

# CLI consistency checks

Rel. 1.0

Technology WG



## CLI Principles

- Calling Line Identification (CLI) facilities provide information about the party making a telephone call.
- CLI Data consists of both **Network information** and **Presentation information**:
  1. **Network information** refers to the caller's asserted identity that is included in either:
    - For IP trunks in the P-Asserted Identity (PAID) header in the SIP signalling. The SIP PAID header is pseudo mandated as the inclusion of this header is a prerequisite for most IP interconnections
    - For TDM trunks in the Calling Party Number parameter in the SS7 ISUP signalling. This parameter is a mandatory parameter in SS7 ISUP.
  2. **Presentation information** refers to the callers CLI to be presented to the called party in either:
    - For IP trunks in the FROM header in the SIP signalling and a mandatory header in SIP INVITES
    - For TDM trunks in the Generic Number parameter in the SS7 ISUP signalling. This is an optional parameter in SS7 ISUP and not supported in all networks for TDM trunks (Note)

The Presentation Information is accompanied (for both IP trunks and TDM trunks) with:

  - A privacy marking, which indicates whether the number can be shared with the recipient of the call, or not
  - Optionally, depending on national regulation and technical capabilities, an indication about the trustability of the presented CLI Data.
- CLI Data needs to be provided/verified by originating operator
- Transit and terminating operators must not alter CLI Data
- Transit and terminating operators may perform CLI consistency checks based on **format** and **content**



## Known Issues

- CLI data is to be generated by the originating platform and validated by the originating operator (which is a licensed operator) collecting the call and confirming the “Right to Use” (RTU) of the CLI, but it comes with issues like:
  - Some originating operators allow CLI data to pass through without adequate validation
  - Use cases exist whereby CLI data is generated outside the network of the operator responsible for the numbering resource
  - Global implementation practices vary due to a long history of loosely specified interworking situations and mapping differences to SIP (From, PAID) and ISUP (CgPtyNb, GenNb) fields, and privacy settings (markings that indicate whether the number can be shared with the recipient of the call)
- There are legitimate scenarios where the CLI in the FROM field (Note) is altered (Uber driver, call center, work from home). However, this is handled at the originating point (originating operator), thus not an action by transit carriers and terminating operators.
- CLI consistency checks apply to the CLI in both the PAID field and FROM field.
- OBR fraud is example of CLI altering by transit carrier that must be detected and stopped

Note – Only changes to the FROM field apply. The PAID field is always the originating number, not to be altered. However, there could be a number anonymity use case involving CPaaS platforms where both FROM and PAID are altered (example, facilitating calls between taxi rider and driver – these are handled as two separate calls from a network perspective, matched by service application server)


- Use cases where the domestic CLI, mobile and cloud numbers, is used in international call paths without direct control from the network responsible for the numbering resource:

	Use Cases	Description
1	Mobile Roaming	Calls by mobile users roaming abroad under 2G/3G coverage or fallback in visiting mobile networks without CAMEL support.
2	Outbound VoIP calls	Services like Skype Out terminating calls with CLI data inserted by end-users.
3	Click-to-Call (also known as Click-to-Talk, Click-to-Dial or Click-to-Chat)	By clicking an object (e.g., button, image or text) to request an immediate connection in real-time. Click-to-Call requests are made on websites or be initiated by hyperlinks placed in emails or videos, and other Internet-based object or user interfaces.
4	Authentication services *	Services like flash calling (typically used as an alternative to SMS) whereby (part of) the CLI data is used to interact with a mobile app for authentication purposes.
5	Call Forwarding *	End-users allowed to make international outgoing calls without accurate screening of CLI data and services using a pool of numbers to anonymize caller identification (taxi services).
6	Number Anonymity *	
7	Cloud Contact Center *	Various services that generate international outgoing calls using CLI data (mobile, fixed and service numbers) for enterprise clients
8	Corporate Telephony *	
9	Call Center *	
11	Conferencing Platform *	
10	Retail Use *	Services like Home Country Direct or other use cases where toll free or virtual numbers are used specifically by end users.
12	IoT device management *	Niche use cases related with remote devices where DID's could complement IoT or mobile connection with numbers provided for IoT (IP end points) devices (e-call in cars).

