection between operators rather than a central solution.

The SRI-SM response provides less sensitive data compared to the alternative ATI response.

4.2.6 Norway

Since 2013, as specified in [9]:

- Operators are obliged to block, if technically possible and economically feasible, calls where the end user does not have rights to the A-number or where the A-number is not routable.
- The Norwegian Communications Authority (Nkom) has created an expert working group to develop legislative measures to prevent CLI spoofing and Wangiri. So far, the agreed solution for CLI validation includes call filtering including traffic monitoring and location verification.
- Further measures proposed by Nkom include guidelines for victims of spoofing, and collaboration with National Electronic Communications Industry Anti-Crime Organization to arrange regular training sessions and workshops with police authorities and operators.

4.2.7 Belgium

CLI Guidelines from the Belgian Institute for Postal Services and Telecommunications (BIPT) [7] set out four principles to ensure the validity of CLI:

- Each call must be associated with the network number. The network number is a telephone number uniquely identifying the identity of the calling line or the access point of the fixed access to the electronic communications network.
- The caller must have the right to use this number, i.e., the number has been assigned to the caller by the operator from which the call originates.
- The end user who receives any CLI must be able to call this number and a full-fledged phone call can take place.
- The number must comply with ITU-T recommendation E.164 and the BIPT-managed blocklist.

4.2.8 Latvia

According to the Latvia's national regulatory authority, CLI spoofing, or partial or full replacement of A number is considered fraud [8]. Also:

- Electronic Communications Service Providers (ECSPs) must block routing of calls or access to specific numbers if CLI manipulation has been detected (including incorrect use of numbering).
- The Latvian NRA suggests that ESCPs should specify in their interconnection agreements measures and monetary compensations to be provided in case fraud has been detected.
- The regulator has the authority to withdraw an ECSP’s rights to use numbering resources if fraudulent activity has been performed using numbering or incorrect use of numbering.

4.2.9 Australia

In 2020 the Australian Communications Alliance published “Reducing Scam Calls and SCAM SMS” Industry Code (CODE C661:2022) [6] as an amendment to earlier code of conduct.

- Article 4 defines conditions for CLI blocking which includes standard CLI compliance checks with E.164.
- Origination carriers must not send calls to international operators if an A-party CLI was not provided. And originating operators must not send calls if the A party does not have the right to use to the number.
- The code encourages operators to cooperate, and share confirmed fraudulent call data.

4.2.10 Ireland

As described in [15] (June 2023), the Irish regulator ComReg is proposing that telecommunications operators implement a number of technical interventions to combat scam calls and texts, as follows:

- Fixed CLI Blocking: To stop fraudsters abroad spoofing Irish geographic numbers (e.g., 01-xx) to make scam voice calls.
- Mobile CLI Blocking: To stop fraudsters abroad spoofing Irish mobile numbers (e.g., 087-xx) to make scam voice calls.
- A Protected number list: To stop fraudsters using numbers that are not yet in service or have yet to be allocated to a telecoms operator prior to entering service.
- A Do-Not-Originate list: Allows businesses/organisations to secure their numbers never used for outgoing calls by having telecommunications providers block calls that appear to come from those numbers.
- Voice-firewalls: To block spam calls wherever they arise (Ireland or abroad) and protect against future more sophisticated scams.

Comreg is also proposing to establish a SMS ID Registry. This would allow businesses/ organisations to register a SMS Sender ID. Telecommunications providers would then block any message bearing a Sender ID from any source other than those in the registry.

ComReg has also proposed industry implementation of a SMS scam filter to block scam SMS and protect against future more sophisticated scams, but this would require supporting legislation prior to introduction.

4.2.11 Finland

The Finnish Transport and Communications Agency Traficom adopted on 16 May 2022 an updated version of its Regulation 28 [16], [17]. It imposes new obligations on telecommunications operators to prevent caller ID spoofing and the transfer of scam calls to recipients. The objective of the updated regulation is to prevent the use of Finnish telephone numbers in international cybercrime and to reduce the number of scam calls from abroad. The obligations to prevent the use of spoofed numbers enter into force gradually: they become applicable to telephone numbers in fixed networks from 1 July 2022 and to numbers in mobile networks from 2 October 2023.

