CEPT ECC
Electronic Communications Committee

ECC Report 338

CLI Spoofing

approved 7 June 2022

0 EXECUTIVE SUMMARY

Calling Line Identification (CLI) spoofing has been increasing during the last years and one of the main reasons is that such practices are facilitated by the migration to IP-based networks. Nevertheless, in most countries one still finds traditional networks and IP-based networks co-existing, and for that reason it is difficult to find a singular solution that would solve all the problems of CLI spoofing. In this regard, this Report reviews current regulatory practices across multiple jurisdictions and different technical practices to combat CLI spoofing. It then proposes a two or three stage approach to rolling out solutions which may be considered.

For the short-term, traffic pattern analysis may reduce some of the problems, but it is not generally a real-time solution. At both the national level, and within international/regional fora such as ITU or BEREC, CEPT administrations should promote industry groups to facilitate discussions on traffic analysis and information sharing to combat CLI spoofing. Also, regulatory requirements should require that user provided CLI is validated by the originating service provider, for instance to check if the CLI is to be overwritten or to block the communication. Other requirements may also be imposed on transit service providers.

In the mid-term, national solutions may be implemented, pursuing, as a minimum, that domestic calls are more reliable than nowadays. Nevertheless, since termination charges for calls originating outside the EU are typically higher, there needs to be a mechanism that prevents calls being presented as originating from within the EU when they actually originate from outside, to avail of the lower charges which affects EU operators' revenues.

As a long-term solution, techniques such as Secure Telephone Identity Revisited (STIR)/Signature-based Handling of Asserted information using toKENs (SHAKEN) or any other technique could be implemented. STIR is intended to facilitate the verification of the calling party’s authorisation to use a particular number, in that phone numbers are attested and signed at call origination and verified at call termination. However, such techniques generally require an all-IP environment, and it is expected that networks may need several years to get there from now.

TABLE OF CONTENTS

LIST OF ABBREVIATION

Abbreviation	Explanation
A2P	Application-to-Person
ARCEP	France's Electronic Communications, Postal and Print media distribution Regulatory Authority
ATIS	Alliance for Telecommunications Industry Solutions
BEREC	Body of European Regulators for Electronic Communications
BIPT	Belgian Institute for Postal Services and Telecommunications
CEPT	European Conference of Postal and Telecommunications Administrations
CLI[1]	Calling Line Identification
CPN	Calling Party Number
CRL	Certificate Revocation List
CVT	Call Validation Treatment
DDI	Direct Dialling In
DLT	Distributed Ledger Technology (e.g. Blockchain)
ECC	Electronic Communications Committee
ECNO	Electronic Communications Network Operator
ECSP	Electronic Communications Service Provider
EECC	European Electronic Communications Code
ePR	ePrivacy Regulation
ETSI	European Telecommunications Standards Institute
EU	European Union
FCC	Federal Communications Commission
GDPR	General Data Protection Regulation
GMSS	Global Mobile Satellite System
GW	Gateway
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Service Digital Network
ITAKT	Norwegian National Electronic Communications Industry Anti-crime Organisation
ITU-T	International Telecommunication Union Telecommunication Standardisation Sector
LEA	Law Enforcement Agency

[1] In this document, CLI is also used to refer to other originating identifiers

Abbreviation	Explanation
Nkom	Norwegian Communications Authority
NP	Number Portability
NRA	National Regulatory Authority
PBX	Private Branch Exchange
P2P	Person-to-Person
PSTN	Public Switched Telephone Network
RFP	Request for Proposal
ROA	Recognised Operating Agency
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SMPP	Short Message Peer-to-Peer
SMS	Short Message Service
SPC	Service Provider Code
SOLID	Social Linked Data
SS7	ITU-T Signalling System No. 7
STI	Secure Telephone Identity
STI-AS	STI - Authentication Service
STI-CA	STI - Certification Authority
STI-GA	STI - Governance Authority
STI-PA	STI - Policy Administrator
STI-VS	STI - Verification Service
STIR	Secure Telephone Identity Revisited
TKG	Telekommunikationsgesetz
USD	Universal Service Directive
VoIP	Voice over IP

1 INTRODUCTION

The origination, transit and presentation of Calling Line Identification (CLI) digits in the Public Switched Telephone Network (PSTN) was traditionally the sole responsibility and custody of the Electronic Communications Network Operators (ECNO) and the possibility of manipulating CLI digits was remote and required specialised equipment. This secure environment promoted trust in the CLI digits presented to end-users for voice and messaging services and the supply chain extended from the originating network, through a transit network if needed, to the terminating network.

The transition from legacy networks has transferred intelligence to the network edge and more sophisticated end-user devices and applications have empowered end-users with the ability to manipulate CLI digits thereby extending the supply chain well beyond the traditional players. At the same time, many new, and typically smaller, operators who are less familiar with the concept of CLI have been seen, appearing on the market who also offer voice and messaging services based on Internet Protocol (IP).

These developments imply that as the "chain" for handling the calls/messages from the originating party to the receiving party becomes longer and more complex, it has become more difficult to maintain the integrity of the CLI.

Clarity on the CLI rules is important for the market. This is the main objective of the ECC Recommendation (19)03 "Measures for increasing Trust in Calling Line Identification and Originating Identification" [1] which contains measures to increase trust in the CLI.

ECC Report 248 "Evolution in CLI usage – decoupling of rights of use of numbers from service provision" [2] contains further information on flexible CLI usage, which has advantages for end-users when it is not used with malicious intent. This Report recommends that CLI validation techniques should be made mandatory. The alternative operator should provide validation measures ensuring that the end-user has the right to use the number presented as CLI.

Based on ECC Report 275 "The role of E.164 numbers in international fraud and misuse of electronic communications services" [3], CLI spoofing is a technique that enables the originating party, originating network and/or transit network to manipulate the information displayed in the CLI field with the intention of deceiving the receiving party into thinking that the call/message originated from another person, entity or location. CEPT countries observe more and more instances of consumer harm through CLI spoofing. Different fraud cases based on CLI spoofing have been explained in ECC Report 275. Fraudsters use CLI spoofing to take advantage of the inherent trust that end-users have in the integrity of CLI information. Normally, the CLI presented is a national geographic or mobile E.164 number with a format that the receiving party would be familiar with. With CLI spoofing, the number displayed could be an assigned number, an unassigned number or a number that does not exist in the national numbering plan.

More recently, and related with a trend leading towards lower mobile and fixed termination rates inside the EU, CLI manipulation has been used by non-EU country operators and EU transit operators where calls or messages originate from numbers of non-EU countries, in order to take advantage of lower intra-EU terminations rates (bypassing higher termination rates).

Clarity on the rules is important but is not enough to deter some actors who deliberately manipulate CLIs to mislead end-users. Due to the complexity of the international voice telephony and messaging systems, it is difficult to identify and to sanction these bad actors. Therefore, additional measures must be considered.

In this Report, the different solutions will be addressed, pros and cons, the operational impacts of the different solutions to mitigate the effects of spoofing, roll out aspects and international aspects. This is in line with ECC Report 275, section 11.1.

To end, and for the sake of clarity: the average user does not necessarily see the difference between a call or message with a "correct" (i.e. valid and legitimate) CLI and a “trustworthy” call or message. Using technology, it is possible to ensure that CLIs can obtain a certain level of trust but that does not necessarily mean that the originating party has good intentions.

2 SCOPE

The scope of ECC Report 275 was limited to cases of CLI spoofing where end-users are the victims. In this Report, the ECC recognises that operators can also be negatively impacted and that the issues that arise are relevant to voice calls as well as messaging services (e.g. SMS).

Indeed, the use of E.164 numbers and short codes as CLI has also emerged and grown for messaging services such as Short Message Service (SMS). For routing and transmission of CLI information, SMS service providers typically make use of both ITU-T Signalling System No. 7 (SS7) and IP-based protocols (e.g. Short Message Peer-to-Peer (SMPP)) which increases the number of actors in the supply chain that can modify the CLI field. The innovative use of SMS in recent years, particularly in the area of business-related SMS services has increased. The use of alphanumeric characters in the CLI field has increased significantly. In smartphones, hyperlinks can be included in the content of SMS and other messaging types which can lead to an increase in phishing scams and to attract call-backs to high-tariff numbers.

Notwithstanding, this Report examines and evaluates regulatory initiatives and technical solutions to tackle CLI spoofing only related to voice calls.

3 DEFINITIONS

Term	Definition
CLI spoofing	A technique that enables the originating party and/or any network operator handling the call or message to manipulate the information displayed in the CLI field with the intention of deceiving the receiving party or the network operators intervening in the handling of the call or message into thinking that the call or message originated from another person, entity or location.
Originating party	Party that initiates the communication (call or message).
Receiving party	Party that receives the communication (call or message).
Recognised Operating Agency	Any operating agency, which operates a public correspondence or broadcasting service and upon which the obligations provided for in Article 6 of the ITU Constitution are imposed by the Member State in whose territory the head office of the agency is situated, or by the Member State which has authorised this operating agency to establish and operate a telecommunication service on its territory.
Wangiri	Wangiri (or ping calls) is a technique where the fraudster originates, usually via an automated technique, high volumes of very short call attempts to a whole range of numbers. When the attack happens through calls, these calls are dropped after one or two rings so that they appear as missed calls on the end-user's display.

4 CURRENT REGULATORY PRACTICES TO COMBAT CLI SPOOFING

Many countries have introduced regulatory practices intended to disrupt and combat CLI Spoofing. A number of these practices are examined below.

4.1 APPROACH IN BELGIUM

4.1.1 CLI guidelines

On 4 December 2020, the Belgian Institute for Postal Services and Telecommunications (BIPT) published the CLI guidelines. With this publication the BIPT wishes to, in addition to decreasing fraud, provide the sector and the end-user with more clarity as regards CLI use and presentation, from the moment a call is initiated until the time the call is terminated. That is why the BIPT puts forward four principles governing call routing, aiming at safeguarding the CLI's veracity and at increasing the CLI's reliability.

The first principle the BIPT puts forward is that each call has to be associated with a network number. This network number identifies the call's origin. It is a telephone number corresponding to the line (in case of a fixed network) or connection (in case of a mobile network) between the user and the public electronic communications network. The user-generated CLI identifies the caller and is optional. For want thereof, the CLI shall be the same as the network number.

The second principle states that the network number identifies the calling connection (of an individual or an organisation**)** in a unique manner. The caller has to be entitled to use this number as the number was assigned to the caller by the operator originating the call.

The third principle is that the presentation number has to be dialable. This means that the end-user receiving such a CLI, has to be able to dial this number himself, setting up a fully-fledged telephone call.

The fourth principle is that the network and presentation numbers have to be valid. A valid number is a number that complies with the international public telecommunication numbering plan (Recommendation ITU-T E.164) and that, for Belgian numbers, comes from a number block assigned by the BIPT in accordance with the terms of Art. 4 of the Numbering Royal Decree. Furthermore, the number has to be assigned - possibly through sub-assignment - to the end-user. To be perfectly clear, it is not allowed to use a telephone number from a number block that was not assigned by the BIPT to an operator.

4.1.2 Blacklist

Certain geographical numbers (e.g. from banks) are especially sensitive to CLI spoofing with a view to phishing fraud for instance. To fight CLI spoofing coming from abroad, the BIPT has proceeded to drafting and keeping a list of geographical numbers susceptible to fraud ("blacklist"), the end-users of which (e.g. from banks) can explicitly request to be included in the list. The main Belgian operators use such a "blacklist" to block calls with these CLIs originating abroad. The actual terms and conditions and processes are developed further within the BIPT Anti-Fraud Working Group.