- Some of the above use cases are not legitimate depending on national regulations (legitimacy can vary from country to country)
- Understanding how these use cases are abused for fraudulent calls, while not completely preventable, can help lead to targeted solutions including
  - CLI consistency checks
  - International traceback
  - Trusted trunks
  - KYC/KYT

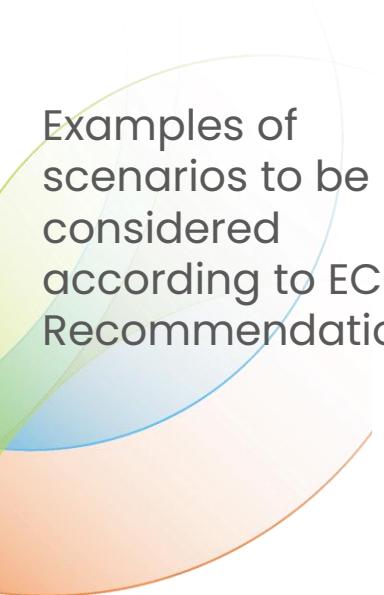
\* For further details be referred to the Cloud Numbering Use Cases

Use cases with domestic CLIs generated abroad



Sample use  
cases not  
legitimate in  
some countries

1. UK – CLI guidance:
  - Where the Communication Provider can't demonstrate the traffic has originated on a UK network, then onward routed outside the UK before then re-entering through a UK network. This includes calls originating on nodes or cloud services located in the UK
  - Where the Communication Provider can't demonstrate the call is being made by a UK customer but has originated on a non-UK network. This includes traffic that is hosted on nodes or cloud services outside the UK
2. Japan passed a law that makes it illegal to use machines to dial phones and then hang up before the call is connected. The purpose of this law was to tackle *wangiri* but it effectively prohibits flash calling too. Flash calling would be a crime in Japan but not in most other countries
3. China – legitimate international traffic must comply with the following guidelines:
  - No calls allowed with a duration shorter than 3 minutes
  - No unsolicited marketing calls
  - No high volume of repeated calls from the same origination (From) Number within a rolling hour
  - No calls allowed from invalid, modified, spoofed or restricted origination (From) Numbers
  - Calls must be sent from an international, non-China number when making calls to China

