Response to Ofcom Consultation (28th April 2023): Calling Line Identification (CLI) authentication – a potential approach to detecting and blocking spoofed numbers.

XConnect welcomes the opportunity to respond to this consultation. We support Ofcom's open approach to understanding the various steps which can be taken towards implementing authentication and validation of call traffic in the UK and we support Ofcom's objective of creating trust in numbers to protect end users from receiving harmful and malicious calls.

We believe this supports the government's recently announced Fraud Strategy to make scam calls harder for fraudsters through 'spoofing' numbers of legitimate UK businesses.

Introduction to XConnect

XConnect[1] provides a trusted global registry of network and subscriber information, based on privacy compliant phone number data, including global number portability, global number ranges/prefixes and mobile phone subscriber status.

Established in the UK in 2005, XConnect delivers mission critical carrier-grade numbering information services to over 200 operators globally, including MNOs, business messaging (A2P) hubs, aggregators, carriers and interconnect providers. XConnect is an ISO 27001 certified company and annually processes nearly 50bn queries per year.

Our number information services are used for voice and message routing, fraud protection, phone number validation as well as fraud mitigation and risk scoring. XConnect also supports the deployment and evolution of next-generation communications, such as VoLTE[2] and RCS[3]. Our Number Information Services[4] are accessed through our global distributed hybrid cloud platform using simple, secure, scalable real-time protocols and APIs.

In 2020, XConnect was acquired by Somos, Inc., a USA-based company providing number information and services to over 1,400 organisations, and the trusted USA telecom sector administrator for over 3 billion numbers throughout the USA and North America. Somos helps to enable seamless communications between enterprises and consumers through the management of the USA regulatory agency's ("FCC") mandated databases including North American Numbering Plan ("NANP"), Toll-Free Number Administrator ("TFNA") and the Reassigned Numbers Database ("RND"). In addition, Somos administers the USA's largest Do Not Originate ("DNO") list.

First Steps

XConnect agree that technology has been a significant enabler for bad actors to continually find new ways to cause harm, that trust must be restored in the number being displayed to enable end users to use communications without being fearful of the outcomes. That trusted communication can only be achieved where there is a verified CLI that the End User can have faith in being correct and that the number presented represents a legitimate call.

[1]About Xconnect: https://www.xconnect.net/about-xconnect/

[2]VoLTE - Voice over Long-Term Evolution (VoLTE) is a LTE high-speed wireless communication standard for mobile phones and data terminals

[3]RCS - Rich Communication Services protocol is designed as a modern take on texting that rolls features from Facebook Messenger, iMessage, and WhatsApp into one platform

[4]About XConnect Number Information Services: https://www.xconnect.net/services

The CLI sanity checks which Ofcom has recently implemented[5] to validate the CLI against the authoritative National Number Plan number information and Do Not Originate ("DNO") checks are important first steps which we strongly support in the journey to restoring trust in the CLI. Know Your Customer ("KYC") and Right to Use ("RtU"), including the presentation CLI, we believe, underpin a variety of opportunities and options which the UK industry could implement to create trust in the CLI presentation. We would suggest that these steps are the first of many joint initiatives necessary between industry and Ofcom, but which must also be underpinned by regulated interventions in order to achieve the ultimate goal of "trusted communications".

We appreciate, in the short term, that full end to end checking of all CLI types, regardless of whether the calls originate nationally or internationally, or are IP or TDM, is unlikely to happen and therefore Ofcom cannot realistically demand blocking of all untrusted calls with a big bang approach without impacting many legitimate calls. Yet, without a comprehensive approach covering all call types (national & international, IP & TDM) fraudsters will continue to take advantage of any holes in network checks carried out in the call routing, therefore we will continue to see 'attacks' move to these non-verified call types. "Whack-a-mole" is often the term used to best describe how the industry chases fraudsters around call types and networks today and this will be especially true if avenues such as TDM and international remain open.

While we have focused on voice, the same concept and goals of "trusted communications" applies equally to messaging (SMS, RCS) both for businesses and personal messages and therefore we believe it would be beneficial for government, regulators and industry to develop and recognise a roadmap towards a converged solution in due course.