4.2 APPROACH IN FRANCE

France's Electronic Communications, Postal and Print media distribution Regulatory Authority (ARCEP) has taken several decisions throughout the years to combat CLI spoofing. The first one was taken in 2012 [13] in order to prevent Wangiri from premium rate numbers and ended by forbidding the use of premium rate numbers (starting in France by 089) as a CLI.

Then, ARCEP modified in 2018 and in 2019 its current decision regarding the French numbering plan. In these decisions, some recommendations have been made to reduce fraudulent calls using spoofed CLIs:

- for calls or messages with a French geographic or non-geographic number received through an international interconnection (outside the EU), ARCEP concluded that it is justified that operators are allowed to block the routing of these calls or messages;

- for calls or messages sent from automated systems (national and international), it is forbidden to use mobile numbers as a CLI from 1 August 2019. The same interdiction will be in place for geographic and fixed non-geographic numbers from the 1 January 2021. A dedicated numbering range is available for calls and messages from automated systems;
- the phone number used as a CLI must be a part of a range assigned by ARCEP, a number assigned by an operator to an end-user and the number must allow, during the period of assignment of the phone number, to contact the user who made the call or message.

ARCEP has also, in the same decision, forbid the sub-assignment of new numbers for non-geographic and mobile numbers since 1 August 2018 (it will become effective for geographic numbers 1 January 2023), and asks each year every French operator to give the list of every sub-assigned number.

In order to check the implementation of these recommendations, ARCEP invites the operators to regularly provide information about the different implementations, the number of calls blocked and their origins. For example, in December 2019, the French incumbent operator (Orange) publicly indicated that it had blocked 111 million of calls from abroad during the period of September 2019-November 2019 [14].

The French decision of 2019 [15] also evokes STIR/SHAKEN as a long-term solution. In order to test it, ARCEP has already introduced specific ranges (for geographic, mobile and non-geographic numbers) which are dedicated to authenticated numbers. Furthermore, a French law aiming at tackling fraudulent calls has been enacted on 24 July 2020, as the outgrowth of an almost two-year effort. It requires operators to block calls and messages with a French CLI received through an interconnection with an operator that does not provide telecommunications services to end-users in Europe by 24 October 2020. Some exceptions apply for international roaming or a potentially specific range for toll-free numbers. The law also requires all carriers to implement technologies to authenticate CLI information, preventing call spoofing, within 36 months. Relying on this legal framework, ARCEP organises workshops with operators to discuss the opportunities and the best way to deploy the STIR/SHAKEN framework in France.

ARCEP is aware that STIR/SHAKEN only works through IP interconnections but, in its latest market analysis decisions for the markets 1 and 2, ARCEP has stated that any request of an IP interconnection from an originating operator was necessarily considered reasonable from 1 July 2015 for the metropolitan area [16] and from 1 July 2018 for the overseas territories [17]. While monitoring progress on legacy network support, from ARCEP's point of view, it is therefore reasonable to work on a long-term mechanism working only through IP interconnections. In addition, the French incumbent operator has already planned the end of PSTN and Integrated Service Digital Network (ISDN) networks in the next years so ARCEP expects that the traffic sent through SS7 interconnections will quickly decrease.

4.3 APPROACH IN GERMANY

4.3.1 Legal situation before 1 December 2021

German legislation previously included certain limited provisions regulating the respective rights and obligations for the transmission of numbers when setting up outgoing telephone calls.

Subsection 1 of the relevant provision – section 66k of the German Telecommunications Act (Telekommunikationsgesetz – (TKG)) – dealt with the network-generated number and the respective obligations of the telecommunications service providers involved in the call; subsection 2 dealt with the "generic number" that the calling party can send in addition to the network-generated number. Passing on the generic number in violation of the provisions of section 66k(2) TKG is known as "caller ID spoofing".

Although the Federal Network Agency in Germany, Bundesnetzagentur, as the national regulatory authority, was entitled to exercise the rights conferred on it by section 67(1) sentence 1 TKG, it was hardly ever able to take the necessary remedial measures. With this particular type of fraud, it is necessary to identify the person responsible for the fraud in order to remedy any violation. However, although the Bundesnetzagentur was the body responsible for implementing and enforcing the provisions of section 66k TKG, it was not equipped with the necessary means and powers to do so. Above all, it was not provided with the power to investigate and thus identify the person responsible.

4.3.2 Current legal situation

A revised TKG came into force on 1 December 2021 [18], in which the German legislator – among other things to improve the situation regarding caller ID spoofing – has chosen a new approach for regulating duties and obligations relating to the transmission of numbers.

The relevant provisions can be found in section 120 and section 123(3) of the new TKG.

In particular, the legislation provides for a number of new technical protective mechanisms. For example, if the caller's number for a call from a foreign network is a German number, the number (with the exception of mobile numbers) must not be displayed and the path of ingress of the call into the German network must be identified (new section 120(4) TKG). This provision has been prompted by findings that most of the calls with spoofed caller numbers either originate from foreign networks or are routed via foreign networks. The primary aim of the new provision is to rebuild trust in the validity of German numbers displayed.

The legislation also includes new obligations for disconnecting calls for which "forbidden" numbers are displayed as the caller's number (new section 120(3) TKG). This prevents in particular expensive numbers from being displayed as the caller's number. The list of "forbidden" numbers now also includes the emergency call numbers 110 and 112. This aims to prevent fraudsters from misusing the impact that emergency call numbers have and the public's particular trust associated with these numbers. In the past, there have often been waves of calls where callers have used 110 as the number displayed to the call recipients and convincingly posed as the police.

Finally, the Bundesnetzagentur now has the power to prosecute breaches of the provisions on number manipulation because, for the first time, it is now entitled to request call data information (new section 123(3) TKG).

The new package of measures and, in particular, the technical protective mechanisms are linked to the legitimate hope that there will be a considerable decrease in the number of calls with manipulated caller numbers. The improvements made by the legislator focus on technical measures. In an area where, for material reasons, it is often very difficult to investigate cases of misuse, technical measures provide more effective protection than measures taken afterwards against the perpetrator because they prevent the misuse in the first place.

The legislation partly provides for implementation periods of up to one year, which means that a considerable improvement in the situation can be expected from the end of next year onwards.

The Bundesnetzagentur's possible measures:

- It is expected that there will be a considerable decrease in the number of complaints about calls with spoofed numbers, and especially German numbers, being displayed as the caller's number after the implementation periods end. If, nevertheless, numbers are manipulated, the Bundesnetzagentur can, in appropriate cases, undertake specific investigations into the perpetrators and take action. Possible action in such cases includes disconnecting the numbers actually used for the calls (new section 123(1) TKG) and penalising violations as regulatory offences in administrative fines proceedings (new section 228(2) para 29 et seq TKG).

4.4 APPROACH IN LATVIA

Latvia has used formal regulation to oblige operators to block calls where A-number has been manipulated, including cases when the end-user does not have the right to use the A-number or where the A-number is not routable.

CLI-spoofing, including partial or full replacement of an A-number replacement, is considered a numbering misuse and fraud [9] in Latvia. Latvia's National Regulatory Authority (NRA) has developed a procedure regarding the elimination of fraud using numbering.

Latvia's regulation foresees that Electronic Communications Service Providers (ECSPs) should block routing of calls and access to the relevant number immediately, if fraud performed using numbering or incorrect use

of numbering is detected [10]. Latvia's legislation also foresees that ECSPs should include in their interconnection agreements references to the applicable payment procedure and actions to be taken in case of fraud [11] and should take measures to prevent fraud and incorrect use of numbering [12].

Electronic communication law also defines that the Regulator has rights not to grant or to cancel the right to use numbering for an ECSP in whose activities the Regulator has detected fraud performed using numbering or incorrect use of numbering.

4.5 APPROACH IN NORWAY

In Norway, a formal regulation [4] has been in place since 2013, obliging the operators to block, if technically possible and economically feasible, calls where the end-user does not have the right to use the A-number or where the A-number is not routable.

The Norwegian Communications Authority (Nkom), has also provided legal guidance to stakeholders clarifying the right to block calls to prevent customers from financial loss and consumer harm.

An industry guideline for number display/ CLI has also been created on the initiative of Nkom in collaboration with stakeholders in the Norwegian Working Group on Numbering.

Furthermore, Nkom has created an industry expert group to develop measures to prevent CLI spoofing and Wangiri. This work is an ongoing process, but efforts have so far been put into call filtering (including traffic monitoring and location verification) and ad hoc solutions for victims of spoofing, that is for customers whose number has been misused in spoofing.

There has also been limited operator-based initiatives to reduce SMS spoofing on a case-by-case basis.

Nkom has also arranged joint workshops with police authorities and operators and interacted with National Electronic Communications Industry Anti-crime Organisation (ITAKT[2]).

4.6 APPROACH IN UK

The United Kingdom (UK) is working on several current and future initiatives to ensure that the CLI data presented to callers is correct, thus promoting trust in CLI and protecting the interests of consumers. These measures are based on collaboration between industry and regulators, including developing and complying with regulation and guidelines, and information sharing.

Developments in IP technology have made it easier to change the CLI data associated with a call. As networks migrate to IP technology, more needs to be done to ensure that the CLI is correct and can be trusted. Operators have a greater role to play to ensure, where possible, that accurate CLI data is presented to end-users.

4.6.1 CLI obligations and guidelines

Ofcom (the UK's communications regulator) requires operators [5] to provide CLI facilities, and to ensure that the CLI data provided with a call includes a valid, dialable telephone number which uniquely identifies the caller:

- A valid number is one which complies with the International public telecommunication numbering plan (Recommendation ITU-T E.164) [6]. Where a UK number is used, it must be a number that is available for assignment in the UK's National Telephone Numbering Plan [7] and be assigned by Ofcom to an operator;
- A dialable number must be one that is in service and can be used to make a return or subsequent call;
- A number uniquely identifies the caller (which can be an individual or an organisation) where it is one which the user has authority to use, either because it is a number which has been assigned to the user or because the user has been given permission (either directly or indirectly) to use the number by a third party who has been assigned that number.

[2] http://itakt.no/

Ofcom also published CLI guidelines [8] to clarify what is expected of operators to implement the CLI requirements, setting out the fundamental principles of validity, privacy and integrity which will improve the reliability of CLI information. Guidance is necessary as the carriage of CLI data often relies on cooperation between two or more ECNOs and needs to be conveyed consistently.

The CLI guidelines set out the definition of a valid and dialable CLI for operators in different parts of a telephone call, based on what is technically possible today. Originating operators are responsible for ensuring that accurate CLI data is provided with a call and transit/terminating operators are expected to check that the number provided is from a valid number range.

The CLI guidelines also confirm that:

- all calls must be associated with a Network Number which identifies the origin of the call. However, the CLI that is displayed to the receiving party to identify the caller (Presentation Number) may be changed legitimately to another valid, dialable number that uniquely identifies the caller. The CLI guidelines set out scenarios where Presentation Numbers may be provided, as a commercial service, to meet differing customer calling requirements (for example, a call centre making calls on behalf of more than one client);
- the presented CLI must not be a number that connects to a premium rate service or to a revenue sharing number that generates an excessive or unexpected call charge.