They offer two methods for validation of CLIs on incoming international calls that are suggested for the use of the operators and can be used as a significant basis for call blocking:

1. Validation of incoming calls between telecommunications operators

   a) The receiving telecommunications operator terminating international calls in which the calling party number is a Finnish mobile number performs a number portability query concerning the calling party number.
   b) If the query in step (a) is successful, the telecommunications operator checks where the calling subscriber is located at the time.
   c) Based on the above checks, the telecommunications operator decides whether the call can be connected to the called subscriber. If the checks are successful and the calling subscriber is abroad, the call can, as a rule, be connected to the called subscriber without other measures. In other cases, the call must undergo other specified measures (typically blocking).

2. Validation of incoming calls using a proxy server

   a) Information on the calling party number is sent to the proxy server. The telecommunications operator sending the request does not need to know the mobile network operator or service operator whose customer the subscriber is.
   b) The proxy server forwards the request to the correct mobile network operator that responds to the request by sending the subscriber's current roaming status to the proxy server.
   c) The proxy server forwards the response to the telecommunications operator that made the original request. Based on the information contained in the response, the operator decides whether it can connect the call to the called subscriber.

4.3 Approaches based on Technology-Neutral Recommendations/ Requirements.

4.3.1 China

The new Law Against Telecom and Online Fraud [12], is in force since December 1, 2022.

- The law enforces real time monitoring of traffic for specific call patterns that can be associated with robocalls, Wangiri traffic, and other scams. Fines can be imposed on carriers that carry through such unwanted traffic.
- Legitimate traffic must comply with the following guidelines:
  - No calls allowed with a duration shorter than 3 minutes;
  - No unsolicited marketing calls;
  - No high volume of repeated calls from the same origination (from) number within a rolling hour;
  - No calls allowed from invalid, modified, spoofed, or restricted origination (from) numbers;

- Calls must be sent from an international, non-China number when making calls to China.

4.4 Emerging regulations

4.4.1 India

See “Consultation Paper on Introduction of Calling Name Presentation (CNAP) in Telecommunication Networks” 2022 [13]. CNAP is an attempt to share calling name information between the originating and terminating operators, ensuring an adequate display of the calling party name without disrupting the traffic. This solution is in development as a response to growing customer concern about spam calls, unsolicited commercial communications (UCC) and spoofing. The proposed CNAP deployment models seek to incorporate out-of-band CLI authentication methods (see section A.3).

4.5 CLI Safe Zone

4.5.1 Background and Concept

The CLI Safe Zone is an initiative of international transit carriers through the i3forum to tackle the challenge of interworking between different national CLI validation solutions. The different solution strategies in countries and regions for CLI attestation create business risks for the participating international carriers in the i3forum:

- Declining call/answer rates for international calls, especially in countries where the trust of the CLI is being restored with the implementation of STIR/SHAKEN and other solutions.
- Cost and complexity of implementing a sprawl of solutions to comply with the varying national regulatory frameworks for the termination of international calls and in support of traceback.

The concept of the CLI Safe Zone framework is to provide a path toward inter-operability between the various national strategies, to:

- Stop declining call answer rates if there is more trust for international calls.
- Offer a better quality of service to the customers (operators) of the i3forum members.
- Offer a solution to effectively fight fraud within the international network (thus less risk of diminishing revenue caused by e.g., losses on terminating traffic rates).

4.5.2 Solution Characteristics

The CLI Safe Zone aims to provide CLI spoofing protection capabilities for the four most dominant fraud cases, i.e., Wangiri, robocalling, international revenue share fraud (IRSF) and origin-based rating (OBR) fraud/CLI refiling:

- Stateless CLI signing offers actual real-time per call detection and blocking capabilities against Wangiri, IRSF, and OBR fraud/CLI refiling practices between participating international carriers.