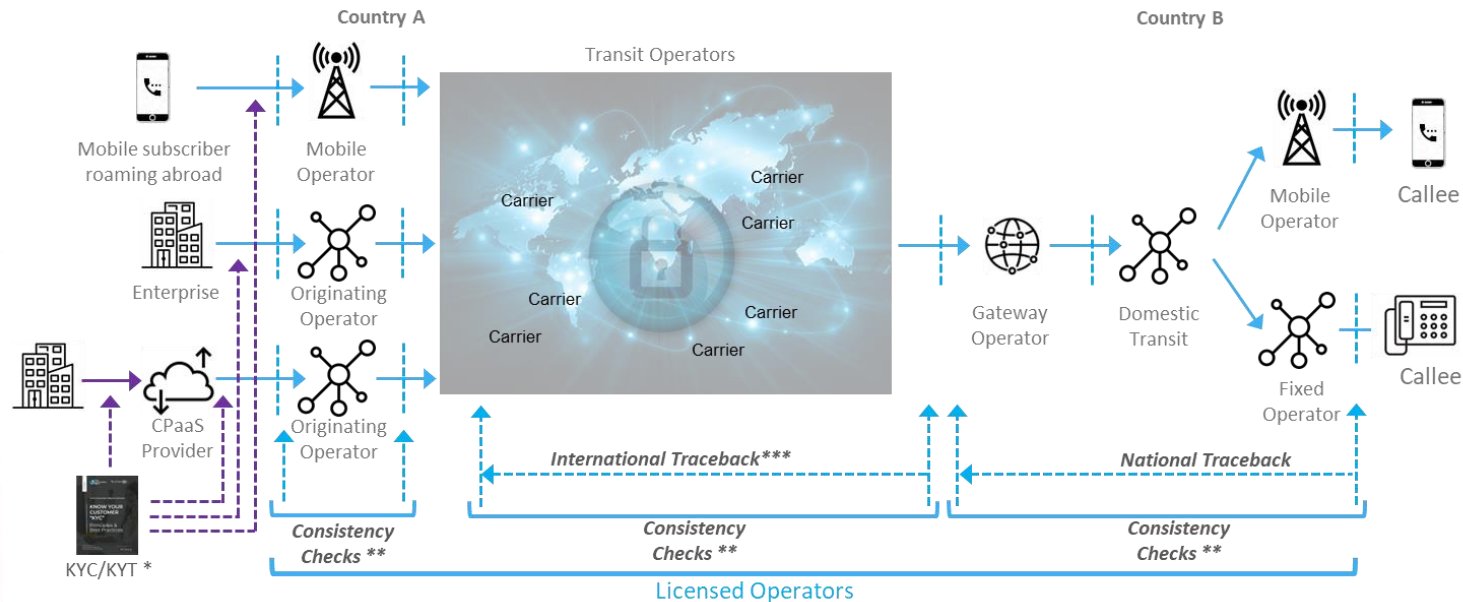


## Examples of scenarios to be considered according to ECC Recommendation

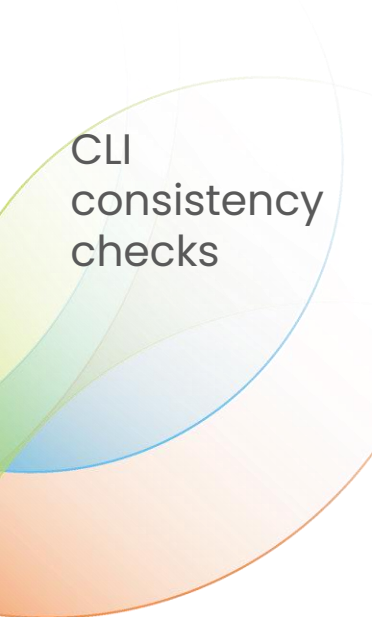
Examples of scenarios of calls where the flow would result in incoming voice calls with national numbers as CLI over the international network interfaces:

1. A call from a national outbound roamer in Country B destined to a national mobile or fixed/geographic number, (where national implies "Country A")
2. A call from a national fixed/geographic or mobile number is destined to an inbound roamer (e.g. an agent of a hotel in Country A is calling a client who is assigned a mobile number pertaining to the national numbering plan of Country B whilst the client is roaming in Country A)
3. The use of call forwarding may result in a scenario of legitimate calls over the international network interfaces with a national E.164 number, as described in the following cases:
  - a) A call from the national number (any fixed/geographic or mobile number) is destined to an outbound roamer who has a late conditional call forwarding to any national number
  - b) A call from the national number (any fixed/geographic or mobile number) is destined to a foreign number and this one has call forwarding to any national number
4. A call from a national service provider implemented in a cloud solution and destined to a national number using the international network interface
5. A call from a number of Country A, which is assigned for extraterritorial (ET) use in Country B, is destined to a national number of Country A
6. The above scenarios do not address the possibility whereby OTT providers, such as Skype, Viber, etc., permit end-users to use their assigned national number served by another provider, (the 'original subscription network') as the CLI in outgoing calls placed through their OTT applications. The possibility of such 'decoupling' could result in having a wide variety of numbers, from multiple numbering ranges, to be decoupled and used to originate calls via such OTT providers

## Overall call scenario for domestic CLI data generated abroad



- \* **Know Your Customer/ Know Your Traffic (KYC/KYT) Principles and Best Practices** CCA provides an extensive list of pre-activation, post-activation and due diligence actions to be implemented by CPaaS providers to avoid the abuse of their services to originate illegal traffic
- \*\* **Consistency Checks** should be executed per call/message and the type of checks depends on the detailed knowledge of the CLI data dependent per situation (originating/transit/terminating) and type of context (fixed line or roaming user)
- \*\*\* **International Traceback** requires agreement and collaboration among Terminating and Transit Operators involved in the call path



## CLI consistency checks

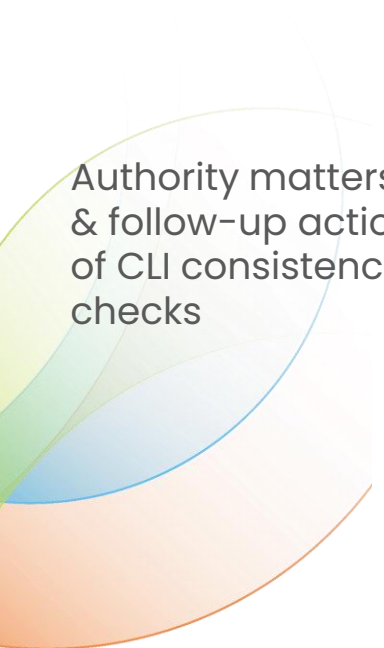
- The CLI must be a valid, active telephone number that uniquely identifies the caller:
  - A **format** of the CLI must be compliant to the International public telecommunication numbering plan (Recommendation ITU-T E.164)
    - International format (beginning with “+” or NAI = INT)
    - All digits 0-9, no alphanumeric digits
    - Max 15 digits length
  - A **valid number** is a number that is designated as a telephone number available for allocation in the national numbering plan of the country and be shown as allocated to a licensed operator in the national numbering scheme  
*Source: NRA of the country the number belongs to*
  - An **active number** is one that is in service and can be used to make calls (so not belonging to Do Not Originate list or assigned to national services, assigned to an active land/mobile/cloud line).  
*Source: Licensed operator the number is assigned to*
  - A **number uniquely identifies the caller** (which can be an individual or an organization) 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 via proper RTU leasing / subleasing numbers) to use the number by a third party who has been assigned that number  
*Source: Licensed operator or the third party the number is given rights to make calls to*