The delivery of reliable CLI data to end-users, which respects the user's privacy, relies on the data being correct in the first place and the co-operation of all the ECNOs/ECSPs involved in the call chain to pass on this information correctly. The CLI obligations require operators to ensure that CLI data is exchanged with greater accuracy and that only valid CLI data is made available to end-users.

4.6.2 Operator action when the CLI is not valid

Where an operator considers that the CLI provided with a call contains invalid or non-dialable CLI data, they are required to prevent the calls from being connected to the called party, where technically feasible. This could be by either blocking or filtering the calls.

For calls that originate outside of the UK (i.e. on a network outside the scope of the UK's requirements), the operator at the first point of ingress is responsible for:

- ensuring that the call is populated with valid CLI data; and if not,
- replacing invalid or missing CLI data with a number that has been assigned to them for this purpose. To facilitate these situations, Ofcom has made a specific range of network codes available: '0' plus 10-digit numbers beginning with 08979.

Previously, industry practice was for the operator to insert a random number from a range that it had been assigned. However, this was not applied consistently across industry. Inserting a number from the 08979 range has simplified and accelerated the call tracing process, as using numbers from a dedicated range indicates clearly (i) that the CLI has been inserted; and (ii) which UK ECNO has inserted the number (the two digits after 08979 identify the operator that made the insertion).

4.6.3 Regulator and industry coordination

Ofcom has also worked with operators to help with the blocking of calls without a trusted CLI, including:

- convening an industry working group on nuisance calls, where members can share information via the regulator on numbers blocked in cases of fraud and misuse;
- Ofcom provision of a list of 'protected' numbers, which are numbers not designated for use in the UK's National Telephone Numbering Plan, therefore not valid numbers and should not be in use. Operators can use this list as a reference tool for blocking any calls with those CLIs;
- compilation of a 'Do Not Originate' list of numbers. Recognising that some of the most malicious cases of fraudsters spoofing numbers relates to those used by financial or government agencies, the 'Do Not Originate' list contains numbers that are not used by organisations to make outbound calls, such as inbound-only customer contact numbers. Ofcom is working with various bodies to share information with operators about the numbers that should not be used in call origination;

- working with the mobile networks and police to find innovative technical solutions to text message scams encouraging call-back to false numbers.

4.7 INFORMATION SHARING

Information sharing initiatives may be useful in studying and understanding fraud and misuse of numbers, including spotting trends. However, such measures are not real-time in nature and are therefore not that effective in stopping CLI spoofing from happening. This requires real-time or near real-time information and action. These initiatives can be implemented in the short term. Nevertheless, some examples of information sharing are looked at below to see what benefits these may offer.

4.7.1 BEREC cooperation process

In 2013, BEREC published a report on Article 28(2) USD Universal Service Directive: A harmonised BEREC cooperation process [30] outlining a process for cross-border cooperation in the intervention by NRAs or other relevant national authorities in cases of fraud or misuse, which can include CLI spoofing. The harmonised BEREC cooperation process was developed to assist NRAs in the effective application of powers (in the former Art. 28(2) USD, now Art. 97(2) of the EECC) that require EU Member States to "ensure that the relevant national authorities are able to require undertakings providing public communications networks and/or publicly available electronic communications services to block, on a case-by-case basis, access to numbers or services where this is justified by reasons of fraud or misuse and to require that in such cases providers of electronic communications services withhold relevant interconnection or other services revenues".

The BEREC process is best understood as a cooperation and information sharing tool to complement national processes in combating fraud and misuse. However, the process has been applied relatively few times and is largely untested. Experience learned that the process is too lengthy to be effective taking into account the speed of transfer of interconnect payments between carriers. Its use in a more frequent, faster, and harmonised manner across the EU, with the application of 'best practice guidelines', could improve its effectiveness in understanding and combatting trends in fraud and misuse, including CLI spoofing.

4.7.2 ITU-T guidance

4.7.2.1 Recommendation ITU-T E.156 - Guidelines for ITU-T action on reported misuse of ITU-T E.164 number resources

This recommendation was issued by ITU-T Study Group 2 in order to allow the reporting of alleged misuse of E.164 telephone numbering resources.

The different types of E.164 numbering resources considered are those with:

- Country Code for Geographic Areas;
- Codes for Inmarsat (+870) and Groups of Countries (+388);
- Country Code for Networks (+882, +883);
- Country Codes for Global Services (e.g. +800, +878, etc.);
- Country Codes for GMSS Operators (e.g. +881);
- Country Codes for trials (+991);
- Unassigned Country Codes.

Member States or Recognised Operating Agencies (ROA) could report alleged misuse by using the form available on the ITU website.

Based on the received reports there is a database[3] associated to Recommendation ITU-T E.156, nevertheless since 2005 only a few notifications were made (242) and only 31% had got replies.[4]

As an example of the data contained in the database, it is possible to classify the types of misuse. The following table shows this information:

Table 1: Type of misuse and number of reports

Types of misuse	Number of reports
Code used for premium-rate type services	105
Code used other than as intended	105
Other	13
Code used for web dialler	5
Unassigned code	5
Misrouted code	3
Unable to choose any of the above	3
Reserved code	2
Code used for shared-cost type services	1

4.7.2.2 Recommendation ITU-T E.157 - International calling party number delivery

Recommendation ITU-T E.157 was developed in order to provide guidance for the delivery of calling party numbers (CPN - equivalent to the A-party number/CLI) across different countries to improve security and minimise fraud and technical harm.

The main guideline given in Recommendation ITU-T E.157 was that the delivered calling party number should consist of a calling party number prefixed with a country code to identify in which country or network the call was originated (not including international roaming or nomadic calls) before it is delivered from an originating country to a receiving (succeeding) country. Additionally, to the country code, the delivered calling party number should include the national destination code, or sufficient information to allow proper billing and accounting, for each call.

[3] https://www.itu.int/net/ITU-T/misuse/table.aspx - this database can be only accessed using a TIES account.

[4] Based on information from 16 March 2022

5 ANALYSIS OF THE DIFFERENT TECHNICAL SOLUTIONS TO COMBAT CLI SPOOFING

In this section, some solutions that in the long term may combat CLI spoofing are presented. Some of them are already partially implemented, e.g. STIR/SHAKEN, others are still reaching a stabilised phase, such as SOLID or DLT.

On the other hand, this section does not analyse solutions/recommendations being developed within a number of ITU-T Study Groups (SGs) dealing with CLI spoofing and trust between networks. For example, ITU-T SG2 published in 2021 a technical report [34] that could assist in implementing measures to counter spoofing. ITU-T SG11, that works with protocols, have published a Recommendation [33] that presents the signalling architecture and requirements for interconnection between trustable network entities in support of existing and emerging networks. Other SGs, like ITU-T SG17, dealing with security, might also work with aspects concerning spoofing.

5.1 HIGH LEVEL DESCRIPTION OF THE STIR/SHAKEN IMPLEMENTATION IN THE UNITED STATES

This section describes STIR/SHAKEN as implemented in the United States, including the governance structure adopted in the United States. Other countries could implement STIR/SHAKEN and supporting global interoperability, while using a different approach for governance. For example, it would be possible to implement governance at a European level rather than at the individual country level.

In networks based on SS7 the originating operator inserts the CLI in the network signalling and via a chain of trusted operators the call terminates at the destination operator with an accurate CLI (for fixed and mobile). It is also allowed that e.g. the PBX inserts a number (the extension number); with two options: not verified and passed, or verified (in case the number does not belong to the DDI range the operator inserts main number as CLI) and passed.

Nowadays via IP technology any number can be inserted as CLI and also many more operators intervene in the handling of a call to the end destination which makes the chain less reliable.

5.1.1 Key insights behind SHAKEN

With the SHAKEN protocol, the underlying assumption is that the originating operator always knows something about the call origination:

a) sometimes the number in the CLI (e.g. in case of mobile authentication done by the network, fixed number controlled by the switch);

b) sometimes the customer, but allows another CLI to be inserted (PBX, receptionist and local callback number);

c) sometimes only the entry point (i.e. the gateway) into their network.

SHAKEN provides a secure mechanism for the originating operator to communicate this information to the terminating operator. In other words, SHAKEN ensures that what an originating operator knows is securely and reliably communicated to the terminating operator.

Therefore, the originating operator creates a digital signature based on what it knows about the call origination (the customer and their right to use the number; or the customer (but not the number); or the point it enters into their network); and inserts that in the signalling part to be transported to the terminating operator. The terminating operator verifies the digital signature. In case a party between the originating and terminating operator changed the CLI the verification process will flag the change.

Also, a special number referred to as the origination identifier (“origid”), uniquely identifies the call origination and is generated for every call and inserted in the signalling part to be used for trace-back of calls and

reputation purposes. The "origid" is a globally unique opaque[5] identifier corresponding to the operator and may include information on initiated calls themselves, customers, classes of devices, or other grouping that an operator might want to use for determining reputation or trace back identification of customers or gateways.

SHAKEN is based on STIR, a protocol developed by IETF and designed as an end-to-end mechanism. A STIR client would be present on both the originating party's phone as well as at the terminating (receiving) party's end. The operator is transparent in the process as the creation/verification is a phone-level task handled by the users involved in the call. As SHAKEN is based on STIR, it needs certificate management systems, and this part of the implementation is done at the operator level (namely, the creation of a digital signature by the originating operator; and the subsequent verification by the terminating operator).

STIR/SHAKEN would not directly block calls with spoofed CLIs. The result of the verification from SHAKEN could be displayed directly to the called end-user or fed into a “call-blocking app” that provides a rating system that essentially identifies calls as good, questionable or likely fraudulent. The call-blocking app can then act, on behalf of the called party, to stop unwanted calls from getting through. If no call-blocking app is used then the called end-user can decide on a per call basis.

In summary, SHAKEN not only gives operators the tools needed to sign and verify calling numbers, it provides end-users with a level of reassurance on whether or not to trust the caller, before answering the call.

5.1.2 Attestation Claims (i.e. different levels of attestation)

In SHAKEN, three different attestation levels are defined:

- Full attestation
- Partial attestation
- Gateway attestation

5.1.2.1 Full attestation

The signing operator satisfies all of the following conditions:

a) is responsible for the origination of the call;

b) has a direct authenticated relationship with the user and can identify the user (important for Law Enforcement Agency (LEA));

c) has established a verified association with the telephone number used for the call.

Important: In Full attestation, the signing operator asserts that its user can legitimately use the number that appears as the CLI but they are not asserting that the call is actually from the number that appears as the calling party (“legitimate” spoofing is allowed); ultimately it is up to the operator’s policy to decide what constitutes a “legitimate right to assert a telephone number” but it will impact “reputation”.

In STIR, this kind of “legitimate” spoofing is not allowed; but it was introduced in SHAKEN.

5.1.2.2 Partial attestation

The signing operator satisfies all of the following conditions:

a) is responsible for the origination of the call;

b) has a direct authenticated relationship with the user and can identify the user (important for LEA);

c) has not established a verified association with the telephone number used for the call (i.e. either the checking was not done or didn’t result in a positive answer).

[5] An identifier is opaque if it provides no information about the thing it identifies other than being a seemingly random string or number.

Important: Partial attestation does not imply that the call does not originate from this number, but only that this was “not checked” (i.e. the signing operator does not know). Each user will still be assigned a unique identifier to allow, based on data analytics, the establishment of a reputation profile and an assessment of the reliability of information asserted by the user assigned such unique identifier. (Reverse engineering the identity of the user purely from the identifier or signature would not be possible, thereby safeguarding the privacy of user's information).