- Mobile status check offers real-time per call detection and blocking capabilities to defend against robocalls with spoofed mobile CLI numbers of subscribers not roaming abroad.
- The signing solution may cover more fields than solely the CLI to exclude other unauthorised manipulation of signalling information within the IPX domain.
- Although call signing does not protect against frauds in sending operator networks (garbage in – garbage out), the identity of the sending network will be known for traceback and reconciliation.
- More sophistic heuristics like number portability data and data analytics may be added by the participating international carriers to protect in real-time against external fraud practices.
- Key management will need careful evaluation to balance political, technical and scalability issues.
- The per call protection solution will not disrupt and impact the business and interconnection practices of the participating international carriers:
    - No disruption of the present international inter-carrier business model based on freedom of choice for operators with least cost routing, volume pricings, etc.
    - No disruption to the existing technical interconnects because of their backward compatibility support.

5 Unintended or Unforeseen Effects Regulation/ Solutions on External Parties

Issues may arise for service providers and/or customers outside the jurisdiction of regulation and/or solutions implemented for the purposes of CLI spoofing prevention. These include (but are not limited to):

- Call can be blocked before reaching the intended customer due to an invalid CLI;
- The CLI can be removed from the call;
- “Likely spam” or similar warnings can be displayed;
- Traceback requests can be received from the regulators / interconnect partners.

Some of the measures an operator can undertake to overcome these issues may include:

- Aligning least cost routing settings with the regulations applied at different terminating destinations;
- Running analysis on CLI delivery to the affected destinations either via direct interactions with the interconnect / roaming partner or specialised tools;
- Working with (enterprise) customers to ensure correct understanding of the regulations affecting their traffic;
- Participating in solutions / initiatives protecting calls from CLI manipulation. However, one needs to understand the limitations of such solutions / initiatives;

- Investigate representation of CLIs for calls of roaming customers;
- Protect numbering resources including unassigned numbers; protect networks from PBX hacking scenarios.

Annex A Different Methods and Technologies of Detecting and Blocking Calls with Spoofed CLIs

A.1 General Methods

A.1.1 "Do Not Originate" (DNO) lists.

DNO lists are lists of numbers that should not originate traffic. These lists are intended to be used to identify and block traffic where the caller ID has been spoofed.

DNO list data may be gathered from multiple sources, including:

- Invalid numbers within the national numbering plan
- Unallocated numbers
- Numbers that are valid but have been designated as terminating only.
- Number identified and blocked as known sources of fraudulent or nuisance traffic.
- Numbers that have been disconnected or in the process of reallocation.

Some national regulators maintain and publish DNO lists or specify the requirements for operators to maintain a compliant DNO list.

Blocking or rejection of calls or messages that have a CLI found on a national DNO list is now mandated by regulators in an increasing number of countries as a mechanism to mitigate against scams and nuisance traffic (often referred to as robocalling) and is applied to calls within a country and also at international gateways.

A.1.2 Managed Blocklists

In several countries blocklists are coordinated either via governmental agencies or based on industry initiatives. Operators are to consult these lists and block calls that have a blocklist entry as A-number.

In additional, managed data sets with fraudulent numbers are offered by specialized vendors and by some organizations. Operators may use these data sets in their campaigns against various fraud and nuisance calls involving international calls.

A.2 In Band Methods

A.2.1 Original STIR/SHAKEN (US)

Signature-based Handling of Asserted information using toKENs (SHAKEN) is an end-to-end CLI authentication and attestation architecture defined by the IP-NNI task force, which is a joint task force of the Alliance for Telecommunications Industry Solutions (ATIS) and the SIP Forum. SHAKEN includes a profile of technologies developed by the Internet Engineering Task Force (IETF) Secure Telephone Identity Revisited (STIR) working group, as well as a governance framework. These are often referred to collectively as “STIR/SHAKEN.” The US deployment of STIR/SHAKEN technologies and governance is called Secure Telephone Identity (STI).

