ONE CONSORTIUM

# White Paper – Call spoofing protection mechanisms

Release 1.0 – November 2025

Working Group 4

## FOREWORD

This document explains the basic mechanisms of international calls and the mechanisms that can be used to detect spoofing with special focus on roaming checks.

One Consortium

## CONTENTS

## 1. Document purpose

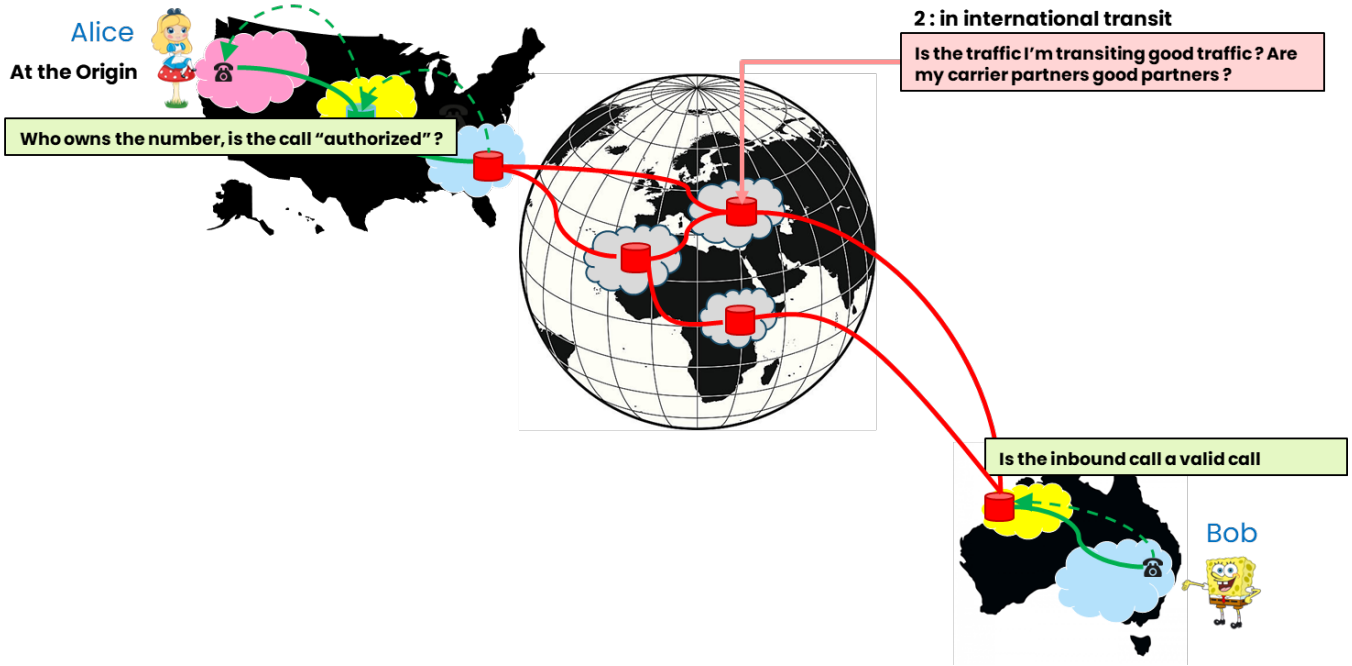
This document is intended to be an overview of mechanisms to detect spoofing and specifically tools to validate national numbers are not spoofed. It is intended to be a reasonably non-technical overview for regulators and policy makers to understand the options available.

## 2. Introduction

The restore trust initiative aims to help restore faith in the calling line identity (CLI) visible when a phone call is received. This CLI should be the phone number of the originating party (the A party), but the technology of telecommunications networks and the complexity of interconnecting parties makes it straightforward to manipulate this number at the origin or along the signalling path.


The focus of this document is on the international calling case, as for networks (and for regulators) the national scenarios are easier to control.

Ultimately if I am to trust a call, I need to know and trust the person or company making the call and I need to be confident the phone number of the caller hasn't been non-legitimate modified (i.e. spoofed) either at the origin or in transit.