We note two significant global industry bodies i.e. the i3forum[6], who have for the past 17 years represented international communications for voice, and the MEF[7] (Mobile Ecosystem Forum) which represents the global business messaging sector, are both actively developing solutions and structures to support trusted communication in their respective domains. XConnect recognises that each domain (voice/message) should initially develop and implement their own initiatives but strongly believes that we should be working towards a global unified approach which will be the only course of action to combat fraud and abuse of communications.

We would recommend to Ofcom that there are a variety of solutions which enable a hybrid mix of cost-effective solutions to support the outcome of a "Trusted Call", notably the concept of a 'regulated CLI Trusted Identifier' as outlined in the following section, which will enable informed choice, allowing the end user to recognise the validity of the call and therefore, to answer or ignore the call.

We also note that ComReg has recent published their consultation[8] "*Combatting scam calls and texts Consultation on network based interventions to reduce the harm from Nuisance Communications",* which is proposing a combination of ways that the industry could implement checks on inbound calls and messaging, therefore establishing a broader approach to stopping harm.

Trusted Identifier

We would urge Ofcom to consider an alternative approach which should be technology neutral. We suggest the introduction of a new concept of regulated "Trusted CLI" which is identified by a trusted CLI indicator and will provide the validity the end user requires to trust the call.

[5]Statement: Improving the accuracy of Calling Line Identification (CLI) data. https://www.ofcom.org.uk/consultations-and-statements/category-2/improving-cli-data-accuracy
[6]https://i3forum.org/, an industry body driving global collaboration and innovation.
[7]https://mobileecosystemforum.com/, has members from 45 countries. MEF's SMS SenderID Protection Registry was established to automate cross-stakeholder processes to reliably and quickly share information to facilitate an orchestrated blocking system.
[8] https://www.comreg.ie/comreg-consults-on-combatting-scam-calls-and-texts/

There are several ways which a “Trusted Identifier” can be presented to the end user, for example, for a smartphone this could be a regulated green tick or for fixed line with a simple CLI alpha numeric display where the trusted indicator mark “**” or “v” (verified) could be a prefix or suffix to the CLI. This easily recognisable regulated trust mark enables the end user to have informed choice: answer, be aware or ignore the call.

XConnect recommend Ofcom mandate a Trusted Identifier be displayed to the end user to indicate a “Verified Call” which the Terminating Network Operator (“TNO”) (or a call trust APP on the device) would only classify when the call’s legitimacy is “beyond reasonable doubt” (the UK legal definition as used in criminal cases). This places a clear onus and responsibility on the UK industry to only issue the Trusted CLI Indicator when a call is “beyond responsible doubt”. However, this does allow industry to develop a variety of technology, contractual and process solutions to support the responsibility and use of a trusted CLI indicator.

This approach is technology, process and methodology neutral allowing industry and CPs to develop relevant solutions allowing differences such as national or international, IP or TDM (and eventually SMS, Business Messaging) to be accommodated in the most efficient and viable way. No one solution will address all call types (international, national, TDM or IP). However, it would allow for a hybrid solution of multiple technological and industry solutions which would be applicable in different situations and allow the TNO to only apply the regulated Trusted Identifier (green tick “**”) once they are satisfied ‘beyond reasonable doubt’ of the call’s CLI legitimacy. This allows the TNO to be held accountable if the call is proven to be slamming, spamming, scamming, spoofing, etc. by ensuring the originator can be traced. Overall, the solution is restoring trust in the CLI, therefore helping to reduce or eliminate CLI spoofing.

The approach will also indirectly reduce nefarious calls such as spamming, phishing, scams since with a trusted CLI, the ultimate originator of the call will be able to be identified by the relevant authority. The green tick or “**” will ultimately enable the authorities to identify the originator as the foundation in KYC and RtU will enable appropriate action to be taken to deal with the bad actor/ business.

Today, there are four potential ways which a trusted call, enabling the CLI to be “beyond reasonable doubt”, could be achieved:

- STIR/SHAKEN
- Trusted Trunks & Trusted Traffic
- i3Forum CLI SafeZone
- Out-of-Band SHAKEN

It is likely that a hybrid solution including some or all of the above would be useful to provide a trusted communications solution addressing TDM, IP, national and international.

Below we provide further detail with respect to each of the elements suggested above.