STIR/SHAKEN allows SIP-based network service providers (SPs) to attest to the calling numbers associated with calls, as well as the SP's confidence that the caller is authorized to make calls from that number. That attestation takes the form of a Java Web Token (JWT) extension known as a "Personal Assertion Token" (PASSporT). A SHAKEN PASSporT contains, among other fields, the origination and destination identities (typically telephone numbers) for a call, a creation timestamp, signature algorithm, an attestation level, and a link to the SP's STI-Certificate. The originating SP's (OSP's) STI-Authentication Service (STI-AS) signs the PASSporT with the private key associated with the signing certificate and imbeds the serialized PASSporT and signature in a SIP Identity header field.

The SHAKEN PASSporT attestation level can take one of 3 values:

- Full (A) Attestation: The OSP is responsible for originating the call onto the IP-based SP voice network, has a direct authenticated relationship with the caller, can identify the caller, has established that the caller is authorized to use the calling number.
- Partial (B) Attestation: The same as "Full" attestation, except that the OSP has not established that the caller is authorized to use the calling number.
- Gateway (C) Attestation: The OSP has no relationship with the call originator, for example, calls originated via international gateways.

When the terminating SP (TSP) receives a call with a SHAKEN PASSporT, it's STI Verification Service (STI-VS) verifies the signature. It may also perform other Call Validation Treatments (CVT) according to local policy. If these are successful and the PASSporT indicated "A" attestation, the STI-VS may insert a "verification status" (verstat) parameter into the SIP request to indicate to the end-user device that the call has been verified.

With the exception of the "verstat" parameter, STIR/SHAKEN only defines behaviour for the network-to-network interface (NNI). It does not define the user network interface (UNI). In particular it does not define how an OSP authenticates callers. The UNI may be defined by other specifications, such as the SIP Connect specification from the SIP Forum.

The STI framework is governed by the following entities:

- STI Governance Authority (STI-GA) -- Defines policies and procedures that govern which entities can acquire STI certificates, manage the PKI, and issue certificates.
- STI Policy Administrator (STI-PA) – Implements STI-GA policies, manages the list of approved STI-CAs, distributes CA certificates and CRLs, and issues Service Provider Code (SPCs) tokens.
- STI Certification Authorities (STI-CAs) – Act as root CAs for the STI PKI and issue STI certificates to STI Participants.
- STI Participants – Receive STI Certificates from STI-CAs. Typically, STI Participants are network operators, but there are exceptions. An STI participant must be issued an SPC token by the STI-PA to receive a certificate.

The current US SPC access policy requires the entity to have a 499A form on file with the FCC or have proof of payment of an annual Responsible Organization (RespOrg) fee, have been assigned an Operating Company Number (OCN) or RespOrg ID, and have certified

with the FCC that they have implemented STIR/SHAKEN or comply with the Robocall Mitigation Requirements.

The core specifications for SHAKEN/STIR are in the following documents:

- ATIS-1000074.V003 – ATIS Standard on SHAKEN
- ATIS-1000080.v005 – SHAKEN Governance Model and Certificate Management
- ATIS-1000084.v002 – Operational and Management Considerations for STI-CAs and PAs
- RFC 8224 -- Authenticated Identity Management in the Session Initiation Protocol (SIP) [STIR]
- RFC 8224 – Personal Assertion Token [PASSporT]
- RFC 8226 – STIR Certificates
- RFC 8588 – SHAKEN PASSporT Extension

A.2.1.1 Strengths

- STIR/SHAKEN provides strong end-to-end authentication of CLI and attestations about the caller's authorization to originate calls from a number. There can be any number of IPX or other IP-based entities between the OSP and TSP without compromising this authentication.
- It provides strong traceback to determine sources of prohibited calls.
- Standards based.
- It has well-established deployments.
- The US FCC strongly supports it.

A.2.1.2 Weaknesses

- It needs careful screening of the incoming CLI as STIR/SHAKEN works on the basis of 'garbage in, garbage out'. So, any false CLI entering the system becomes undetected.
- Its use is limited to end-to-end SIP-based IP networks. However, there are efforts in the ATIS Non-IP Call Authentication (NIPCA) task force to mitigate this limitation (see OOB STIR/SHAKEN description in A.3.1)
- It may cause problems with IP interconnects that do not implement Transmission Control Protocol (TCP) or that modify SIP messages in certain ways.
- It is not a complete solution. Instead, STIR/SHAKEN helps to enable other policies and procedures to mitigate unwanted calls, such as filtering, labelling, and traceback.
- It has limited support for federation among different governance jurisdictions. ATIS-1000087 describes an initial mechanism for cross-border SHAKEN that uses merged Trusted CA lists. The IP-NNI task force recognized that this approach is cumbersome and reopened ATIS-1000087 for updates on 16 March 2023.