Trust in a phone number can be achieved by experience interacting with the person or enterprise associated with the number or by the home telco validating their identity.

Validating the owner of a phone number and the right to use a number requires both know your customer (KYC) checks on the enterprise or subscriber as well as on the communication use-cases and mechanisms to tie the connection, phone device and phone number to the user's identity and communication use-case. KYC is however outside the scope of this document and is covered in other One Consortium documents. This document discusses the deliberate and non-legitimate modification of a phone number to impersonate an identity by using its CLI.

Stopping illegitimate spoofing will not completely eradicate scams, it will however mean that the phone number of the scammer would be visible and can be traced back. Being confident the CLI has not been changed from its origin means the called party can have a greater level of trust based on past communication from that CLI. If a subscriber receives a call from a known number (e.g. in their contacts) then without spoofing the subscriber knows the caller and can make a judgement on who to trust. If the number is unknown to the subscriber, they must rely on KYC processes run by the home network.

An excellent overview of the issue can also be found in the Europol Call ID spoofing position paper (ISBN 78-92-9414-055-5).

## 3. CLI manipulation

### At origin

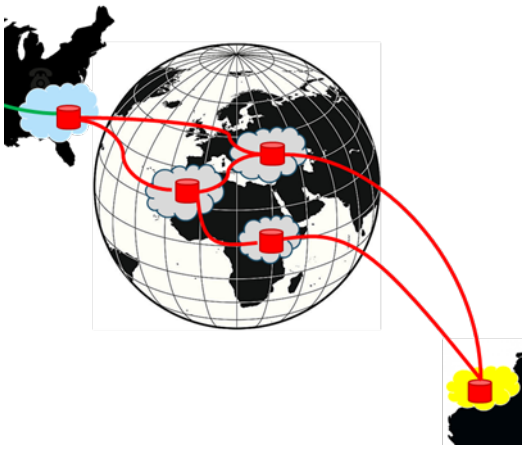
User agents that allow the CLI to be manipulated are readily available, typically for use on (fixed line) SIP phones. Without checks by the origin network that the connected gateway is authorised to use that CLI it is then simple to spoof any CLI.

On a mobile network spoofing is much more difficult as the CLI is tied to the SIM and thus validated as associated with a subscription and any associated KYC. However a fixed line SIP user agent can spoof a mobile CLI so in practice any CLI can be spoofed at the origin.

Most malicious spoofing is done at the origin.

### In transit

A call may dynamically transit several carriers between the call origin and its destination. At each stage particularly with IP telephony (SIP) the call parameters can be easily changed. Usually, for privacy of subscribers and networks, parameters that identify the origin device and network are removed at each hop making spoofing detection during transit (and traceback) very difficult.



## 4. Call scenarios

Not all calls are the same. The way calls flow depends on the technology, whether the parties are fixed or mobile and the location of the A and B party. The protection provided at home may, for example, be different to that provided when roaming. Similarly, the protection on national CLIs may be different to that provided on international CLIs.

We must consider not just the normal call flows, but also the edge cases. This is because fraudsters and scammers will exploit any “useful” edge cases where they exist and are not controlled.

In most (but not all) countries different number ranges are allocated to fixed and mobile and so it is easy to determine if a call originates from a fixed or mobile device. This document does not deal with the complexity of determining whether a number is fixed or mobile.

The scenarios below are considered in the context of the B party receiving the communication – i.e. “home” is the home country of the destination subscriber

### National calls

Calls that originate and terminate within one country will typically have direct connections (or limited and trusted intermediaries) from the origin network (A party) to the terminating network (B party). Controls in place at the origin network can be used to link the identity of the originator to the device and phone number.

Checks in place at the origin network can therefore ensure trust in the CLI delivered to the destination network.

For a mobile network the phone number (MSISDN) is securely tied to the SIM and so difficult to spoof from the mobile device For fixed line KYC controls by the origin operator (e.g. Allowed CLI for that IP/user agent) should ensure confidence in the CLI.