Note 1 – The CLI consistency checks used today vary by country and often are not nearly as ‘advanced’

Note 2 – Right To Use (RTU) applies for verifying leased and subleased numbers


Note 3 – A CLI may include a privacy marking whether the number is allowed to be presented, or not






## Authority matters & follow-up actions of CLI consistency checks

- Accurate, updated data is needed for the CLI consistency checks, but raises issues given 230+ countries, thousands of operators, and no single source for Numbering Plan data
  - For the CLI of a **landline** number (fixed line, enterprise, special service, or else) this is known by resources in originating country A and the consistency checks may be performed either:
    - **originating** operator; and a CLI becomes also trusted for the terminating operator if a secure transfer of the CLI can be guaranteed (e.g., via trusted trunks)
    - **terminating** operator; and a CLI becomes also trusted for the terminating operator if the last can verify the CLI by querying a database (either offered by a provider in the originating country or by a global/regional data service provider)
  - For the CLI of a **mobile** number (i.e., for non-home routed calls of roaming users) this data is known by resources in terminating country B and the consistency checks are to be done by an operator in country B including an isRoaming check (see the explanation later in the deck)
- Depending on the outcome of the above verification, the following guidelines apply:
  - CLI is **trusted** (i.e. it can be assumed the CLI uniquely identifies the caller); then the CLI may be presented to the callee. Depending on the system capabilities at the receiving end, the CLI can be accompanied by a mark indicating it is trustable
  - CLI is **not trusted** (i.e. it can't be assumed the CLI uniquely identifies the caller); the call may be blocked or proceed depending on local regulations and operator policies. If the call proceeds, the following actions are advised:
    - Do not present the CLI to the callee, or display an anonymized CLI
    - Display the CLI with a mark indicating it is not trustable, if supported by the receiving system



## isRoaming and cloud numbers checks

- Even if CLI Data has the right format and it contains a valid, active number uniquely identifying the user, there could be abuses or fraudulent behaviors
- Legitimate use cases must be guaranteed:
  - Mobile telephone numbers generating calls with devices roaming abroad (International roaming) – additional 'isRoaming' technical check(s) to determine whether the user is actually roaming abroad or not
  - Telephone numbers assigned to users/organizations to generate calls from outside the country they belong to (like in India numbering plan allocation for domestic CLIs originated abroad & use cases such as banking services) – explicit assignment for this use case could be requested by NRA so that only telephone numbers entitled to generate calls from abroad are allowed to be terminated – *Note: good topic to raise w/ NRAs. Put in summary slide*
  - KYC/KYT polices can be set between:
    - Enterprises and CPaaS providers (e.g. KYC Principles & Best Practices by CCA)
    - CPaaS providers and licensed originating operators
    - Enterprises and originating operators
  - KYC/KYT polices about the use of numbers like:
    - Asymmetric numbers: numbers are either allowed for generating calls but not for terminating calls or allowed for terminating calls but not for generating calls
    - Support of a Private Number service which means the number presented can be different to the network number

A graphic on the left side of the slide featuring several overlapping, semi-transparent circular arcs in shades of green, blue, and orange. The text "Trusted Trunks" is overlaid on the green and blue sections.

## Trusted Trunks

- Trusted Trunks are secure logically separated trunks between carriers for transiting legitimate international traffic containing domestic CLI (and potentially other types of international traffic), initial principles include:
  - The traffic passed defined checks (CLI consistency, KYC / KYT, RTU) and as such carries trusted traffic towards the destination point
  - Includes traceback capability
  - Policy development including oversight, and monitoring compliance of trusted community
  - Penalties, remediation, and potential removal processes for non-compliance
- Traffic coming in on a trusted trunk has met the checks and policies above and is therefore trusted, the CLI and/or the traffic, should not be blocked.

Note: A 'long line' is the connection between the customer (Enterprise or CPaaS) and the originating operator where the customer is not located in the same country as the originating operator.  
'Trusted trunks' are trunks between two international operators.

**Call via Trusted Trunk**

**CLI data format checks**

- International format?
- All digits, no alphanum?
- Max 15 digits length?

YES

**CLI data content checks**

- Valid number?
- Active number?
- Uniquely caller identity?

YES

**Call screening checks**

- CLI on DNO list?
- B-nb on black list?
- Not-mobile CLI with RTU\*?