STIR/SHAKEN

Whilst STIR/SHAKEN is a viable technology, it will however incur considerable network upgrade and deployment costs. The introduction of STIR/SHAKEN in the USA required substantial industry costs to upgrade or develop / modify every SIP component involved in the call path from the Originating Network Operator (“ONO”) via all the transit carrier steps to the TNO. Our anecdotal evidence indicates the upgrade and development costs in the USA were approximately $1bn (including SIP firewalls, SIP proxies, SIP routing platforms and SBCs), all of these elements are likely to require material level vendor licensing upgrade costs and or development, as well as testing / deployment costs for a UK variant.

In addition, the NICC STIR/SHAKEN recommendation is a UK variant of the USA STIR/SHAKEN and this may mean the UK vendor licence cost could be even higher than the USA equivalent due to the extra costs of creating a further version of STIR/SHAKEN.

Given that vendors are working in a global marketplace, any regional or country specific version of any measures are likely to add considerable cost. Such additional costs, as highlighted above, will ultimately flow through to the end user.

Annex 1 (USA - implementation of STIR/SHAKEN) provides additional detail regarding our comments on USA STIR/SHAKEN implementation which is limited to national IP calls. By excluding national TDM or international origination the USA, by omission, has effectively pushed the illegitimate traffic to these routes which do not require checks.

If this method is to be implemented in the UK, we urge Ofcom to provide guidance to TNOs as to how they must treat calls including the presentation to the end user (e.g. block, allow, mark as spam, mark as trusted). As detailed in Annex 1, the FCC did not provide instructions to the TNO and this element of any STIR/SHAKEN solution still allows for uncertainty for the end user and does not provide informed choice.

Trusted Trunk – a national and international solution.

This is a contractual solution which can be implemented between the ONO and terminating CPs where direct routing exists and a dedicated trunk is specified for the delivery of verified CLI calls. This solution is predicated on the existing obligations to Know Your Customer ("KYC") and Right to Use ("RtU") of the CLI to ensure they are authorised to use the number allocated to them. Note however, that calls which originate from ONOs where KYC has not been carried out (e.g. PAYGO mobiles) needs clarification. As this solution allows the TNO to be confident all the checks necessary to enable them to apply the Trusted Indicator have been undertaken.

The 'trusted' direct route relationship providing an end to end trust in the CLI calls could be extended to enable wholesale or transit operators to offer aggregated trusted trunk solutions enabling greater efficiency. We propose that Ofcom and industry should develop a framework which defines trusted trunk and the associated existing obligated minimum checks.

Some cloud solutions for enterprise customers may select the presentation of their own CLI, however, these solutions should only be enabled where KYC and the RtU CLI checks have been enforced.

This element of a mix of solutions does not require costly upgrades of all UK networks and could be available much sooner than the implementation of All IP STIR/SHAKEN.

We understand, in the messaging world, a similar concept of trusted trunk has been deployed by [redacted] and in addition this concept is being developed in the i3 Forum for voice.

Out-of-Band SHAKEN – a solution supporting national, international, TDM, IP and potentially messaging.

Out of Band ("OOB") SHAKEN enables CLI Attestation & Verification, though only requiring the ONO and TNO to support this technology and, in addition, it does not require any support from the transit carriers in the call path. Overall, the technology requirements and cost/effort to implement would typically entail less impact/cost for operators to implement, as well as not requiring an obligation on the transit operator, versus traditional in-band STIR/SHAKEN.

Therefore, OOB can be used in many situations which would be more challenging for traditional in-band STIR/SHAKEN e.g. transit, international calls (with unknown or hybrid IP / SS7 transit). This solution also supports future capabilities such as rich call data – Branded Caller Name, Branded Logo

etc. are likewise feasible under OOB. Further details on how this solution could be implemented are found in Annex 2.

There are multiple providers of this out-of-band solution existing today and standards are being enhanced to enable multiple OOB providers to work in parallel, so at a national level for example, it would not require an exclusive OOB provider. It is reasonable to expect that the overall cost to the industry would be much less than the in-band solution of STIR/SHAKEN.

i3Forum CLI SafeZone – international solution

This solution is primarily an international initiative being developed by the i3forum which is being discussed at the GSMA and is an extension of trusted origination. An example would be if a call originated in France under the local STIR/SHAKEN obligations and is terminated in the USA under different STIR/SHAKEN obligations. This call would be considered originating from a SafeZone even though the originating and terminating zones consists of differences in governance, technical solutions and certification structures but both entities are independently trusted domains. Therefore, the call would be checked and trusted at origination and the TNO would accept the checks carried out at origination in order to apply the Trusted Indicator.