The entirely national call case is therefore not dealt with in more detail in this document as it is inherently more secure and KYC checks and CLI preservation (and signatures to protect manipulation) can be mandated by local regulation.

### National CLI

Calls originating from a national subscriber should have a national CLI. For fixed line calls all CLI that have not been manipulated will have originated within the country and have a national CLI. As such they are national calls as described above.

Importantly there are some valid use cases (i.e. cloud numbers) for manipulating the CLI to modify the number so that it shows a different CLI to the originator such as a specific number for a company or a national number for an international call centre or a modified number for a doctor or taxi service who doesn't want to share their real number. There is no valid reason for an individual or company to manipulate a CLI without being transparent that this is being done. Both fixed and mobile numbers may be legitimately modified. These use cases are dealt with in a separate document on cloud numbers. For the purposes of this document the use case of cloud numbers is noted as an exception and is addressed in a separate One Consortium document.

Calls from roaming subscribers will have a national CLI if the A party is from the B party's home country. The destination subscriber is not aware of whether the caller is roaming. Note that the A party may not have the same home mobile network as the B party and this limits the information (such as roaming status, call forwarding information etc) that the destination network has about the A party. Number portability means that the home network cannot be determined merely from the phone number.

For most subscribers their trusted contacts will be from home and present a home CLI. If my contact from home is roaming it will still present a home CLI whether I am at home or abroad. If a fixed line call from home calls it will still present a home CLI if there is no manipulation.

### Fixed and Mobile calls, devices and numbers

Fixed line calls originate from a landline phone or PBX connected directly or indirectly to the telco provider. The description "fixed line" is somewhat of a misnomer as these devices are commonly wireless and the phone is typically in software with a programmable CLI. However, the connection to the telco network is a constant configuration and does not allow for full mobility. Mobile devices and calls specifically have mobility management mechanisms to allow full mobility so that calls can be made and received globally.

Both fixed and mobile use the same basic technology (ISUP and SIP) for calls although there are adaptions to enable for example mobility for mobile networks.

In most countries mobile numbers and fixed numbers have different number ranges with fixed line numbers typically being allocated to regions/cities. In some countries (most notably North America) mobile numbers are also allocated geographically so that the number range cannot be used to determine if a CLI is fixed or mobile.

For most countries the country code in the CLI aligns with national borders and so national numbers can be determined by the operator or the subscriber from the country code (e.g. +44 for UK). For the North American numbering plan several countries have a +1 prefix (e.g. USA, Canada, Bermuda) so determination is at the area code level and is less obvious for consumers.

These issues make it more difficult to apply national CLI roaming checks described in this document.

### International calls to home B party

For a fixed line caller, the originating CLI (before any valid or otherwise manipulation) will be a CLI from the originating country.

For a mobile subscriber, the originating CLI will be a CLI from their home country even if they are roaming in another country.

Therefore, if there is no CLI manipulation if a caller receives a call with a home CLI it must have originated from home or from a roaming mobile subscriber.

Similarly, if it is an international number it will correspond to the home country of the caller.

### Calls to roaming B party

Calls to a roaming mobile subscriber visiting a network will be routed directly or via home to the visited network depending on technology. However, the routing will transit potentially multiple carriers/hops and so the potential for in transit manipulation exists. The protection against CLI spoofing thus relies on the visited network and this will potentially be limited (for example will they have permission to query roaming status).

### OTT calls

Calls using (proprietary) OTT applications connect handset clients together via encrypted IP connections and the OTT providers backend.

OTT calls are seen by the service providers, the interconnect providers and the carriers as simply an encrypted data tunnel. Typically, only the OTT provider can view the CLI and call data and therefore protect against spoofing. This is in many ways simpler as there is a limited ecosystem to control, but protection at origin and in transit depends on the OTT provider. OTT calls are not covered in the remainder of this document for this reason

## 5. Technology differences

Calls are routed and connected using signalling between telecoms networks and carriers. At a high level two technologies are used:

### SS7 ISUP (Signalling system number 7 ISDN user part)

Designed in the 1970s this originally used TDM (analogue) transport, but this has evolved to predominantly IP. ISUP has a limited set of messages and parameters for setting up and connecting a call. With ISUP the signalling and the media (voice) follow the same path.