A.2.1.3 Where used.

The “original” STIR/SHAKEN is currently deployed in the US and Canada.

A.2.2 STIR/SHAKEN solution in France

The implementation of STIR/SHAKEN in France should be ready for operational launch by July 25th, 2023. During the initial phase it is only for calls in France and no actions are planned yet for incoming international calls.

The solution is intended to be completely IP-based with only SIP interconnections. No Time Division Multiplexing (TDM) overlay solutions are considered. The STIR part is based on ATIS-1000082 like in the US and Canada.

The SHAKEN part is very different and simpler than the approaches used in the US and Canada:

- There will only one Certificate Authority that will also manage a single Certificate Registry, so no distribution is needed in each operator.
- The interface for certificate management will not use Automated Certificate Management Environment (ACME) but a French specific IT-friendly REST-based interface.
- To simplify initial deployments and recovery schemes, an operator will be able to download a file with all the certificates so that it can prepopulate its cache.
- No use will be made of delegated certificates. Instead, operators will use indirect certificates for signing calls from other operators that have no direct access to the STIR/SHAKEN network.

This STIR/SHAKEN regulation in France comes with strict call treatment instructions for operators:

- An unsigned call or with an incorrect identity header will have to be dropped, excluding non-SIP calls and emergency numbers.
- In the future only calls with attestation A will be authorised. B and C attestation calls will also be dropped.

Future extensions are planned to cover incoming international calls, prevention of spoofed diverted calls (IETF DIV) and priority calls (IETF RPH), and the support of delegate certificates.

A.3 Out of Band Methods

A.3.1 OOB STIR/SHAKEN

A.3.1.1 Introduction

Out of Band (OOB) SHAKEN enables CLI attestation and verification, through only requiring the originating and terminating operators to support this technology. In addition, it does not require any support from the transit carriers in the call path.

Overall, the technology requirements and cost/effort to implement would be typically less than traditional in -band STIR/SHAKEN. In addition, there would be no obligations on transit operators.

OOB can be used in many situations that would be more challenging to implement for traditional in-band STIR/SHAKEN e.g., TDM transit, international calls (with unknown or hybrid IP / SS7 transit). Future capabilities such as rich call data – branded caller name, branded logo etc. are likewise feasible under OOB.

A.3.1.2 Technical Implementation

OOB uses a real time matching between the originating operator and the terminating operator (or relevant entities on their behalf). Each operator confirms its role in the call to the other, i.e., that a call with Caller ID X and termination number Y has been generated by the originating operator and received by the terminating operator. Solutions of this nature are commercially available.

The Out of Band SHAKEN specification is specified by ATIS in ATIS-1000096. The specification does not take away SHAKEN obligations from the originating service provider (OSP) and the terminating service provider (TSP).

In the SHAKEN architecture, the STI-AS adds the PASSporT to the SIP signalling. This PASSporT is verified by the terminating service provider using the STI-VS and an optional Call Validation Treatment (CVT). However, the intermediate networks may or may not support SIP signalling for transit and may use TDM interconnections along their transit paths. Hence OOB capabilities are necessary.

OOB signalling preserves the key STIR/SHAKEN capabilities such as STI-AS, STI-VS and attestation levels for appropriate presentation (green tick etc) to the receiver of the call.

To satisfy OOB, a few new components are added to the SHAKEN framework:

- STI-CPS (Call Placement Server) - This is an entity that can receive a PASSporT from a service provider for eventual retrieval by another service provider responsible for onward transit or termination. These can exist alone or as a network of STI-CPS that allows for exchange of PASSporTs within the network.
- STI-OOBS (Out of Band Service) - This service is an entity in a service provider’s network that publishes the PASSporTs to the STI-CPS.
- STI-IWF (Inter Working Function) - This is a component that performs SIP-TDM signalling and vice versa.