5.1.2.3 Gateway attestation

The signing operator satisfies all of the following conditions:

a) is the entry point of the call into its VoIP-network;

b) has no relationship with the initiator of the call.

Basically, Gateway attestation only says that the operator only knows the entry point for the call into its network. Gateway attestation is useful for trace-back purposes since the “origid” would point to the originating node or trunk.

5.1.2.4 Principle

In case of Full attestation, a single identifier will be used for all direct operator-initiated calls on its VoIP-network, but an operator may also choose to have a pool of identifiers to differentiate geographic regions or classes of customers.

In case of Partial attestation, a single identifier per customer is required in order to differentiate calls both for trace back and reputation segmentation (so that one user's reputation does not affect the reputation of other users of the same operator).

In the case of Gateway attestation, best practices dictate that the “origid” should be sufficiently granular to identify the originating node or trunk to allow for traceback identification and reputation scoring.

The objective of the different attestation levels is to reflect the level of trust. Also best practices will develop for traceback and illegitimate call identification. "Origid" allows quick traceback once problems are detected (ex-post) but data analytics is needed to identify “bad calls”.

Given that, nowadays, CLI can easily be spoofed, operators need to rely on data analytics to detect fraud, and inherent limitations must be recognised as there are always risks of false positives. With the deployment of the "origid" and the SHAKEN mechanism, this (analytics) parameter can now be trusted to a greater extent.

5.1.3 Network implementation

5.1.3.1 Calls between users on Session Initiation Protocol (SIP)-based networks

Where the call is between users on SIP-based networks (e.g. IMS environment), the handling of the authentication and verification services requires the presence of the Secure Telephone Identity - Authentication Service (STI-AS) at the originating service provider and the Secure Telephone Identity - Verification Service (STI-VS) at the terminating service provider respectively.

Upon receipt of a SIP INVITE from the calling party, the originating service provider determines the level of attestation to provide for the calling number on the basis of the call source and calling number. The originating service provider then sends the SIP INVITE to the STI-AS which implements the mechanism at the origination of the call to sign the calling party information, including attestation claims and the “origid”, to generate the token (called PASSporT). This information and other parameters including the location of the certificate repository of the originating service provider are put in the SIP-identity header [24].

Upon receipt of the SIP INVITE with the SIP identity header, the terminating service provider sends it to the STI-VS. The STI-VS makes use of the location of the certificate repository of the originating service provider included in the SIP identity header to obtain the digital certificate with the public key, decodes the SIP identity header, verifies the signature and validates the PASSporT claims. The terminating service provider completes the call to the called party with potentially some optional treatment like a display that is dependent on the level of attestation and the resulting verification.

This mechanism works with Full and Partial attestation.

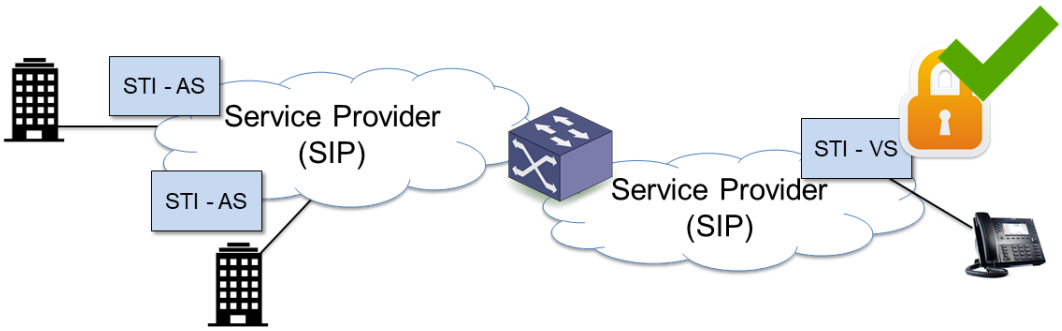

Figure 1: Mechanism for calls between users on SIP-based networks (Source: ATIS)

5.1.3.2 Call originates from SS7 network and terminated on SIP-based network

In such cases, the call is not based on SIP end-to-end. Since there might be multiple transit operators between the originating and terminating service providers, the call is signed by the STI-AS at the entry point to the first SIP-based network. The STI-AS returns the SIP INVITE with the SIP identity header which includes the token (called PASSporT) and the location of the certificate repository.

Upon receipt by the terminating service provider, the SIP INVITE with the SIP identity header is sent to the STI-VS for verification as described for calls between users on SIP-based networks. However, for calls originating from SS7 networks, the STI-VS at the terminating service provider can only verify where the call has entered the SIP-based network. Therefore, only Gateway attestation is possible in such cases.

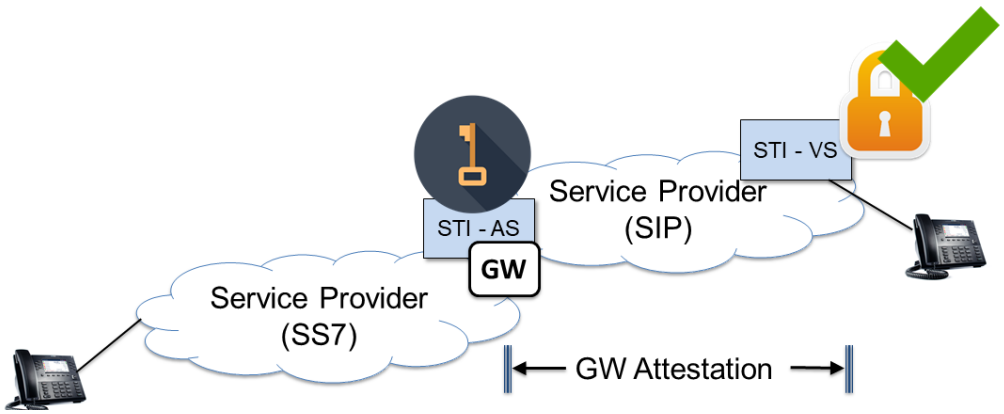

Figure 2: Calls originating from SS7 networks and terminating on SIP-based networks (Source: ATIS)

5.1.4 SHAKEN governance model

This section describes STIR/SHAKEN as implemented in the United States, including the governance structure adopted in the United States.

For the creation of the digital signatures, STIR/SHAKEN certificates are needed, and it must be ensured that these certificates do not fall in the hands of bad actors.

For this reason, a Governance Authority (STI-GA) is set up and tasked to define and modify the rules for the whole ecosystem as well as the mechanism for operators to obtain SHAKEN certificates. It is important to note that the STI-GA has to ensure that only legitimate operators can obtain a digital certificate and take part in the system. The STI-GA is also responsible to select the STI-Policy Administrator (STI-PA) following a Request For Proposal (RFP).

The FCC has only an arm's length oversight function on the Governance Authority. The board of the Governance Authority consists only of industry actors in order to react quickly to adapt the rules because it is expected that fraudsters will try to find ways to bypass the system.

The STI-PA applies the rules created by the STI-GA, thereby adopting an operational role and validates that the operators are authorised to obtain STI certificates. They issue the "operator tokens", approve the STI Certification Authorities (STI-CAs) and maintain the list of all secured authorised STI-CAs (comprising the root of trust in the whole system) and the Certificate Revocation List (CRL).

The STI-CA issues the STI certificates to the operators. These are Certification Authorities (CAs) specific for STIR/SHAKEN. The CA has to apply with the STI-PA to participate in the SHAKEN system. In the application the CAs must demonstrate they fulfil the criteria as defined by the STI-GA.

Operators who want to participate in the system have to file in an application with the STI-PA demonstrating they fulfil the criteria defined by the STI-GA. If they pass, then the STI-PA issues a "Service Provider Code" (SPC) token. Based on the token they can buy a STIR/SHAKEN certificate from a validated STI-CA.

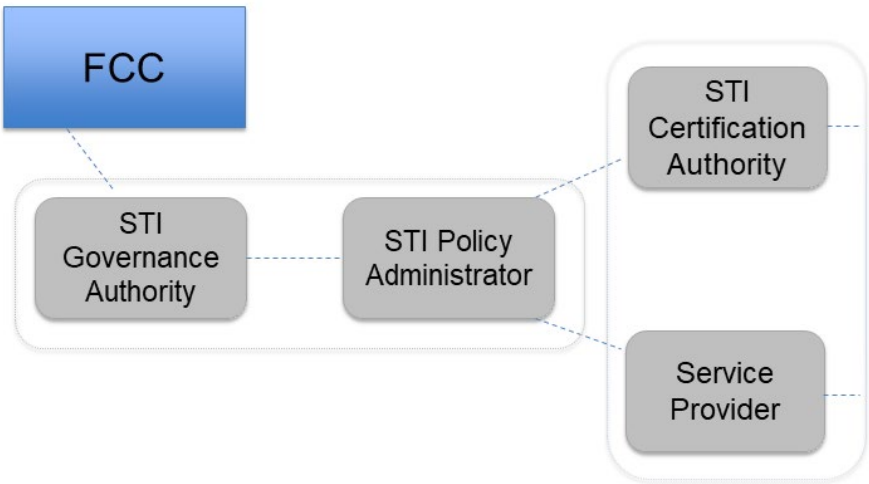

Figure 3: STIR/SHAKEN governance model (Source: ATIS)

5.1.5 Extension for Implementing Call Authentication on IP and Non-IP Networks

FCC has mandated the US ECSPs to implement a mechanism in order to validate CLI in calls made in SS7 networks. The solution will be based on the STIR/SHAKEN architecture and queries, but the information could be sent through the SS7 signalling. It is expected that this work will finish in 2022 or 2023.

5.2 INTERNATIONAL STIR/SHAKEN

The technical solution based on STIR/SHAKEN is a centralised architecture and was initially designed for a single country – the United States. With the agreement with Canada, the model needed to be updated to allow to have two distinct instances, but both countries still have the same country code and a common organisation for the management of the numbering plan. The initial cross-border SHAKEN standard defined a mechanism to allow STIR/SHAKEN to work between countries, based on bilateral agreements. Nevertheless, there are a number of strategies that could help with cross-border, including coordinated regional implementations (e.g. Europe wide governance), industry forums, or "communities-of-interest". This initial approach would eventually run into scaling problems, but it can readily be extended to accommodate deployments over the next several years.

But there are more and more countries, that want to have a CLI validation mechanism to mitigate fraud and misuse of numbers. For that reason, the STIR/SHAKEN technical solution needed to be expanded in order to fulfil this new requirement.

The most prominent challenges identified related to the following:

- Setting up a rigorous vetting process to ensure legitimacy;
- The difficulty to get all countries accepting vetting process;
- The implications of requiring a very large number of bilateral agreements.