YES

**CLI mobile number?**

YES

**Subscriber roaming?**

NO

NO

YES

**Drop or Flag the Fraudulent Call (depending on legislation, etc.)**

**Proceed the Call**

Internal

NRA, lic. oper,  
third party

NRA

mobile  
operator

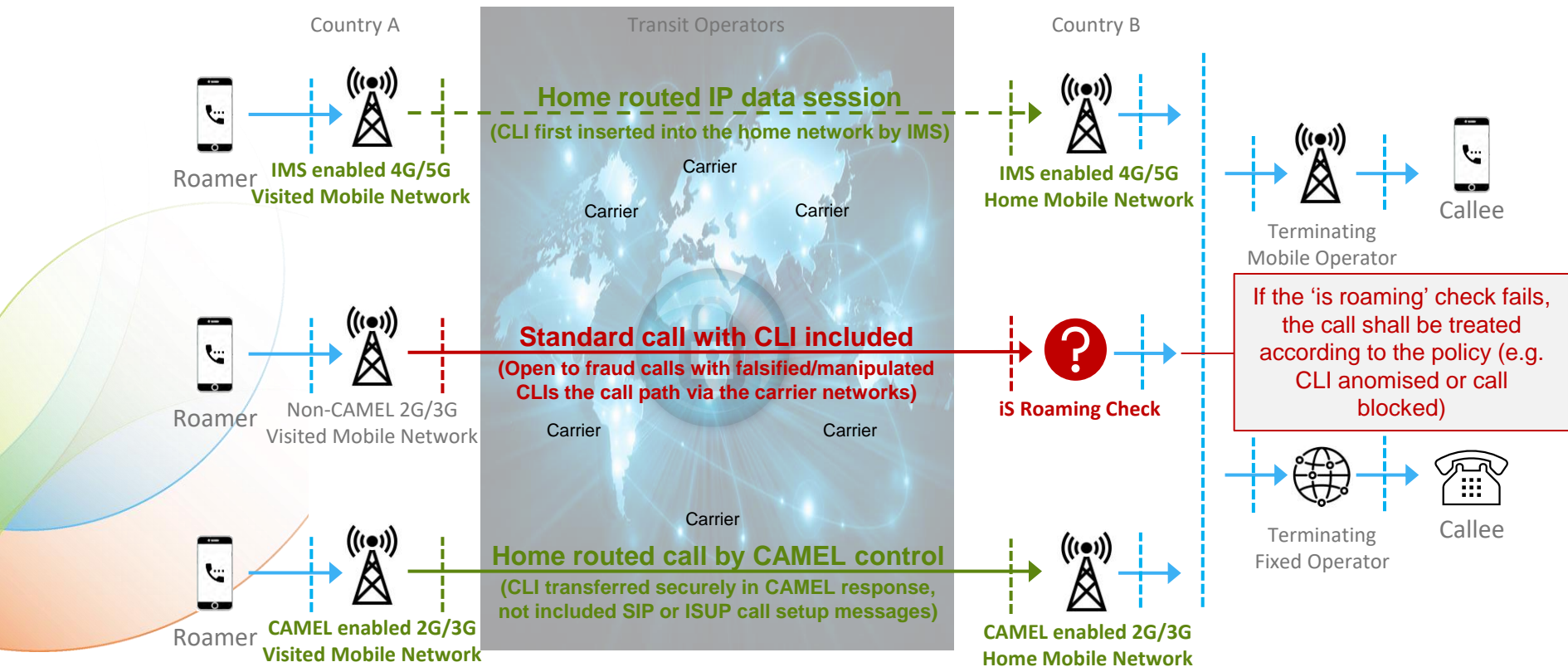
Flow chart for  
serial CLI  
consistency  
checks

Considerations for Policy Development

The originating operator must perform both KYC and verify RTU for the CLI.

Each carrier and transit operator must perform the CLI consistency checks. But these checks will be less effective and more difficult to do as you go further down the line

# CLI Restoring Trust Solutions for Calls by Users roaming abroad



- Market adaptation and specific pro's/cons of the solutions for isRoaming check:
  1. Use of **Home Routing** for calls generated by subscribers roaming abroad with adaptation of SS7 CAMEL-based solution between home and visited networks

Primary pushed by mobile operators in Europe. However, it can only provide fragmented coverage (so not suitable as a single solution) as there is no worldwide support for CAMEL

    - + Simple development based on 3GPP standards, no MNP correction needed at gateway
    - Requires support of CAMEL by the networks of roaming partners. Adding CAMEL to legacy 2G/3G mobile networks is complicated, involves licensing costs and capacity issues
  2. Use of SS7 signalling **MAP based queries** towards the mobile network of the calling subscriber or access to **API of the mobile operator** to determine whether he/she is standardized, abroad

SS7 MAP solution used in Middle East and North Africa, API solution used in Europe (next to CAMEL)