This solution is primarily aimed to facilitate the concept of Trusted Calls international calls.

Interim Summary

As previously mentioned, KYC and RtU must be enforced as they provide the foundation for other technical solutions such as Trusted Trunks, SafeZone, STIR/SHAKEN and Out of Band SHAKEN. These alternative solutions can be more easily and quickly implemented than pure STIR/SHAKEN and would provide joined up solutions for national, international, TDM and IP.

The concept of regulated Trusted CLI would become a foundation for more advanced trusted communication services, which is noted by Ofcom in 4.40 c), such as Branded Caller ID services. These services could include: Branded Call, Brand Logo and a reason code. [redacted]. However, these branded calling services are only viable once there is a trusted CLI, for example using a regulated trusted CLI marker. These should be provided and displayed, only when the TNO / Terminating Device are “beyond reasonable doubt” – using the concept of the regulated Trusted CLI indicator. If there is no recognisable Trusted Identifier supporting the presentation of a business brand name or logo, the current situation of spoofing will be made much worse as end user confidence will be eroded.

In due course, with the adoption of an appropriate mix of hybrid solutions to manage all traffic streams (national, international, IP and TDM), the vast majority of calls would be marked as a Trusted CLI, greatly reducing the avenues which bad actors are able to utilise.

We note in clause 4.48 that Ofcom states there are two high level components required to achieve assurance (namely a method to convey information along with the call and a framework of tools, processes and governance to support multilateral interworking). As discussed above, we would propose this journey should include a variety of solutions to support the UK market and, following Ofcom’s initial steps which have been recently implemented, we believe the proposals outlined below support the intended outcome and the closure of all potential loopholes.

However, any further phases must be mandated by Ofcom to achieve the desired outcome and should be implemented over the immediate and short term. Listed below are six solutions which we suggest support a hybrid mixed approach.

Comments on Current Regulations

The checks which have recently come into force must be the basic minimum treatment that the number being used are validated against. In addition to these basic steps, we strongly recommend

international validation is carried out against Global Number Plans – based on publicly available information from NRAs. This information is also provided by associations such as i3forum number plan initiative and commercial service providers such as XConnect and can be easily enabled.

DNO checking.

We fully support the steps taken by Ofcom to date to utilise this information and would urge Ofcom to expand the list to include mobile numbers including [redacted]. There are various low-cost products, solutions and global industry associations which support the management of these data sets[11] available today which can be easily deployed on an operator-by-operator basis from multiple suppliers.

As demonstrated in other countries,[12] this method needs to be scaled up to support hundreds of thousands and more numbers. [redacted] In our previous submission to Ofcom, we suggested that the DNO could be substantially more effective if the list were to include a broader set of information. For example, it could include Government departments, old banking numbers such as 0845x and CPs unallocated numbers or numbers only allocated for internal use. In the USA, conferencing and numbers used for internet advertising which are in-bound only take advantage of DNO.

Other Comments on the Consultation

"Is Roaming" checks. XConnect fully supports the steps Ofcom have previously taken with respect to roaming and would suggest these can be expanded to a national CLI originating on an international trunk. The four legitimate use cases today (section 5.40) do not accommodate blanket blocking. We would recommend that before blanket blocking can be achieved there are viable solutions to address these legitimate use cases.

The first example is where a mobile number legitimately roaming abroad requires a particular solution querying the MNO Home Location Register (HLR) to confirm the number is actually roaming and therefore, if not confirmed as legitimate, the call would be blocked [redacted] Other solutions being investigated or implemented are shown in the table in Annex 4. Additionally, the i3Forum is looking to encourage sensible and viable architecture and technology to support these checks.

Further examples of legitimate national presentation on international routes are that of an outsourced cloud call centre and enterprise international DDIs solution. For example, a USA company with a UK DDI to show local presence. As mentioned above, solutions such as Out of Band STIR/SHAKEN and Trusted Trunk are being looked at to address these examples. Again, these calls should only be allowed if the call is validated 'beyond a reasonable doubt'.

This is a very dynamic area across the globe with many NRAs and governments looking at the issue of trusted communications for both voice and messaging and potential solutions. The table in Annex 3 provides a snapshot of our current understanding of various international initiatives. We urge Ofcom to work with other international bodies, such as the i3Forum, to develop international attestation.