Nevertheless, it should be necessary to provide a lightweight process allowing countries to enrol and let individual countries/regions decide who to trust. The model for registration could be different from country to country, as shown in the following figure:

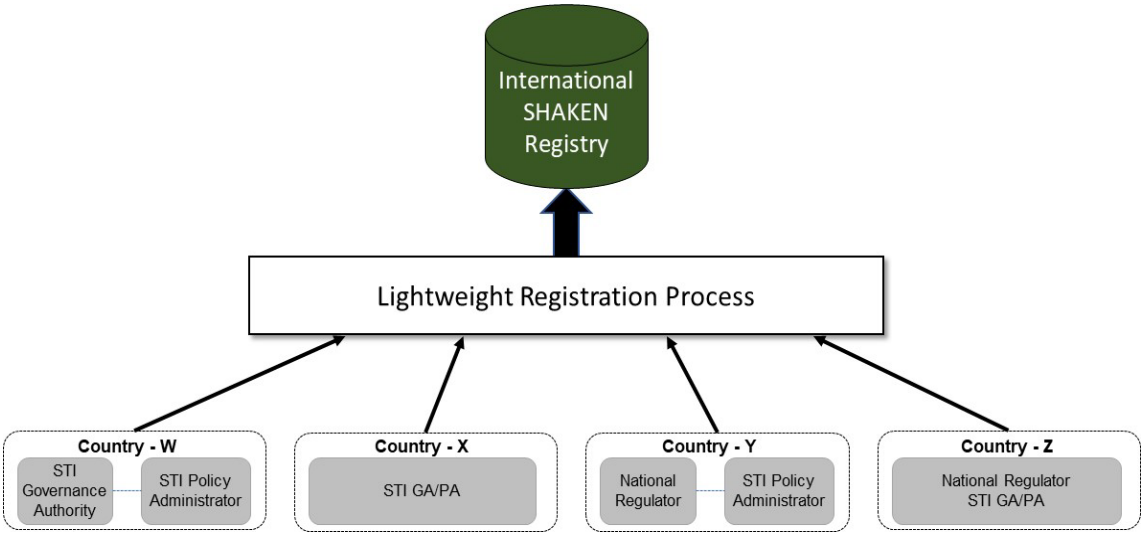

Figure 4: International SHAKEN Registry (Source: ATIS)

Each country or region could independently decide what to do with the registration information in the International SHAKEN Registry. Nevertheless, there should be some minimum criteria defined to make sure there is consistency across countries.

The longer-term strategy of a central registry requires additional work to fully implement, and faces several administrative challenges, and is therefore likely to require widescale deployment of STIR/SHAKEN before it is practical.

A more general diagram of the International STIR/SHAKEN model is shown in Figure 5.

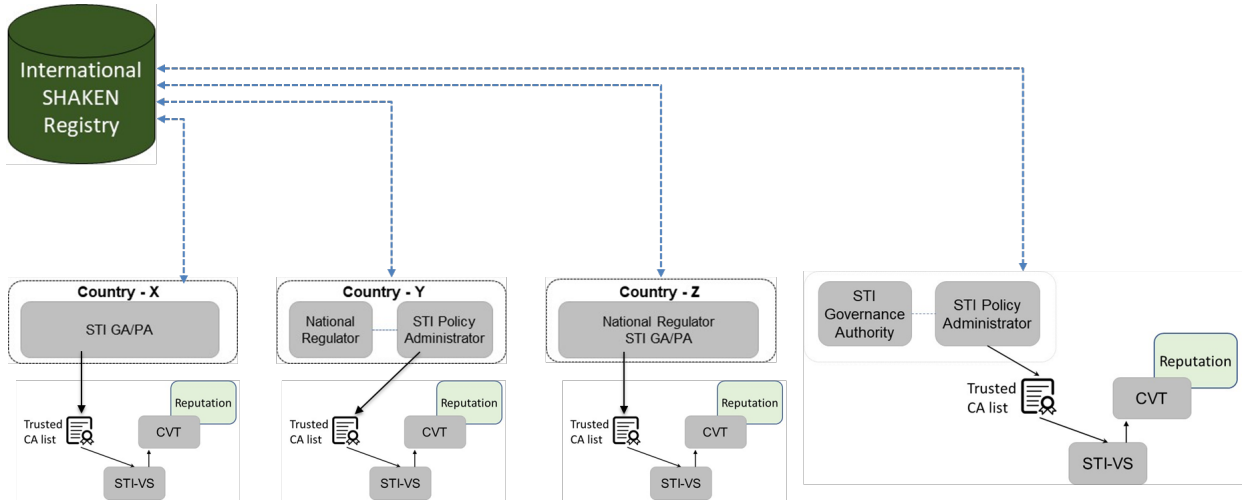

Figure 5: International SHAKEN Forum (Source: ATIS)

5.3 SOCIAL LINKED DATA (SOLID)

SOLID (Social Linked Data) is a proposed set of conventions and tools for building *decentralised applications* based on Linked Data[6] principles. SOLID framework allows individual entities to separate their data from the systems and applications that leverage it into private data stores. SOLID is modular and extensible, and it relies as much as possible on existing W3C[7] standards and protocols.

SOLID allows individual entities to separate their data from the systems and applications that leverage it into private data stores, or "Pods". Each individual entity controls the data in its Pod and chooses which other entities it will share that data with. It is built on top of the Hypertext Transfer Protocol (HTTP), which it extends it through a set of open standards and protocols.

SOLID's decentralised architecture provides the foundation for a Distributed Peer to Peer Fraud Mitigation Network. Because it is built on the web, it does not introduce any new protocols or infrastructure requirements, which limits added complexity and allows for the reuse of existing infrastructure already in place to facilitate web traffic.

SOLID is applicable to telco ecosystem for A-party Number validation where the decentralised identity and security model provides peer-to-peer authentication, authorisation and crypto.

[6] https://www.w3.org/DesignIssues/LinkedData

[7] https://w3.org/

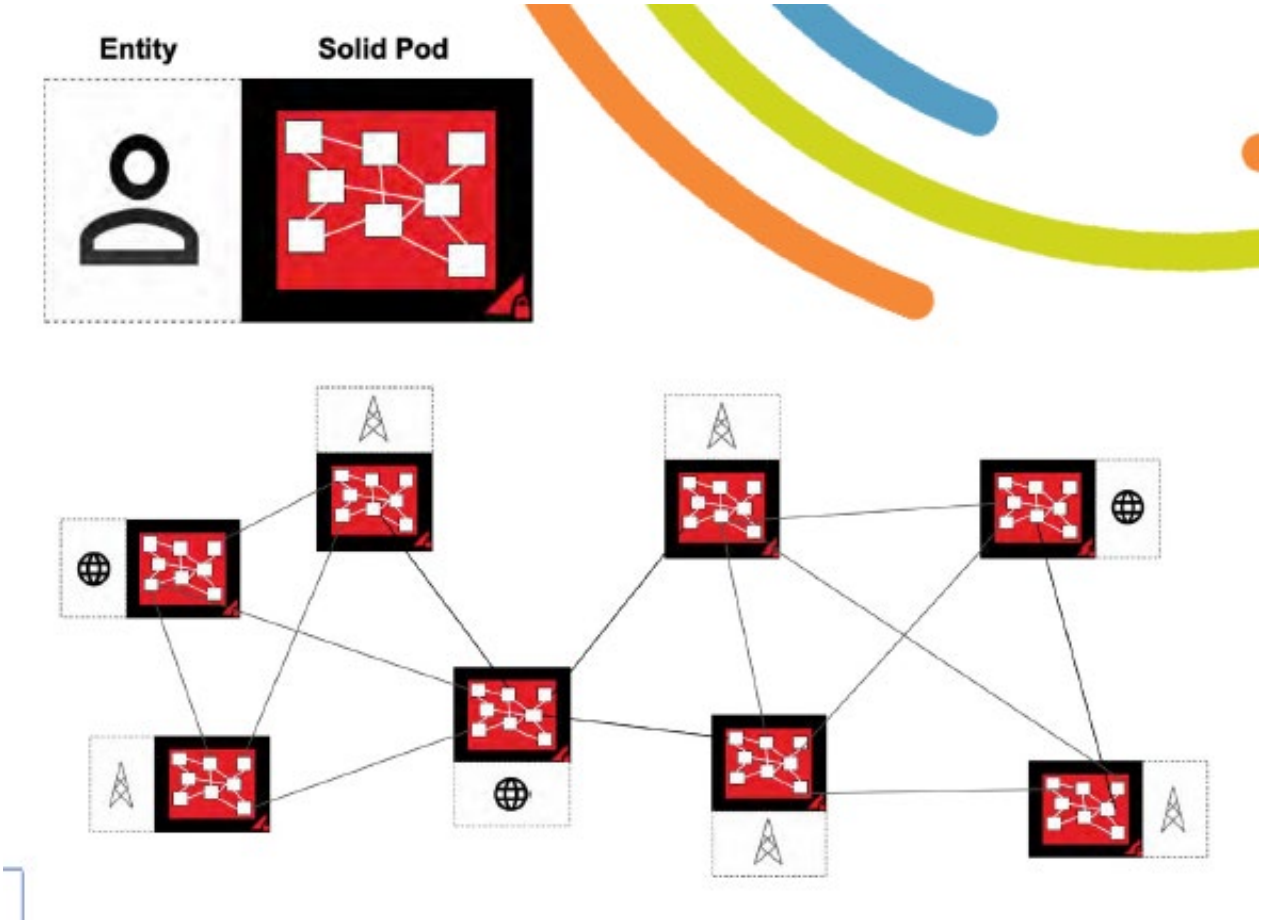

Figure 6: Architecture
(Source: I3forum)

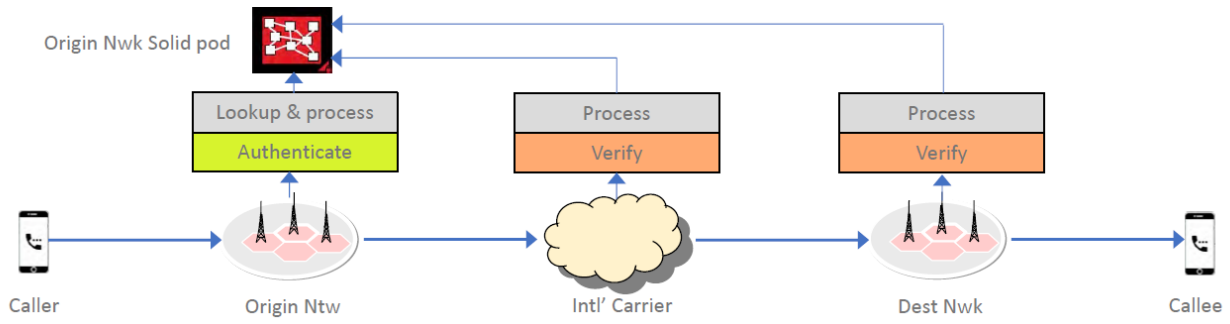

Figure 7: Processes
(Source: I3forum)

SOLID has been discussed specifically in combination with Secure Telephone Identity Revisited (STIR) to mitigate internetwork call fraud through a Distributed Peer to Peer Network. STIR can be used for call origin validation and for the secure transport of call meta-data between Origin and Destination Networks. SOLID can be used for flexible and secure data sharing between the same. This theoretical approach addresses the fraudulent behaviour without any disruption to the legitimate eco-system of operators, carriers, callers, and callees.

In this approach, each participating network has an associated SOLID Pod that they host themselves. For every initiated call to a different participating Destination Network, the Origin Network creates a call record in their SOLID Pod, in an area that only that Destination Network is authorised to access. The Origin Network

stores important metadata like call initiation time, caller number, callee number, and call state into that call record. It stores the URL of the call record in the SIP Identity Header, and changes the "To" header to an anonymised callee identifier at the Destination Network. When the call is received by the Destination Network, it looks up the call record in the Solid Pod at the URL stored in the SIP Identity Header, and updates the "To" header to the real callee number stored therein. It also updates the call record to let the Origin Network know the call was received by the intended Destination Network.