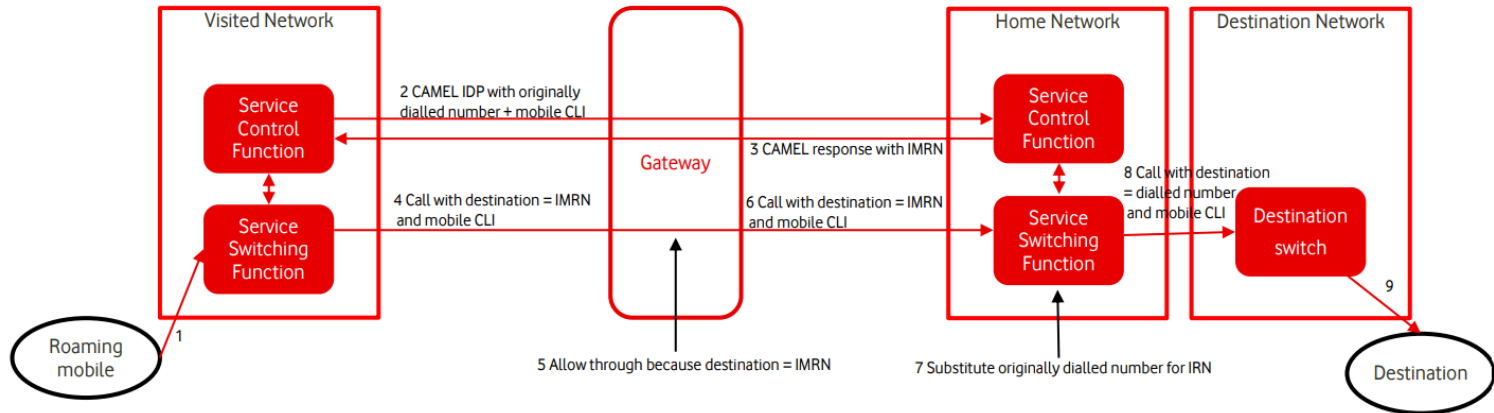
    - + Independent of network capabilities of roaming partners, GSMA standardized solution, reuse of existing SS7 roaming interconnection technology for MAP-based solution
    - Need for gateway development, filtering needed to avoid privacy/data protection risk, need for MNP correction at gateway to query the CLI serving mobile operator
  3. Use of a **Proxy/Hub** to be queried in order to retrieve location status information of the calling subscriber. Proxy/Hub acting as front end with respect to mobile operators in a country

Newest approach and especially considered by operators in Asia and Americas

    - + Independent of network capabilities of roaming partners, minimizes gateway development, no MNP correction at gateways, and potential support of international inter-carrier queries
    - Need for regulatory consent and bilateral trust between operators for Proxy/Hub to process privacy/data sensitive information of end-users

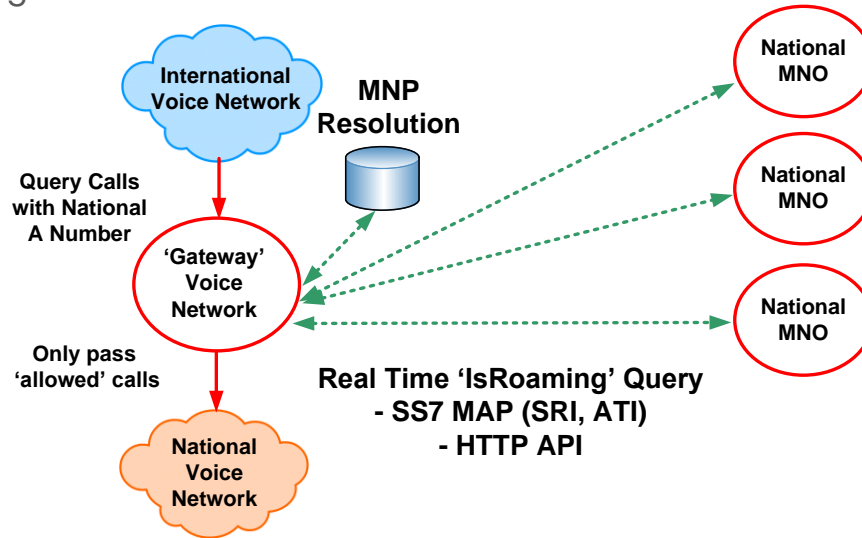
## Home Routing solution

- With CAMEL interaction home network instructs visited network to change called party number into an Inbound Mobile Roaming Number (IMRN) so that calls are delivered to home network regardless of the destination
- Home network then replaces IMRN with original called number and it delivers the call to end destination
- Screening rules are applied on international gateways of the country the home network belongs to: calls with national mobile calling number and IMRN as called party are allowed, while calls with the same calling party towards any other national destination are classified as “spoofing”