Technology Neutral Solutions. As previously mentioned, no one technological solution will address all call types (international, national, TDM or IP). Any proposals need to allow for a hybrid of multiple

[9]MSNRs, Mobile Station Roaming Number, used by mobile operators to facilitate roaming services.
[10]Global Title, (GT) is an address used for routing messages within Signalling System Number 7 (SS7)
[11]The i3Forum has a number plan working group. To enable ease of access operators are not required to be members of i3Forum. https://i3forum.org/
[12]Annex 4, Robocalling Table

technologies and industry solutions which are applicable in different situations. As mentioned above, the i3Forum and the GSMA are developing international and potentially national solutions; STIR/SHAKEN, Trusted Trunks & Trusted Traffic, CLI SafeZone and Out-of-Band Stir all provide a mix of applications. These solutions in turn provide legitimate calls for services such as offshore call centres and enterprise international DIDs.

Traceback. National solutions like the Industry Traceback Group ("ITG"[13]) which is a USA solution utilising a Spam Mitigation Operator list, ideally to be provided as a searchable database, helps identify SPAM/SCAM originators. We fully support these initiatives and encourage the concept of international traceback which allows the originator to be identified and, where applicable, for legal action.

International traceback. XConnect fully support this concept and encourage Ofcom with respect to this element as to eradicate illegitimate calls clearly requires a global unified solution which is why the i3forum is actively engaged on this topic and actively engaging with NRAs globally.

International Collaboration

As discussed, we recommend to Ofcom that any solutions should be viewed in the round and not, for example, limited to national traffic. Without addressing international inbound calls, any solutions will only provide limited protection to the end user. International traffic should be addressed with international collaboration in order to avoid a myriad of different in-country solutions for international calls, in turn creating a disjointed approach and providing a loophole for bad actors to exploit. Various organisations are today exploring and developing international solutions, an example includes the i3Forum and collaborations between CCA[14], CCUK[15], CDRT[16] and other national associations.

Conclusion

If you accept the premise of a hybrid mix of a variety of solutions, predicated on KYC and RtU, industry does not need to wait for the IP migration to be completed before it can implement solutions to address loopholes. Once in process, this will reduce options available to fraudsters and the game of "Whack a mole" will gradually peter out. Many of the solutions suggested by XConnect are already available, are technology neutral and considerably lower cost to implement than STIR/SHAKEN.

If Ofcom mandates that all calls will be approved, legitimate and trustworthy, it follows that competitive and commercial forces will rapidly drive adoption. End users, using informed choice, over time will move towards only answering calls with the Trusted Identifier as we believe the implementation of branded calls or company logos accompanying calls will become the commercial and business driver for early adoption.

If Ofcom publicises the concept of regulated trusted CLI indicator to the general public enabling UK citizen, consumers and businesses informed choice, this will then encourage the industry to adopt trusted communications.

We would strongly recommend that Ofcom considers the various solutions as a holistic approach to stop the growth of fraudulent and misuse of telecoms.

[13] https://tracebacks.org/ - Industry Traceback Group
[14] https://www.cloudcommunications.com/ - Cloud Communications Alliance.
[15] https://commscouncil.uk/ - Communications Council UK,
[16] https://www.cdrt.fr/. The CDRT: Think Tank of the unified communications market.

XConnect
A Somos Company

Annex 1 USA - Implementation of STIR/SHAKEN

As has been seen in the USA, the implementation of STIR/SHAKEN has been an important first step but has not provided the ultimate answer and was never intended to be the ultimate answer. It is also worth noting that the implementation of STIR/SHAKEN in the USA has had mixed results. One recent report highlights the benefit of reduced volume of robocalling[17] and while Youmail[18] points to robocalling having risen from 4bn/m in 2022 to 5.1bn/m.

The GSMA RIFS: *Spoofing Against Spoofing: Towards Caller ID Verification in Heterogeneous Telecommunication Systems* research paper[19], references public data showing that since STIR/SHAKEN, which was mandated in June 2022, has not been as effective as expected.