In this solution, STIR is used to validate the caller and prove the identity of the Origin Network, which is essential to the integrity of the workflow. STIR introduces the SIP Identity Header, which the Origin Network uses to pass the URL of the call record to the Destination Network. STIR allows the Destination Network to be confident that the Identity Header (and therefore the URL of the call record) hasn't been tampered with in transit.

Up to now SOLID has not been actually implemented by operators. SOLID technical specification draft is available on https://github.com/solid/solid-spec.

5.4 DISTRIBUTED LEDGER TECHNOLOGY - BLOCKCHAIN

Distributed Ledger Technology (DLT) is a protocol that enables decentralised database management by multiple participants across multiple nodes. Three characteristics of DLT mean that its platforms are particularly well-suited to establishing telephone numbering databases:

- Delivers trust and assurance within the processes;
- Creates secure immutable assets (with numbers being the digital asset in this case);
- Delivers ‘smart contracts’ (programmes that encode the rules for specific types of transactions in a way that can be validated and triggered by specific conditions).

Blockchain is a type of distributed ledger. It is composed of digitally recorded data arranged as a successively growing chain of blocks, with each block cryptographically linked and hardened against tampering and revision. If applied to number management, blockchain could provide a type of distributed ledger based on the right to use and status of the telephone number as the digital asset, using a platform that is distributed through decentralised nodes among members. A ‘Permissioned Blockchain’ platform (as opposed to private or public), ensures functionality for all parties involved in number administration but has the additional security measure of an access control layer that allows actions to be performed only by certain identifiable and permissioned participants. Data can therefore be exchanged securely and transparently.

Substantive work on the implications and applications of DLT in the communications sector is being undertaken by a range of organisations, most notably the ITU [33].

Blockchain to share public key certificates so as to verify user identity

- Blockchain is a distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way;
- Use case where operators share information on subscribers’ identity and certificates;
- Blockchain ecosystem to be created among international carriers as well as domestic operators;
- Governance, policy and certification to be further analysed;
- To be compared with Solid for certificate management.

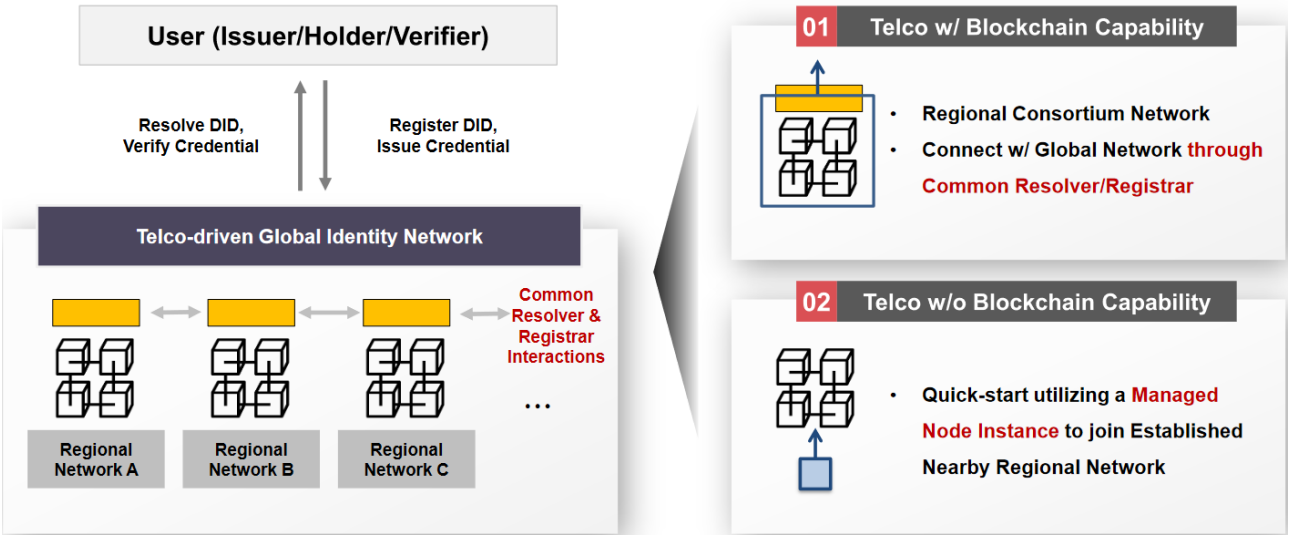

Figure 8: Blockchain global network architecture (Source: SK Telecom)

5.5 AB HANDSHAKE

AB Handshake is a solution which is used to detect fraud in real time relying on cooperation between operators and to eliminate fraud within the group of operators by validating the traffic between their networks.

AB Handshake was developed as a neutral solution without connection to a specific country or set of regulations. It currently validates live traffic of operators located in different geographical regions. Operators can opt-in and connect to the service on an individual basis, regardless of the decision of other operators in the same country.

In case of spoofing a fraudster changes the A E.164 number of an outgoing call to mimic a number that is familiar to the recipient. With AB Handshake, the originating switch sends the call data to the originating call registry and subsequently a validation request is initiated over the Internet (so out-of-band parallel HTTP side path) to the terminating call registry. The terminating switch (after receiving the call from operator A) sends the call data to the terminating call registry. The terminating call registry sends the verification request – based on the A E.164 number data – to the operator to whom the A E.164 number as received on the terminating side has been assigned. If the A E.164 number is spoofed the response will be no call initiated (for operators participating in the system) or no response at all. The B operator detects in real time that the call is fraudulent and can block the call or label it as fraudulent. All call details are collected in a call log in order to be used in an investigation or dispute. In case the A E.164 number is not spoofed, operator A will receive the termination verification request and will reply that the call is verified. In case the A E.164 number is spoofed, operator A will receive the notification that the call has reached the B operator with a different CLI.

In case the call validation is not possible due to absence of response from either end, the calls proceed without interruption. Corresponding notifications are sent to other participating operators, so false positive fraud alerts are not generated. Call validation is performed directly between the Call Registry nodes controlled by the operators, the central database does not take part in this process. Call logs are stored in individual Call Registries of the participating operators. The central database holds a list of participating number ranges and IP addresses of Call Registry nodes. This information is distributed to the individual Call Registries for the purpose of routing call validation requests.

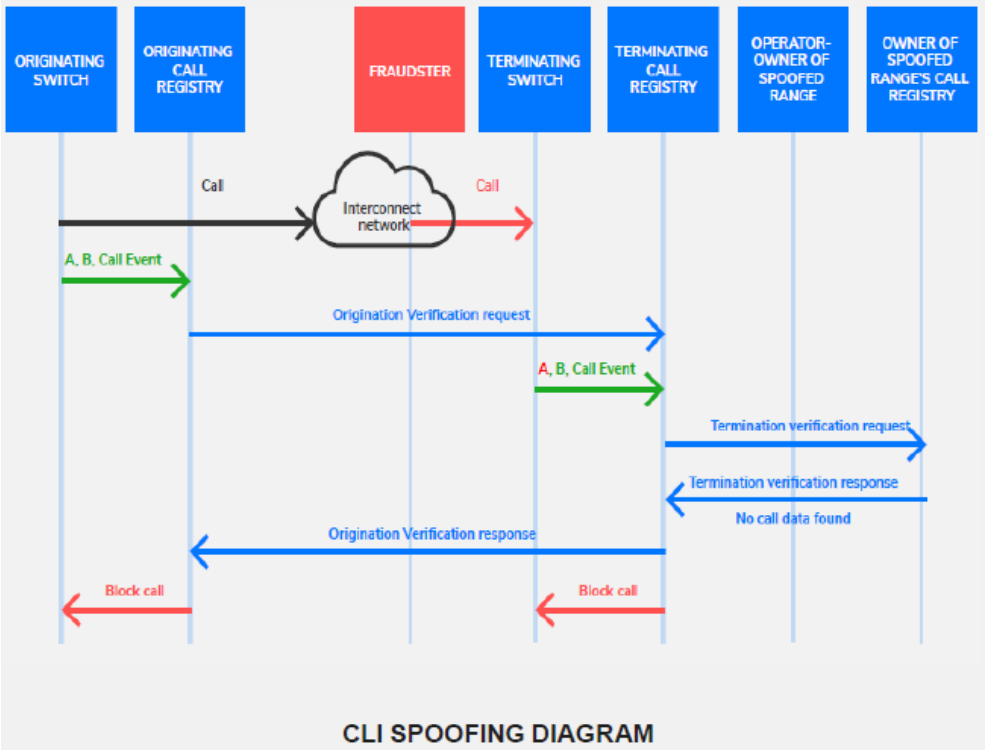

Figure 9: CLI validation for CLI spoofing detection (Source: AB Handshake)

The AB handshaking is promoted by AB Handshake Corporation, which is a commercial entity. The system uses an out-of-band validation method, which does not interfere with the call establishment process. Such architecture enables non-invasive integration with an operator's network and can support both IP and legacy operator networks. The international or local call flow is not affected by addition of this validation method.

Because AB Handshake method validates all call parameters between the originating and terminating parties, it allows to detect and block other types of voice fraud beyond CLI spoofing.

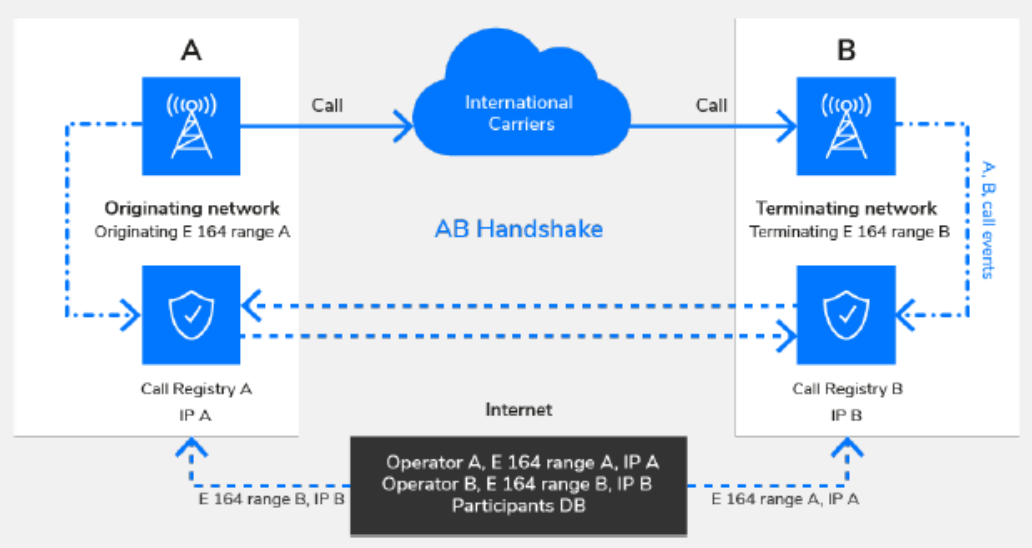

Figure 10: AB Handshake Out-of-Band System Architecture (Source: AB Handshake)

The same out-of-band handshake is also applicable to the validation of P2P and A2P SMS traffic. AB Handshake has announced a trial of this service. The architecture and logic of the SMS validation solution will be in line with the principles described above.

Detailed real time knowledge on which operator serves a given active E.164 number is needed which is a big challenge given the complexity of the supply chain of telephone numbers (number portability and sub-assignment). Within the AB Handshake ecosystem this is handled by either integration with Number Portability (NP) databases on the network level or an integration with the authorised numbering plan administrator. It seems that a neutral central registry needs to be created and managed (also with the IP addresses to support the call registries) which is, in an international context, delicate.