## MAP based query/API solutions

- International gateways querying mobile network the calling party number belongs to:
  - MAP query (using SRI, SRI-SM or ATI procedures)
  - API call towards mobile network
- With or without MNP resolution, depending on querying method
- Screening rules are applied: calls with national mobile calling number that is actually roaming abroad are allowed, otherwise they are classified as "spoofing"







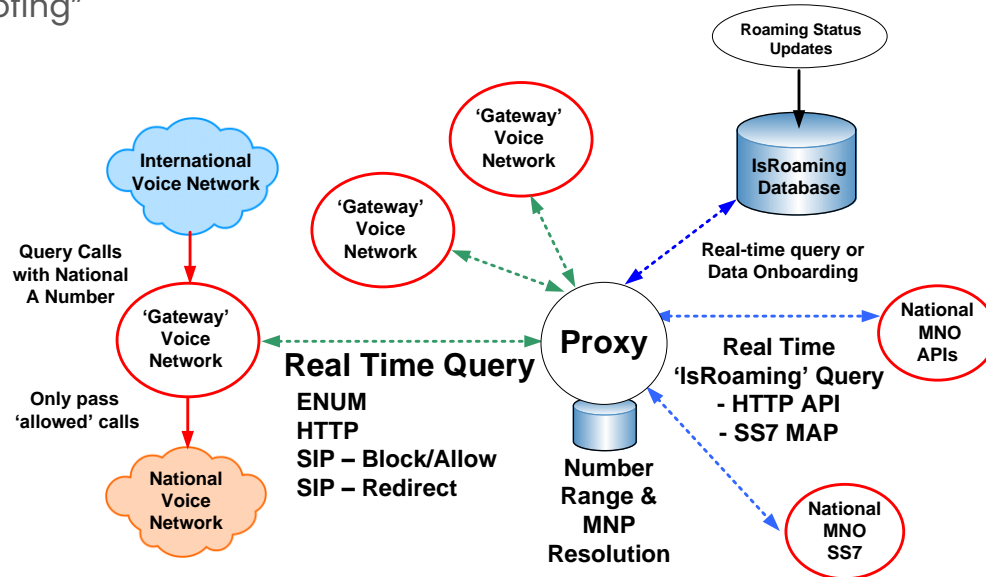
## MAP based query/API solutions


Pros	Cons
<ul style="list-style-type: none"><li>▪ Uses existing MNO interfaces (SS7 or HTTP)*</li></ul>	<ul style="list-style-type: none"><li>▪ MxN connectivity issue (Operationally expensive to deploy and maintain, requires a contract with each Gateway and MNO)</li><li>▪ Gateway ability to query the MNO (Not typical Gateway functionality)</li><li>▪ Issues with MVNOs and 'other Mobile number' users (Ability to provide query interface)</li><li>▪ Data privacy and protection (MNO interfaces open to a large number of entities)</li></ul>

\*Although not necessarily designed for this use-case

## Use of Proxy/Hub as centralized solution

- International gateways querying Proxy/Hub acting as front end (MAP, API, DB query)
- Proxy/Hub solves MNP and it retrieves information on calling party number by querying the mobile operator the number belongs to
- Screening rules are applied: calls with national mobile calling number that is actually roaming abroad are allowed, otherwise they are classified as "spoofing"





## Use of Proxy/Hub as centralized solution

Pros	Cons
<ul style="list-style-type: none"><li>▪ Single connection and contract with the Hub</li><li>▪ Minimises MNO development requirements</li><li>▪ Hub solving MNP routing</li><li>▪ Acts as a Security and Privacy anchor</li><li>▪ Resolves MVNO and other 'non-Mobile' use cases (Centralised hot-lists and special interfaces)</li><li>▪ Extensible for other 'validation' use cases</li><li>▪ Avoids the necessity of multiple MxN bi-lateral interfaces</li><li>▪ Allows for a flexibility of protocols</li></ul>	<ul style="list-style-type: none"><li>▪ Cost of deploying and maintaining Proxy</li><li>▪ It may require development and/or configuration of interfaces and modification of call handling procedures at the International Gateway</li></ul>