The architecture is as shown in Figure 1 below:

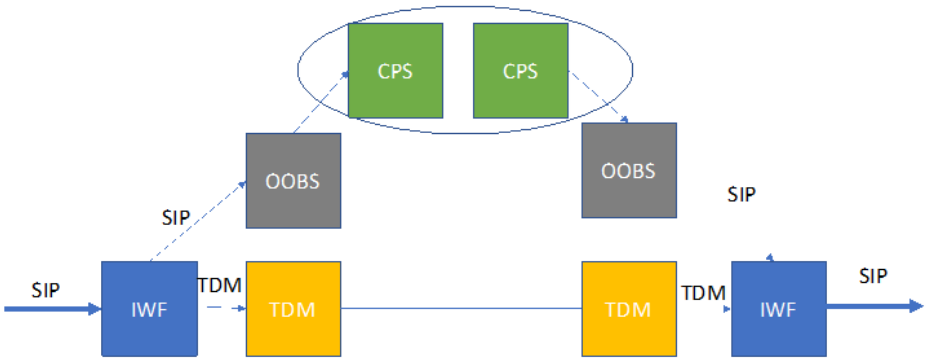

Figure 1 – OOB STIR/SHAKEN Architecture

A.3.1.3 Future Roadmap

Standards are being developed to support efficient interworking (such as broadcasting, peering or federation) between different CPS entities, enabling multi-vendor implementations where originator and terminator are utilising different OOB vendors.

For policy administrator (PA) and governance authority (GA) functions – for international calls, where originating or terminating jurisdictions do not (yet) have country level established STIR/SHAKEN PA/GA functions, there is potential for a global PA/GA function, to be governed by preferably a neutral global industry association (i.e. not for profit) – preferably aligned, where possible, to existing national regulated structure such as existing NRA organized number plan allocation to NRA recognized operators.

For more details, see ATIS-1000096 “SHAKEN: Out-of-Band PASSporT Transmission Involving TDM Networks”.

A.3.2 AB Handshake

The AB Handshake patented call validation solution performs out-of-band end-to-end validation of calls in real time. It enables operators to validate every call, originating from or received by its subscribers.

The AB Handshake call validation solution requires both originating operator A and terminating operator B have an AB Handshake Call Registry installed. In order to participate, each operator needs to provide its E.164 range and the IP addresses of its Call Registry. All required data is uploaded to the Central Participant Database (CDB), distributed among all the participating Call Registries. The CDB is currently managed by AB Handshake Corporation but could be transferred to a neutral and trusted organisation. For the purpose of call validation, AB Handshake facilitates an encrypted channel between each Call Registry A and Call Registry B.

The real time validation of traffic takes 5 main stages:

- When an international call is initiated the originating operator sends call data (A, B numbers and ‘Start of the Call’ message) to the call registry A;

- As soon as the call is received, the terminating operator sends call data to call registry B for validation;
- Both registries reach out to each other through an encrypted channel to match call details;
- Results of this comparison are processed by the fraud detection logic units in the corresponding Call Registries to see if any manipulation took place and call details are valid;
- If fraud activity is detected or call details do not match - the BLOCK command can be initiated in real time.

A.3.2.1 CLI Spoofing Detection Example

- A fraudster uses a number assigned to Operator A to send a call to Operator B;
- A and B numbers and the call start event timestamp are sent to Call Registry B;
- Call registry B sends a call validation request to Call Registry A;
- Call Registry A does not find the matching call data;
- Call Registry A notifies Call Registry B that call details DO NOT MATCH;
- Call Registry B sends an alert and/or BLOCK command to the network of Operator B.

A.3.2.2 Strengths

- Works with any type of network and interconnect.
- Does not require any intermediate carriers to be a part of the solution.
- A combination of push and pull models makes sure validation is triggered for any call.
- The originating operator has full visibility on whether the call was delivered with the correct CLIs.
- No bilateral communication is required between participants.