> *First of all, after the mandate of STIR/SHAKEN, the number of robocalls actually went up and reached a record of 5.5 billion calls in October 2022. Many of the robocalls are now signed with STIR/SHAKEN to look more legitimate. Among all the signed calls with the B-attestation, about a quarter are robocalls; for calls signed with the C-attestation, about a third are robocalls. Many of these signed robocalls present a different caller ID from where they are calling. The statistics also show that although nearly 70% of the outbound VoIP calls are signed with STIR/SHAKEN, only 15-24% of the calls received by the terminating networks have valid signatures; for many calls, the signatures are removed as they traverse intermediate non-IP networks. It is also reported that many calls are signed with wrong attestation levels, which should not be surprising given that STIR/SHAKEN only authenticates the ''carrier'' and the attestation of the caller ID is entirely based on the carrier's ''word of mouth''.*

Other articles point to the rise in robotexting as the newly favoured method by bad actors. Therefore, it is still early in the USA implementation to assess fully the impact of STIR/SHAKEN.

Robotexing is proving to be the latest channel of attack on end-users and this has been recognised by the UK government in the recent consultation *Preventing the use of SIM farms for fraud*[20] which specifically mentions scam texts. Even with the implementation of STIR/SHAKEN, the methods used by bad actors are continually developing.

The implementation in the USA focused solely on the originating call and didn't provide guidance to the TNO with respect to the actions they are permitted to take (or not) when terminating the call and therefore what the end-user should expect to see to give them trust in the call.

We strongly suggest that Ofcom must consider all elements of the call routing and appropriate checks. If the TNO is not obligated to provide the end user with specific information (acknowledgement the call can be accepted) the call termination will be open to interpretation. We believe without clear guidelines on the presentation of a call to the end user on how the TNO can handle (block or mark) an inbound call, there is a significant risk of the current situation being made worse.

A mix of options when suspecting the legitimacy of the call could be blocking, marking as suspect or do nothing and deliver as normal, whether the call is attested or not. We would strongly urge Ofcom to provide clear guidance or mandate to the TNO the actions they should perform on the inbound

[17] https://www.robokiller.com/robocall-insights

[18] YOUMAIL https://robocallindex.com/ Press - https://www.prnewswire.com/news-releases/us-consumers-received-over-5-billion-robocalls-in-may-according-to-youmail-robocall-index-301844605.html

[19] GSMA RIFS: Update on Research "End to End Authentication of Caller ID in Heterogeneous Telephony Systems" report provided separately.

[20] https://www.gov.uk/government/consultations/preventing-the-use-of-sim-farms-for-fraud

call when it is questionable and to oblige the TNO to clearly 'mark' the call for the end-user with a Trusted Identifier, such as a green tick.

The USA also highlights the potential costs involved in implementing STIR/SHAKEN. While there will be costs associated with the management of the certification function this is likely to be dwarfed by the cost smaller and older networks may see in order to implement necessary upgrade their networks.

The cost of implementation is not the platform to support certification. Our anecdotal evidence indicates the upgrade and development costs in the USA industry were approximately $1bn (including SIP firewalls, SIP proxies, SIP routing platforms and SBCs) all of these elements are likely to require material level vendor licensing upgrade costs and or development, as well as testing / deployment costs. Without a CDB, and only partial attestation (see NICC submission) a "partial solution" is likely to see higher costs and even lower success than USA STIR/SHAKEN. Additionally, without a CDB any implementation is likely to be inefficient and not achieve proportional outcomes to the costs involved.

We believe the outcomes in the USA to date support the view that to mandate a big bang single technology solution approach is unlikely to achieve the desired effect and is not the answer.

XConnect
A Somos Company

Annex 2 – Out of Band SHAKEN

Introduction
Out of Band ("OOB") SHAKEN enables CLI Attestation & Verification, through only requiring the ONO and TNO to support this technology and in addition it does not require any support from the transit carriers in the call path. Overall, the technology requirements and cost/effort to implement would be typically less impact / cost for operators to implement, as well as not requiring an obligation on the transit operator, versus traditional in-band STIR/SHAKEN.

Therefore, OOB can be used in many situations which would be more challenging for traditional in-band STIR/SHAKEN e.g., TDM transit, International Calls (with unknown or hybrid IP / SS7 transit). This solution supports future capabilities such as rich call data – Branded Caller Name, Branded Logo etc. are likewise feasible under OOB.

Technical Implementation
The heart of OOB is in essence a real time matching between the originating operator and the terminating operator (or relevant entities on their behalf) that a call with Caller ID X and Termination number Y has been generated by the originating operator and received by the terminating operator. Thus attesting that this call with this Caller ID is attested & verified. Solutions of this nature are now available in live production.