5.6 CALL PATTERN ANALYSIS

Major international spoofing activity may consist of multiple calls towards a specific destination or region. Traffic pattern analysis may in theory, if relevant parameters are set, separate spoofed traffic from real traffic. In particular, the providers receiving traffic in each country, typically by holding a Q.708 International Signalling Point Code when SS7 signalling is used, can be in a position to conduct this analysis of the traffic in order to make the separation. The type of analysis is already implemented or can be considered in the short term.

Also large international operators who terminate or transit international traffic are in a natural position to detect suspicious activity. However, the primary role of these stakeholders is to ensure that traffic is passed through, independent of content or CLI usage. Therefore, one could envisage a more proactive role, for the benefit of the whole value chain whereby the mentioned stakeholders block or mark traffic that fails to meet certain criteria.

The criteria can be set by the contracting parties in order to improve the quality of service, e.g. by setting parameters for when a call pattern indicates that the traffic is obviously malicious. The parameters in the call pattern analysis could be related to an analysis of the amount of calls stemming from a specific number or channel combined with analysis of formal number origin. For example, an input to the analysis could be that a call is probably spoofed if the number of calls exceeds level X from numbers at Y gateway, with Z origin.

Due to the risk involved in blocking calls, a middle way could be to strip CLI and mark as unknown caller.

Wholesale operators need to work as a group on this topic in order to identify the bad actors. This requires a long term collaborative support within the industry and with the public authorities. Sharing information is delicate and contracts within the industry should be reviewed in order to avoid that some parties misuse ‘non-disclosure’ clauses to make this impossible.

After identification of stakeholders facilitating fraudulent traffic, this information can be used to alert other ECNOs/ECSPs allowing them to take sufficient actions.

Nevertheless, the impact of these solutions will not necessarily prevent spoofed calls from passing through. Indeed, spoofers may adapt their strategies, and different stakeholders in the value chain may have different parameters defining actions to be taken. Furthermore, blocking measures implemented could result in false positives, thus blocking or restricting real calls. Notwithstanding, a more proactive approach than the current pure carrier-approach is still desirable.

With STIR/SHAKEN, one can go one step further, namely each call can be uniquely identified via the "origid", which makes traceback possible. If certain originating operators cannot be trusted, for example by manipulating the attestation, this can be detected via data analytics. As a consequence of this, terminating operators can take action under the form of removing the CLI or even blocking calls from these originating operators.

5.7 GATEWAY CONTROL

When an interconnecting mobile call enters the jurisdiction of a country, it passes through an international gateway. When a national mobile number is used as CLI for such a call, at gateway level it is possible for a network operator, possibly through third parties, to verify whether the SIM associated with the number in

question is actually located outside the country. If the case is the opposite, such that an international call comes in at the international gateway but the SIM associated with the number used as CLI is in fact located within the country, the call is likely to be spoofed and therefore may be blocked or restricted. This type of “geo-checks”[8] can decrease the amount of spoofing.

Furthermore, the blocking or restricting of interconnecting calls with domestic geographical number originating from outside the country, pretending to be national calls, should reduce spoofing. However, it will depend on national policies whether international inbound calls from national geographical numbers, are allowed.

[8] The processing of the required information needs further analysis, in particular in the context of ePrivacy legislation.

6 LEGAL/REGULATORY ASPECTS

At EU level there are several legal provisions related to CLI. These provisions stem mainly from the Directive (EU) 2018/1972 [36] establishing the European Electronic Communications Code (EECC) and the Directive 2002/58/EC [37] on privacy and electronic communications (ePrivacy Directive). These instruments focus on introducing CLI and do not as such address CLI spoofing.

According to the EECC, NRAs may require all providers of publicly available number-based interpersonal communications services to make available to end-users a CLI facility (Art. 115 and Annex VI, part B in the EECC) where the originating party's number is presented to the receiving party prior to the call being established. This facility shall be provided in accordance with relevant law on protection of personal data and privacy, in particular the ePrivacy Directive. However, this obligation is subject to technical feasibility.

While replacing most of the former EU-directives addressing the electronic communications sector, the EECC does not repeal the ePrivacy Directive, meaning its provisions are still in effect.

While the principles and main provisions of the ePrivacy Directive remain generally sound, that Directive has not fully kept pace with the evolution of technological and market reality, resulting in an inconsistent or insufficient effective protection of privacy and confidentiality in relation to electronic communications. This Directive will therefore be replaced by the proposed ePrivacy Regulation (ePR) [38], which, unlike the Directive, will become part of the Member State's national legislation. Whereas national implementation of the current Directive may have resulted in small differences regarding obligations on the service providers or rights for the users, the coming Regulation will probably facilitate a more complete harmonisation in these regards.

Therefore, the consequences for ensuring sufficient implementation depends partly on whether national legislation is compliant with the current Directive, but also on the scope and implications of the coming Regulation vis-a-vis the current Directive.

In any case, it should be considered that the referred legal provisions are relevant for EU countries whereas CEPT includes other European countries.

The following sections aim to give a brief overview of the provisions that need to be considered, regarding the implementation of CLI and the potential manipulation of it, in the present Directives and in the proposed ePR.

6.1 EUROPEAN ELECTRONIC COMMUNICATIONS CODE (EECC)

Article 40 (Security of networks and services) and Article 115 (Provision of additional facilities) of the EECC may have some implications on combating CLI spoofing.

According to Article 40 of the EECC EU Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services. Taking into account the state of the art, those measures shall ensure a level of security appropriate to the risk presented and include, but are not limited to, measures that prevent negative impacts on (other) users of the network or other networks and services. Article 40 of the EECC may not in itself provide a sufficient legal basis to fight against CLI spoofing as network security is not in danger.

Furthermore, Article 115 of the EECC states that EU Member States must ensure that competent authorities in coordination, where relevant, with national regulatory authorities are able to require all providers of publicly available number-based interpersonal communications services to make available free of charge all or part of the facility of calling line identification, in the context of the EECC defined as the presentation of the calling party's number to the receiving party prior to the call being established (restricted only to voice communications).

6.2 PRESENT EPRIVACY DIRECTIVE

In the present ePrivacy Directive Article 8 (Presentation and restriction of calling and connected line identification) and Article 10 (Exceptions) are related to CLI.

Article 8

1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.

3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.

5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.

6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Article 10

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override:

(a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service;

(b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.

When implementing the provisions regarding the enabling and disabling of CLI, the provider needs to take into account the possible threats that may arise in so doing. Although not specifically mentioned, fraudulent CLI presentation may result in lower trust in numbers by the called end-users and thus diminish the positive impact of Article 115 of the EECC.

6.3 PROPOSED EPRIVACY REGULATION (EPR)

In the proposed ePR, Article 12 and 13 are relevant to CLI, and mirror the obligations of Articles 8 and 10 in the current Directive. Relevant to CLI spoofing in the proposed ePR are Articles 5 (Confidentiality of electronic communications data) and 14 (Blocking Unwanted, malicious or nuisance calls).

Article 5, Electronic communications data shall be confidential. Any interference with electronic communications data, including listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance and processing of electronic communications data, by anyone other than the end-users concerned, shall be prohibited, except when permitted by this Regulation.

Sub-article 14.1, Providers of number-based interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted, malicious or nuisance calls by end-users.

Sub-article 14.1a, Member States shall establish more specific provisions with regard to the establishment of transparent procedures and the circumstances where providers of number-based interpersonal communication services shall override, or otherwise address, the elimination of the presentation of the

calling line identification on a temporary basis, where end-users request the tracing of unwanted, malicious or nuisance calls.

Electronic communications data shall be confidential and should be defined in a sufficiently broad and technology neutral way. It includes so-called communications metadata, for example data to trace and identify the source and destination of a communication such as A-party number and B-party number. Spoofing is not specifically mentioned in article 5 of the proposed ePR, but it says that any interference with electronic communications data, including manipulation of these data, by persons other than the end-users concerned and without their consent, shall be prohibited. From this may be derived that electronic communication service providers have a (co)responsibility concerning the authenticity of these data.

Nevertheless, it is often the case that the fraudsters themselves would be behind the spoofing of the CLI, such case where the end-user is the source of CLI spoofing is not directly covered by these provisions.

Further, sub-article 14.1 and sub-article 14.1a of the proposed ePR, concerning unwanted, malicious or nuisance calls, stipulate that providers shall deploy state of the art measures to limit the reception of unwanted, malicious or nuisance calls by end-users. Article 14 covers consumer problems that may be facilitated by spoofing. From recital 29 (ePR) it follows that providers of number-based interpersonal communications services should deploy existing technology and protect end-users, free of charge, against unwanted, malicious or nuisance calls such as calls originating from invalid numbers, i.e. numbers that do not exist in the numbering plan, valid numbers that are not assigned to a provider of a number-based interpersonal communications service, and valid numbers that are allocated but not assigned to an end-user. This should be done in line with article 5 of the proposed ePR and article 40 of the EECC.

Synthesis

In the EU, legal framework EU member states are encouraged to establish a national provision that requires providers of publicly available number-based interpersonal communications services to offer calling line identification. The goal of this provision is to identify an originating party number and to enable users of electronic communications services to choose a level of privacy protection in public voice communications. This goal is undermined if the information in the CLI is not trustworthy and in that case the positive impact of facilities implemented by electronic communications providers under Article 115 of the EECC would lose some (or all) of their intended effect.

In the case that providers of publicly available number-based interpersonal communications services offer CLI, either voluntarily or obliged thereto at the national level, it can be derived from EU legislation that consequently they have a responsibility to take measures to assure that the information in the CLI is correctly delivered to the receiving party. However, in this respect the principle of proportionate technical and organisational measures applies from the EECC and the principle of using state of the art technology applies from the ePR. This legal situation seems to take into account that electronic communications services providers may not have sufficient means to fully contribute to the goal of Article 115 of the EECC in all cases. Such a case may typically arise when untrusted CLIs originate from networks outside the country where the call terminates.

A missing element in the mentioned EU provisions is that these requirements are directed only to providers of public electronic communications networks and services. The role of end-users in the practice of CLI spoofing has grown along with the growth of VoIP technology and there is no reason not to include these parties as co-addressees of a provision that prohibits CLI spoofing.

Pending on the outcome of the legislative process of the proposed ePR especially article 5 and article 14 may stimulate national measures to further prevent CLI spoofing.

It is up to national administrations how to embed the above situation in their national regulations. In order to implement the EU provisions referred to effectively in national legislation, national administrations should consider to explicitly forbid CLI spoofing to all parties involved (ECSP/ECNO and end-users), and also constitute proportionate measures that apply to ECSP/ECNO. Such measures should be in line with ECC Recommendation (19)03 [1] and may include the allowance of or obligation to mask CLI information or to block calls in cases where the ECSP/ECNO has no reasonable means to validate the CLI information entering its service.

Notwithstanding the regulatory measures put in place, a lot of responsibility still rests with providers and end-users themselves. Coupled with such regulation, swift and effective action is a must to minimise CLI spoofing.

6.4 EUROPEAN COMMISSION'S DELEGATED REGULATION (EU) 2021/654 OF 18 DECEMBER 2020

The Commission Delegated Regulation (EU) 2021/654 [39] setting a single maximum Union-wide mobile voice termination rate and a single maximum Union-wide fixed voice termination rate, referred to as Eurorates, gives operators the right not to apply Union-wide termination rates for calls if the CLI is missing, invalid or fraudulent (see recital 15).