ISUP is still used for 2G and 3G mobile networks and in a few fixed line networks.

In the 1990s the CAMEL protocol was developed for mobile intelligent network (IN) services such as prepay to work alongside ISUP and trigger queries from a roaming network back to the home network so the home network could control and modify the call.

### SIP (Session Initiation Protocol)

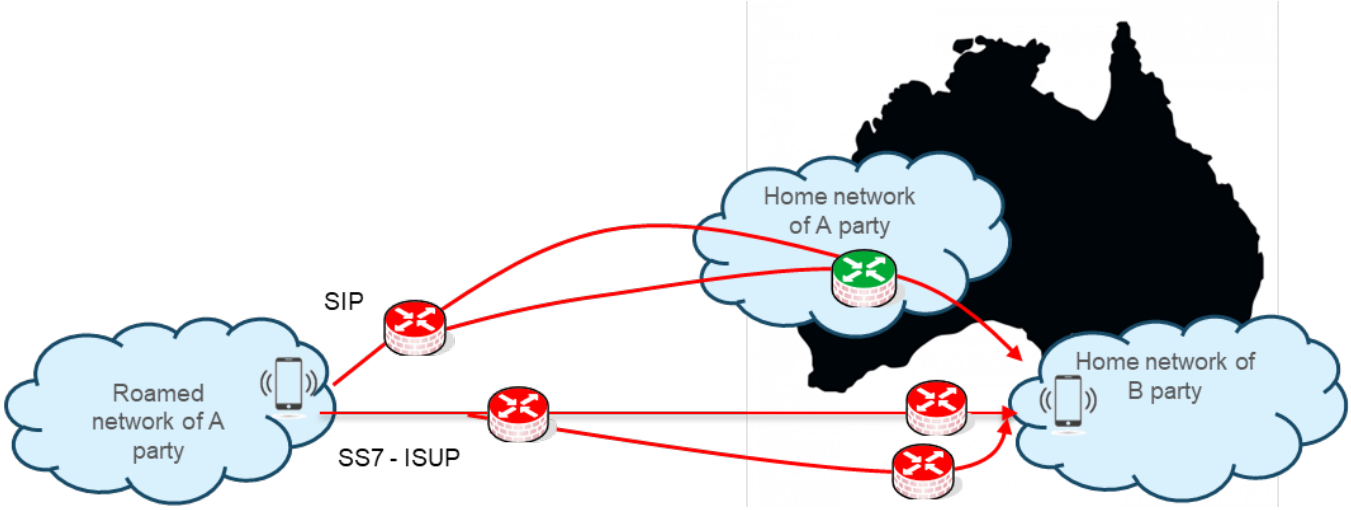
SIP was developed in the late 1990s for fixed line all-IP telephony. It was adopted for 4G and subsequently 5G mobile. SIP establishes a connection for any media (voice, video, messaging etc), but the actual media path does not follow the signalling path. There are a few basic methods (i.e. messages) defined in SIP but a vast number of parameters and a large degree of flexibility in SIP for custom parameters or extensions.

### International interconnect

A key difference between SS7 ISUP and SIP is the way in which mobile calls are routed. For SIP the signalling is always routed first to the A party home network and then towards the B party. For ISUP the signalling (and the call media) is typically routed to the B party destination from the visited (i.e. the current network whether at home or roaming) network (this also reduces latency in the call).

Note that any international connection may have multiple and dynamic transit hops and so is at risk of spoofing in any hop. If the link from the A party home to the B party home is national (i.e. they are in the same country) then those links are likely to be

trusted national trunks.




If CAMEL is deployed in the visited and home network and for the subscriber, it is possible to set triggers on mobile originated calls to force home routing of the ISUP leg. In this case the signalling (and media) would be the same as SIP. CAMEL is widely but not universally deployed.

Note that calls are regularly converted from SS7 ISUP calls to SIP calls and vice versa.