A.3.2.3 Weaknesses

- 100% integration with the traffic of a given operator is required to run the solution.
- Proprietary technology

A.3.3 Caller ID Verification (CIV) - Warwick University

Academics at the University of Warwick have proposed a solution entitled ‘Caller ID Verification’ (CIV) [2]. They claim this overcomes the perceived risk of other trusted third-party solutions such as STIR/SHAKEN.

The fundamental methodology of CIV is as follows:

1. A calls B;
2. B verifies A’s CallerID by placing the initial call on hold and making a verification call to the A-number. The CallerID on this verification call is especially crafted to include a PIN;

3. The verification call is not answered by A, but the CallerID of the verification call is noted and then sent by A when the initial call it is taken off hold;
4. B determines if the challenge and response match and so indicates the CLI as either 'verified' or 'unverified'.

If it is not possible to send the PIN as a modification of the CallerID on the verification call, then the proposal is for the challenge call to be answered and the PIN sent by DTMF in-band.

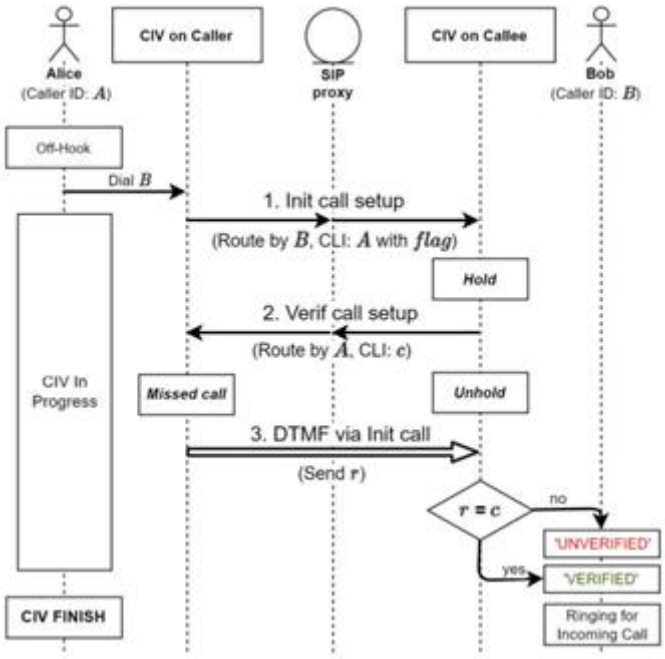

Figure 2 - Caller ID Verification (CIV)

A.3.3.1 Strengths

- No changes would be needed by the A party's network operator or transit operator.

A.3.3.2 Weaknesses

- Additional delay in call establishment
- Additional network resources used for the unsuccessful or 'short duration' verification call.
- 'A' party will need Call Waiting provisioned to receive an indication of the verification call.
- 'B' party's network operator would need to provide the B party with the ability to modify part of their CallerID, which is itself a security vulnerability.
- For mobile devices, it would require collaboration with the large mobile OS vendors to either support the solution in the OS or to provide the appropriate API calls to the application.
- For fixed line telecommunications, special devices would need to be purchased by both the A and B party.

- The solution will not work well when the A party is a call centre.

A.3.4 Consistency Checks of Voice Call Messages

This solution enhances the protection against CLI spoofing on incoming international voice calls. The target of this solution is to combat scammers who have found a way to bypass the existed CLI protection by spoofing the mobile numbers of home subscribers who are roaming abroad (outbound roamers).

A.3.4.1 Solution Description

The objective of this solution is to perform consistency checks of the call information before the call setup, by comparing the call information on the incoming international SS7 signalling message using (PSI, SAI or CAMEL O-CSI) as triggered from the visited MSC, with the information of IAM/INVITE message (CgPn=A, CdPn=B) of the same incoming international voice calls.

The legitimacy of such calls will only be confirmed if this SS7 signalling message was genuinely triggered from the visited MSC's VPMN towards the subscriber’s home network.

To support this enhancement, this incoming international SS7 signalling message has to be cached for a configurable period of time, and then the consistency checks to be performed against the information of IAM/INVITE message (CgPn=A, CdPn=B) of the incoming international voice calls.