The Out of Band SHAKEN specification is specified by ATIS in ATIS-1000096.

This Out of Band (OOB) specification does not take away SHAKEN obligations from the originating service provider (OSP) and the terminating service provider (TSP).

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

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

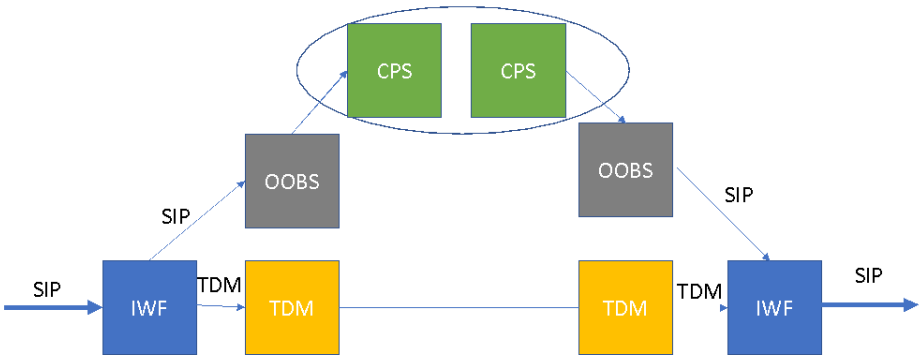
To satisfy OOB, a few new components are added to the SHAKEN framework:

STI-CPS (Call Placement Server):
This is an entity that can receive a PASSport from a service provider for eventual retrieval by another service provider responsible for onward transit or termination. These can exist alone or as a network of STI-CPS that allows for exchange of PASSports within the network.

STI-OOBS (Out of Band Service):
This service is an entity in a service provider's network that publishes the PASSports to the STI-CPS.

STI-IWF (Inter Working Function):
This is a component that performs SIP-TDM signaling and vice versa.

The architecture is as shown below:



Future Roadmap

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

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

Annex 3 *Various National Approaches to Robocall Protection for International Incoming Calls (and Messages)*

	1. CLI Securing Solutions		2. CLI Validating Solutions			3. Roaming Status Checks		4. SMS compliance
	STIR/SHAKEN - Domestic	International	CLI Sanity Checks	DNO	Action	National	International	CLI and DNO
US	US/Canadian version	Intnl Gateways (June '23)	Yes	Yes	No	N.a.	N.a.	CLI Validation and DNO in 2023 - Industry : TCR
Canada	US/Canadian version	N.a.	Yes		No	N.a.	N.a.	
France	French version	N.a.	N.a.	[Yes]	Blocking	N.a.	N.a.	[DNO]
Australia		On international inbound	Industry Code C661		Blocking	N.a.	N.a.	CLI Validation and DNO
Belgium	N.a.	N.a.	CLI guidelines BIPT		Blocking	N.a.	N.a.	
Latvia	N.a.	N.a.	CLI guidelines NRA		Blocking	N.a.	N.a.	
Norway	N.a.	N.a.	Regulation and Nkom Operator agreement 01.09.22		Blocking	N.a.	N.a.	
UK	Consultation June '23	"	CLI guidelines Ofcom National CLI (except mobile)	Yes	Blocking **(non mobile)**	Under study	Consultation (June '23)	- UK Government initiative (May '23) - Industry : MEF SenderID Reg
Finland	N.a.	N.a.	Guidelines Traficom National CLI (except mobile)		Blocking & CLI Removal	Based on API call	Via SS7 SRI-SM access	
Poland	Under study	N.a.	CLI guidelines UKE		Blocking	Based on API call	CAMEL triggering	
Germany	N.a.	N.a.	For specific CLI ranges		CLI Removal	N.a.	CAMEL triggering	
Saudi Arabia	N.a.	N.a.	N.a.		Blocking	Based on SS7 ATI	N.a.	
Oman	N.a.	N.a.	N.a.		Blocking	Based on SS7 SRI-SM	N.a.	
China	N.a.	N.a.	N.a.		Blocking	N.a.	N.a.	
Ireland	Under study	"	Fixed line	In progress >75% complete in operators	Blocking	Under study	Under study	Industry : MEF SenderID Reg
India	N.a.		AI/ML-based filtering May 2023		No	N.a.	N.a.	SMS Blocking of unregistered SenderIDs
Malaysia	N.a.							May 2023 – block SMS containing URLs