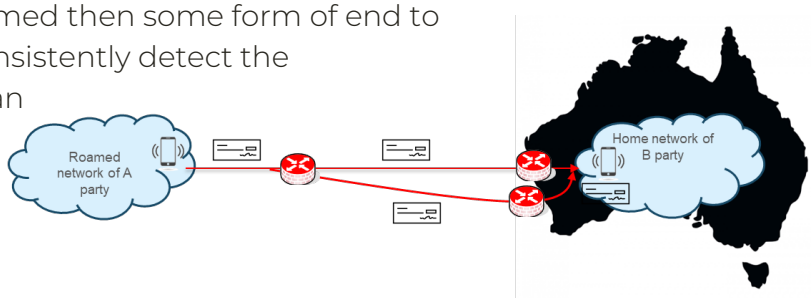
## 6. Categories of spoofing protection

To fully trust that a CLI from any A party requires checks for spoofing at the origin and a mechanism for checking the call has not been manipulated in transit.

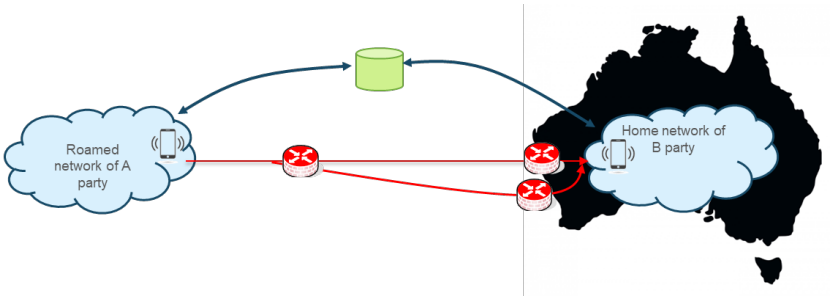
Whilst checks for badly formed or unregistered numbers or analytics to examine call parameters can detect spoofing they are inherently limited as valid numbers can be spoofed, and call parameters are not consistently transported.

Checks such as roaming checks or call in progress checks reduce significantly the risk of CLI spoofing as it is difficult for a fraudster to determine of the target A party is in a call or roaming (unless they control it). They don't completely eliminate the possibility however.

Once checks at the origin are performed then some form of end to end call verification is required to consistently detect the manipulation of CLI in transit. This can be a form of in-band signature such as STIR for SIP or ITU763 CLI authentication for SS7.



It can also be an out-of-band connection to check call details such as simply A, B number pair for active calls. These checks could be network based or for example via handset apps.




Both these mechanisms suffer from two problems:

a) They require wide adoption to be useful. Adoption between countries is technically feasible, but very complex from a governance perspective, but it does not prevent spoofing of a CLI from a third country It should however be able to be detected and flagged to the callee as not verified.

b) It depends on the KYC and associated checks of the right to use the number at the origin country (and potentially to transmit identity and authentication information). For example, a non-spoofed-CLI call can be malicious.

For SS7 calls the authentication signature is not deployed or available in network equipment so for SS7 calls it is unlikely that an in-band signature-based solution is feasible.

Within a country (e.g. USA using STIR/SHAKEN) and via bilateral agreements or for specific cases like cloud numbers these checks could form part of a solution since for these scenarios additional requirements can be demanded, but it will be very challenging for this to be globally and universally applied.

For a more complete list and analysis of the available tools please see the output documents of One Consortium WorkGroup 1

Over the top applications (OTT) such as WhatsApp are commonly used for calling as well as messaging. These only utilise a telcos basic IP data transport. If a mobile device is used, the data connectivity of the phone and its roaming status can be checked by the telco, the signalling, routing, media and any encryption are entirely within the OTT ecosystem. The OTT is thus responsible and can control in transit manipulation (i.e. spoofing) and indeed ensure the presented CLI is consistent with the SIM.

## 7. Roaming checks

### Roaming checks provide trust in national CLI

Most subscribers expect to be able to trust national CLIs and CLIs in their contacts and have less trust in international CLIs. Whilst this is not ideal it is simpler to deal with protecting national numbers and solves a significant part of the problem.