With this approach, fraudulent behavior is not rewarded. Furthermore, it is helpful and appropriate to allow terminating operators to charge additional interconnection fees if operators attempt to terminate spoofed CLI traffic. These additional fees should cover the costs that these terminating operators incur for the prevention and detection of spoofed traffic.

There is a need to define clear verifiable rules of what is and what is not to be considered CLI spoofing, as otherwise there could be cases where terminating operators may take advantage of this right and charge fees that could be considered excessive by other network operators involved in the conveyance of the call.

7 FURTHER ANALYSIS AND CONSIDERATIONS

It is unlikely that all operators in Europe will introduce systems to counteract CLI spoofing on their own initiative, without regulatory intervention. In that sense, the situation is similar to that in the USA where operators only introduced STIR/SHAKEN on a large scale after implementation of corresponding legislation.

The existing provisions in the Code and present ePrivacy Directive form a weak legal basis and may be insufficient to mandate any technology which prevents CLI spoofing. The proposed ePrivacy Regulation offers in sub-articles 14.1 and 14.1a a more solid legal basis but these sub-articles are limited to the principle, which is important but probably not sufficient.

There is clearly a risk to a fragmented approach which will lead to national solutions which are inefficient for a problem which is international in nature.

In order to ban CLI spoofing for the purpose of misuse and/or fraudulent use of numbers it must be included in the EU legislation. In addition, it is recommended that there is a set of common principles and a harmonised technology that countries have to comply with so that interoperability is assured.

For the short-term, traffic pattern analysis may reduce some of the problems, but it is not generally a real-time solution. At both the national level, and within international/regional fora such as ITU or BEREC, CEPT administrations should promote industry groups to facilitate discussions on traffic analysis and information sharing to combat CLI spoofing.

It is likely that all European operators wishing to terminate calls, where both the called party number and the calling party number are US numbers, will in due course have to implement STIR/SHAKEN. Clearly, this technology has the first mover advantage. A real-time solution is needed, as a non-real-time solution doesn't solve the problems. Other technologies to combat CLI spoofing such as blockchain and SOLID are either in a very immature phase or could be used as a non-real-time solution only. It is therefore appropriate that Europe considers STIR/SHAKEN as a strong candidate with significant potential to assist in combating CLI spoofing. There are however some aspects that need further study.

It should be ensured that STIR/SHAKEN or the European variant and its implementation is compliant with GDPR and the future ePrivacy Regulation. That's an analysis that has to be made. Trace-back of calls is essential in STIR/SHAKEN for detecting fraud by bad actors. Therefore, it must be assessed if CDRs (call detail records) can be used according the GDPR/ePrivacy regulation for these purposes. Also, cooperation among all involved parties in order to share information is needed "to feed" the scoring system which is delicate from a competition point of view.

It would be an advantage to have a European harmonised deployment and related governance system vis-à - vis different national deployments. For that reason, the approach should be "as international as possible". An EU/CEPT common approach is the minimum, a global approach is the ideal. Therefore, the idea to create a STIR/SHAKEN industry forum is a pragmatic way forward. However, it should be recommended that vital functions are maintained in European countries.

A pan-European deployment brings advantages in terms of scale and harmonisation. On request of WG NaN a proposal was made by the EC to add a new action (8) "SDOs to prepare a report on measures to mitigate, prevent and/or detect CLI spoofing. The report should address the technical, operational, standardisation and cost aspects of the different possible solutions (STIR/SHAKEN, blockchain, SOLID, etc.) from the European perspective. It should also consider how such solutions could be deployed and managed at the European level" to the EU Rolling Plan 2021.

The costs related to governance structure and deployment will depend on the chosen solution and could be based on EU or larger scale CEPT solution. In any case the solution should interoperate with other similar systems.

It will be impossible to harmonise the criteria (e.g. only entities that have direct access to numbering resources, probably stricter criteria) to be fulfilled so that an operator can take part of the system worldwide. In this regard, future studies could also look into the benefits of adopting a hybrid model, which would consist of 2 layers: the basic layer (the minimum level) and a 2nd level. For the basic level, minimum criteria could be: only parties that have a direct assignment of numbering resources and only parties that fulfil minimum rules regarding the

authentication of their users can get a digital certificate. The 2nd level could be based on "reputation" derived from data obtained from experience.

It is also important to note that e.g. AB Handshake can directly be applied to combat other types of fraud (e.g. Wangiri, call hijacking) but it is a proprietary solution, which could be seen as a disadvantage in terms of its broad applicability compared to open solutions like STIR/SHAKEN.

SOLID's practical application in combination with STIR was discussed at GSMA, and was found to provide limited additional benefits when compared to SHAKEN/STIR, given that the latter has now been enforced by FCC and that it’s spreading across telco parties in North America. This being said, both frameworks are compatible and SOLID addresses wider fraud protection coverage than STIR/SHAKEN.

8 CONCLUSION

Given the damage caused by CLI spoofing, it is appropriate that CEPT administrations take the following approach:

1 an explicit prohibition of CLI spoofing, not only for operators but also for users, in national legislation;

2 the further elaboration of harmonised regulatory guidelines and/or mandatory rules in CEPT countries on how to deal with CLI inter alia:
- the definition of unambiguous technical rules for determining which traffic qualifies as spoofed;
- the clear determination of the respective responsibilities of the different operators handling a spoofed call;
- imposing sanctions for entities and/or persons who are responsible for CLI spoofing;
- offering more legal certainty, if needed, for operators that block traffic as a result of suspected CLI spoofing activity;
- the support and encouragement of information sharing initiatives on CLI spoofing between operators;
- the encouragement of the installation by operators of traffic pattern analyses tools based on artificial intelligence;
- study or propose solutions to address the extent to which 'interconnection surcharges' can be levied by terminating or transit operators, in justified circumstances, in full conformity with the delegated regulation (EU) 2021/654 setting the Eurorates.

3 to consider and to develop the roll-out of a European harmonised approach to call traceback;

4 to consider an ECC Recommendation on blocking mechanisms implemented at international gateways for incoming traffic originated from suspected spoofed national E.164 numbers;

5 the further analysis of technical methods such as STIR/SHAKEN, AB Handshake, SOLID, and Distributed Ledger Technology (e.g. Blockchain) with the aim of eliminating CLI spoofing taking into account the following criteria:
- avoiding national fragmentation as much as possible;
- minimising the impact on the networks (e.g. non-IP networks) and costs of implementation and management;
- ensuring compliance with EU- and national legislation on privacy;
- developments in other geopolitical regions;
- forward-looking potential of the choices to combat other types of fraud and abuse.

6 a coordinated roll-out of the chosen approach in CEPT countries.

ANNEX 1: LIST OF REFERENCES

[1] ECC Recommendation (19)03: "Measures for increasing Trust in Calling Line Identification and Originating Identification", approved November 2019

[2] ECC Report 248: "Evolution in CLI usage – decoupling of rights of use of numbers from service provision", approved April 2016

[3] ECC Report 275: "The role of E.164 numbers in international fraud and misuse of electronic communications services", approved May 2018

[4] Norwegian Regulations on electronic communications networks and electronic communications services (Ecom Regulations). Available here (Norwegian only)

[5] Ofcom UK - General Conditions of Entitlement - Unofficial Consolidated Version. Available here

[6] Recommendation ITU-T E.164: "The international public telecommunication numbering plan", November 2010

[7] The UK's National Telephone Numbering Plan. Available here

[8] Ofcom UK: "Guidance on the provision of Calling Line Identification facilities and other related services", 30 July 2018. Available here

[9] Decision No. 1/20 of the Board of the Latvian Public Utilities Commission - Regulations Regarding the Elimination of Fraud Using Numbering - Adopted 3 December 2015. Available here

[10] Latvian Electronic Communications Law. Available here

[11] Decision of the Council of the Public Utilities Commission No. 1/13, Riga, March 30, 2017 (protocol No. 13, item 6). Electronic Communications Network Technical and Operational Regulations for the Interconnection Service. Available here

[12] Decision of the Council of the Public Utilities Commission No. 1/35, Riga, December 20, 2018 (protocol No. 54, item 7). General Authorisation Regulations in the Field of Electronic Communications. Available here

[13] Decision no. 2012-0856 of the Regulatory Authority for Electronic Communications and Posts dated July 17, 2012 amending the organisation of number ranges starting with 08 and short numbers provided for in Decision No. 05-1085 of December 15, 2005 (Page 35). Available here (French only)

[14] News Article: "Orange, the driving force behind the fight against abusive door-to-door sales, has blocked 111 million spam calls", 12 December 2019. Available here (French Only)

[15] Decision No. 2019-0954 amending the decision establishing the national numbering plans and its management rules, 11 July 2019. Available here. (French only)

[16] Decision No. 2014-1485 of the Regulatory Authority for Electronic Communications and Posts dated December 9, 2014 on the determination of the relevant markets for the termination of voice calls on fixed networks in France and the termination of voice call on mobile networks in France, the designation of operators having a significant influence on these markets and the obligations imposed on this title for the period 2014-2017. Available here. (French only)

[17] Decision No. 2017 1453 of the Authority for the regulation of electronic communications and postal services dated December 12, 2017, relating to the determination of the relevant markets relating to the termination of voice calls on fixed networks in France and the termination of voice call on mobile networks in France, the designation of operators having a significant influence on these markets and the obligations imposed on this title for the period 2017 2020. Available here. (French only)

[18] German Telecommunications Modernisation Act (TKMG), 23 June 2021. Available here. (German only)

[19] Recommendation ITU-T E.156: "Guidelines for ITU-T action on reported misuse of E.164 number resources"

[20] Recommendation ITU-T E.157: "International calling party number delivery"

[21] IETF RFC 7340: "Secure Telephone Identity Problem Statement and Requirements"

[22] IETF RFC 7375: "Secure Telephone Identity Threat Model"

[23] IETF RFC 8224: "Authenticated Identity Management in SIP"

[24] IETF RFC 8225: "PASSporT: Personal Assertion Token"

[25] IETF RFC 8226: "Secure Telephone Identity Credentials: Certificates"

[26] ATIS 1000074: "Signature-based Handling of Asserted information using toKENs (SHAKEN)"

[27] ATIS 1000080: "Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management"

[28] ATIS 1000081: "Technical Report on a Framework for Display of Verified Caller ID"

[29] ATIS 1000082: "Technical Report on SHAKEN APIs for a Centralised Signing and Signature Validation Server"

[30] ATIS 1000084: "Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators"

[31] ATIS 1000085: "SHAKEN Support of “div” PASSporT"

[32] BEREC BoR(13)37 on “Article 28(2) USD Universal Service Directive: A harmonised BEREC cooperation process - BEREC Guidance Paper

[33] ITU-T Technical Specification FG DLT D1.1: “Distributed ledger technology terms and definitions”, August 2019

[34] ITU-T Technical Report TR.spoofing (06/2021): “Countering spoofing”

[35] Recommendation ITU-T Q.3057 (04/2020): “Signalling requirements and architecture for interconnection between trustable network entities”

[36] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. Available here.

[37] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Available here.

[38] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

[39] Commission Delegated Regulation (EU) 2021/654 of 18 December 2020 supplementing Directive (EU) 2018/1972 of the European Parliament and of the Council by setting a single maximum Union-wide mobile voice termination rate and a single maximum Union-wide fixed voice termination rate (Text with EEA relevance). Available here.