Based on the consistency check result a verdict is generated in order to block or allow the call.

A.3.4.2 Strengths

- Easy to implement, it does not require major development on the network.
- This solution provides fraud detection for home subscribers even with mobile number portability scenarios.

A.3.4.3 Weaknesses

- This solution only works for calls that use SS7/CAMEL signalling, and not on purely IP calls.

A.4 Supplementary Solutions

A.4.1 Roaming Status Check

The roaming check principle is based on screening all international incoming calls to verify whether a domestic mobile number presented in the CLI is registered as in roaming state or not.

This applies to mobile numbers only. Fixed numbers need to be handled separately with separate logic. A common approach is to block all international incoming national fixed numbers and handle exceptions with a whitelist approach.

For each international incoming call, the MSISDN or IMSI should be checked against the HLR to receive the current roaming status. There are different options depending on the result.

- If the roaming status is “yes”, the call should be allowed to terminate as normal.
- If the roaming status is “no”, the operator can choose to either reject the call, or blank out the CLI and where possible, mark the call as “not safe”. In some countries regulators may dictate which action to take when the response of the roaming status check is negative.

If the number belongs to another operator within the country, the query can be directed either:

- Directly to each individual operator who owns the number. This requires an API to each existing operator in the country.
- To a central DB/proxy, which directs the query to the operator that owns the number. This only requires a single API to be setup between the operator and proxy.
- The solution is described in GSMA PRD FS.21 section 15.2 “CLI Spoofing Check” based on the SS7-SM or SS7-ATI checks, alternatively API-based solutions can be considered. The implementation of the SS7-SM or SS7-ATI checks is relatively simple given that use can be made of standardized SS7 signalling procedures for the queries between the adjacent mobile networks.
- The API-based procedures require more specification effort between the collaborating mobile operators. It offers the advantage that the solution is signalling protocol agnostic (not dependent on SS7) and may include additional checks performed by the mobile operator serving the subscriber of the CLI.

The ECC has also identified example call scenarios in which incoming international voice calls would be received with national numbers as CLI. In such scenarios, roaming status and identification of MSRNs could be used for validation. See Draft ECC Recommendation (23)03 [18].

The implications of home routing and 5G standalone remain for further study.

A.4.1.1 Strengths

- Implementation can be incremental. A partial solution and logic can first be built to handle incoming traffic received a CLI from a network’s own assigned numbering range. The solution can subsequently be extended to include other national operators.
- Standard SS7-SM or SS7-ATI queries can be used.

A.4.1.2 Weaknesses

- Increased load of queries in the network and increased latency before the call can be connected.

- Security is essential and subscriber information must be treated carefully in the information exchange between the operators so that sensitive information is not revealed.

A.4.2 CDR analysis

CDR analysis can be used to detect cases of CLI spoofing cases based on comparing the data against databases / numbering plans, applying custom rules based on thresholds or previous experience or direct comparing of CDR data with an interconnect partner. This can be carried out manually or using automated solutions. As a result, the operator can identify the number of spoofed calls in the network, the ranges/numbers used for the delivery of such traffic as well as (in case of participation of the interconnect partner) - the true origin of the traffic. This also allows the operator performing the analysis to establish the financial effect of the spoofing in case it used for OBR bypass.

A.4.2.1 Strengths

The involvement of an interconnect partner in the analysis allows an operator to achieve a very high detection accuracy, providing visibility on both the number used for spoofing and the original CLI attached to the call.

A.4.2.2 Weaknesses

The CDR analysis is a non-real time method, making CLI spoofing prevention impossible. In case of cooperation with an interconnect partner this needs to be a joint activity requiring consent and allocation of resources from the partner.

Annex B Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	2 Oct 2023	First version	Dmitry Sumin, ABHandshake

Contributors / Reviewers
Ben Campbell, Akayla
Abdulmajeed A. A Aleid, STC
Nicolaj Aaröe, Tele2
Pieter Veenstra, Titan.ium Platform LLC
Simon Sporton, Vodafone
Tim Ward, XConnect