Calls from international originations should only have a national CLI if it is a cloud number or if it's a mobile number and the subscriber is roaming. In order to be reasonably confident a call is not spoofed we need to check any calls on international links and only allow cloud numbers and calls from subscribers who are roaming.

If it is a cloud number then there should be some mechanism to check it is not spoofed – this could be a signature or a trusted trunk or other mechanisms, but this is outside the scope of this document and is covered in documents from One Consortium on cloud numbers.

If the number is from a mobile subscriber, then a roaming check doesn't prove the number is not spoofed, but it does confirm that they are roaming and so that CLI is justified in appearing internationally. To spoof the number the fraudster would have to know that the number they are spoofing is roaming.

### Mechanisms

### National trunk

As described above, for mobile SIP calls (i.e. 4G/5G) and fixed line, a national caller will arrive on a national trunk (i.e. from a national partner) and this is sufficient to check the caller is really a national subscriber. Connections between national parties are normally trusted.

A check on incoming link is straightforward technically.

It does not prove the national CLI is not a spoofed, but any spoofing is unlikely and would probably have to be in transit as spoofing at the origin would be protected by local KYC/KYT checks and/or mobile SIM/MSISDN linkage.

### Home routing

SIP calls are home routed as discussed above. It is possible to force home routing for ISUP calls (for example using CAMEL).

Home routing means the A party home network can perform any checks on the A party (such as roaming checks) before sending the call to the B party (on a national trunk if it's a national call).

The home routing solution relies on CAMEL being available in the roamed network with associated cost and complexity. It also adds potential latency to ISUP calls if they have to be routed home and back for instance between two roamed parties).

Home routing has been proposed for instance by Ofcom (UK) with the international gateway removing CLI from all national CLI that come via international links. The home operator would additionally perform roaming checks on the A party which because it is home routed would be their subscriber and therefore not have any of the cross-operator limitations noted below. The roaming checks adds confidence there is no spoofing as it means the phone with that CLI is reporting the correct roaming status.

### Roaming check via Signalling

A roaming check lets an international gateway, a service provider or another responsible entity confirm that a national CLI is allowed from an international link.

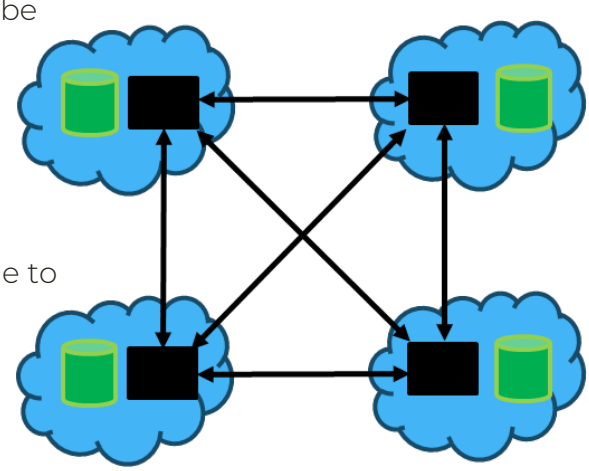
Each mobile operator is aware of the location of each of their subscribers in order to provide service. The HLR tracks the visited location and so roaming checks on own subscribers is simple via APIs or signalling.

To enable other networks (i.e. the B party) to query the A party HLR would enable the destination network to check a subscriber is roaming. This however poses a risk that anyone with a global title (and these can be rented cheaply) could access the HLR. It also exposes more data than simply roaming (e.g. subscription data) which is both a privacy issue and a competition issue. Whilst signalling firewalls should allow control over access and mitigate the risk this is an area where threats are constantly seen. This is however a technically straightforward way to perform roaming checks.

### Roaming checks via API

#### *Telco to telco*

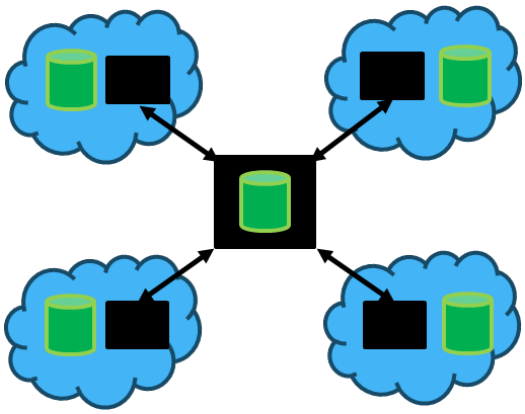
An API reduces the security risk of using signalling for roaming status checks. Standard APIs that can be used have been defined (e.g. Camara). APIs between each telco suffer from the scaling problem that all networks need to be interconnected and this the number of connections expands rapidly even within a country and to extend to a region is probably untenable.



Direct API connections also suffer from the issue that the A party phone number is not sufficient to determine the networks that should be queried (due to number portability). There is no (as yet) defined standard for looking up the home network, although several proprietary solutions do exist many rely on signalling HLR lookups. An API

solution is thus inefficient in that potentially multiple networks need to be looked up – or a central number portability database lookup may be required (if this exists as not all countries use this approach for MNP).

*Via hub*



An alternative API solution is to build an API to a hub (a "super HLR") which is fed by each operator to maintain roaming status. This then enables one API lookup to determine the minimum information required in one API call.

Particularly where an MNP database exists within a country this is technically not overly complex. This solution is deployed and has been effective in countries such as Norway, India and Ireland.

An alternative approach to a centralised hub is to allow an entity (or several entities) to provide an API (or a SIP Interface) for a roaming check and build integrations (API or signalling) to each operator. The GSMA Open Gateway initiative (based on Camara) already offers APIs which are globally deployed and provides a range of defined APIs including a roaming check.

This scales more readily, and offers less competition risk, but relies on a third party to manage security around the API on behalf of the telcos. APIs will need to have low latency and good levels of security.

### Regional trust

The national CLI protection scenarios using national links and roaming checks as described above can be expanded to trust across regions (e.g. Scandinavia), but they get complex quickly as they scale. To trust 3 other countries would require connections between all three countries networks or all three countries hubs. To add link checks would require direct / trusted links between each operator/country.

### Edge cases

As noted in the introduction, fraudsters will exploit unusual scenarios (i.e. edge cases) so they can't be ignored. They need to be either prevented or made sufficiently difficult and expensive that the business case for the fraudster doesn't work.

### Permanent roaming

It is feasible for a fraudster to acquire a SIM and then roam permanently. This phone number could then be used (spoofed or actual) as a national number to make spoofed calls. The number would (if mobile) be unlikely to be a trusted national number (e.g. in a consumer's phone book), but merely being national implies some trust.

This type of action is a common mechanism for fraudsters and typically mobile networks have detection mechanisms to detect these schemes which reduces the business case for fraudsters who would then need to cycle or move these CLIs/devices.

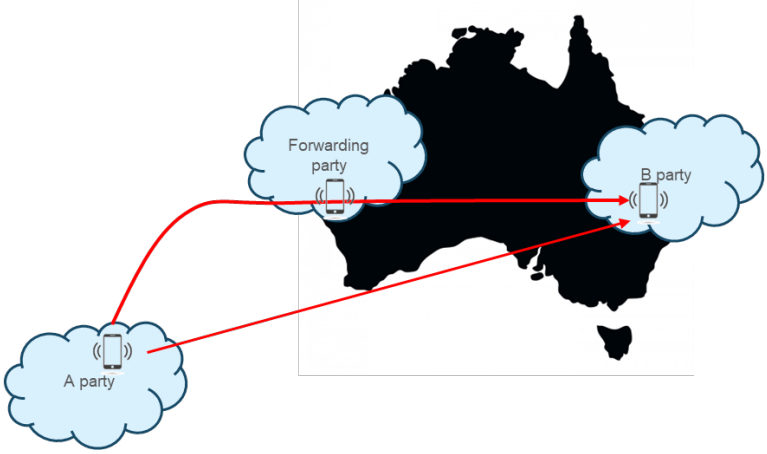
### Wi-Fi calling on mobile device

With Wi-Fi calling the user may be roaming, but the network may not be aware of this as the user has only attached to Wi-Fi and not the roamed mobile network. With Wi-Fi calling however the mobile device essentially connects as it would on the home network with an encrypted tunnel over IP transporting the SIP call so that it can't be modified and SIM authentication is used to tie the phone number to the SIM. The user may show as roaming when using Wi-Fi calling if the user has recently attached to a roamed network. These scenarios should be managed by the home network.

If the call is a normal roamed call it will always correctly show the roamed status.

### Call forwarding

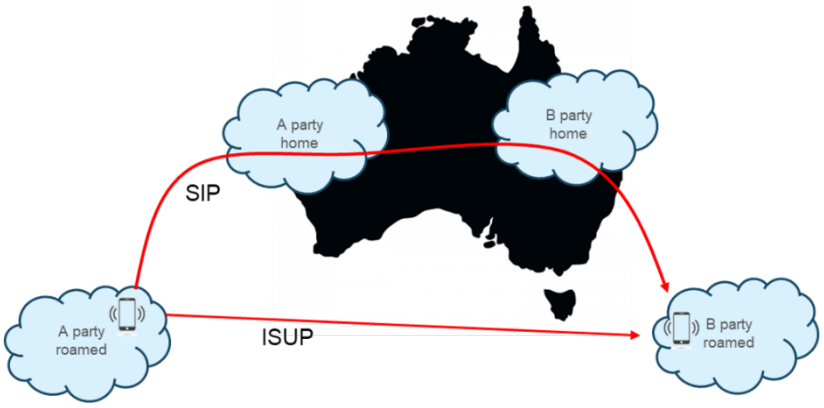
Late call forwarding is the scenario where a call is forwarded (e.g. to voicemail) after an attempt has been made to reach the original recipient.




This can be used maliciously by a fraudster maintaining a device to perform national call forwarding, because for both SIP (4G/5G) and ISUP (2G/3G) an option exists for the forwarding party network to forward the call to the new number. Thus a call originally international could appear to come as a national call. Networks can and should prevent this to avoid this mechanism being exploited.

### B party roaming

If the B party is roaming, then for SIP (4G/5G) the call setup (SIP) still transits the home countries whereas ISUP will go direct between networks. However, in both cases there are international hops that could spoof calls in transit (or the call could be spoofed at origin)



It is therefore the roamed (visited) network that would have to implement checks on the A party CLI for inbound roamers. This is difficult for a network to do for all incoming roaming subscribers.

## 8. Call treatment

When spoofing is detected or suspected, with ISUP the CLI can be withheld, or modified or the call can be blocked.

With SIP as well as these options it is feasible to add logos (branded calls) or confidence indicators etc. This relies on additional SIP headers being added to the call.

## 9. Conclusions and Recommendations

Consumers have a right to expect that the CLI presented on their phone can be trusted. The flexibility and privacy protection built into telco networks and standards, and the complex routing of calls means this is not simple to achieve.

Most consumers understand that trust in CLI does not mean knowing the user of the CLI unless it is in their phone book, but they will also expect many (usually national) numbers from originators they don't know to call them. Thus, protecting national numbers from spoofing is a significant benefit even if there is limited protection for international CLIs.

Performing roaming checks and national trunk checks for national CLIs on international links provides good, but not complete protection against spoofing and therefore enables trust in a call that carries a national CLI when the subscriber is at home.

Roaming checks can be done in several ways such as APIs from the called party network or using home routing and roaming checks from the calling party network.

Roaming checks cannot easily be extended to provide more general protection for any CLI to be trusted. This would require a more comprehensive global solution for end-to-end call checks ideally alongside a global level of KYC/KYT and identity verification.

Roaming checks are recommended as a straightforward solution to significantly improve protection for national CLIs although the best approach to these will vary by country depending on the way MNP is implemented and the maturity of APIs etc.