## Conclusions


- CLI data generated by the originating platform/device and validated by the first licensed operator collecting the call, but it comes with issues
- We recognize there are legitimate use cases (as per country's regulation) where the domestic CLI is used in international call paths without direct control from the network responsible for the numbering resource. We will be providing technical support for the solutions and guidance enabling these use cases
- Countermeasures to guarantee CLI data reliability:
  - a) **Know Your Customer/Know Your Traffic** principles applied by the first licensed operator (originating operator) collecting traffic from devices/platforms/CPaaS
  - b) **CLI consistency checks** (including isRoaming for mobile CLI) performed by originating, transit and terminating operators
  - c) **International** Traceback adopted by transit and terminating operators
- NRA could request explicit assignment of telephone numbers used to generate calls from outside the country they belong to
- isRoaming check can be realized by means of:
  - a) **Home Routing via CAMEL**
  - b) **MAP based queries/API to the mobile operator**
  - c) **Use of Proxy/Hub**

# THANK YOU



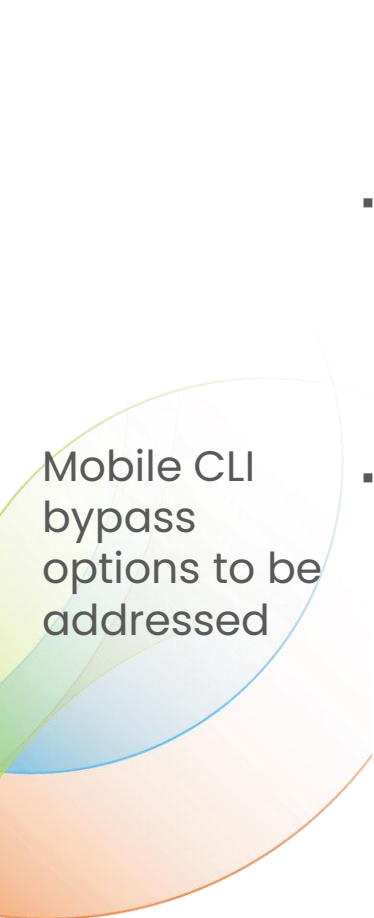
## Mobile CLI spoofing risk via international operators

- Outbound Voice Calls by Users Roaming Abroad
  - These calls are typically destined to users (family & friends, business relations) in the home country
  - The CLI is the mobile number of the user roaming abroad in the numbering plan of the home country
- Local Breakout in 2G/3G
  - Outbound calls by users roaming abroad begin in the **local** visited 2G/3G Circuit Switched (CS) network.
  - When the destination is outside the visited country, such as when calling home, the call is routed internationally through the network of IPX carriers.
  - These international calls enter the home country with CLIs in the home country's numbering plan, whereas international calls usually arrive with CLIs from foreign numbering plans.
  - Attackers are aware of this exceptional situation and may generate manipulated calls containing a CLI with a mobile number to reach and surprise their victim
  - **This creates a vulnerability for CLI spoofing of mobile numbers on incoming international trunks!**
- Home Routing in 4G/5G
  - Outbound calls by roaming users in the visited 4G/5G radio network are distinguishable data sessions and directed to the IP Multimedia Subsystem (IMS) in the **home** 4G/5G network.
  - Since these calls now originate in the **home** 4G/5G network, the calls contain a CLI in the numbering plan of the home country.
  - These calls only exit the home country when going abroad, like any other outbound international call featuring a CLI from the home country's numbering plan.
  - **This reduces the risk of CLI spoofing of local mobile numbers on incoming international trunks!**



## The promise and reality of secure roaming solutions

- VolTE Roaming
  - The worldwide shutdown of 2G/3G networks sparks the migration from legacy SS7 signalling roaming connections to Diameter-based VoLTE Roaming (S8HR)
  - However, many networks worldwide, especially in developing countries, are not prepared for this migration. It requires full 4G coverage with VoLTE ready phones and IoT devices
- 5G SA Roaming
  - In industrialized countries, 5G is a promising security advancement especially with a 5G SA Core
  - But for the foreseeable future, it will coexist with 2G or 3G services in most places
  - This poses a risk of downgrading attacks, where phones or devices may be forced to switch to less secure 2G or 3G roaming services
- CAMEL
  - This enhances SS7 roaming control in 2G/3G by home routing all outbound calls of roaming users by temporary use of a IMRN (Incoming Mobile Roaming Number) assigned by Home Network via CAMEL interaction
  - However, CAMEL support is limited globally, and it's unlikely to be implemented in other networks due to investment challenges in legacy technology



## Mobile CLI bypass options to be addressed

- Over-the-top voice applications
  - Over-the-top voice applications Skype Out, Vonage, CloudTalk, etc. offer many bypass options.
  - A typical risk are services that allow subscribers to configure a mobile number as caller ID, which is included in the CLI of the outgoing VoIP call and presented to the called party
  - These services are popular among fraudsters for CLI spoofing attacks and other irregularities, due to their limited authentication controls
- Unified Communications (Fixed/Mobile) solutions
  - Popular in use among enterprises and may include scenarios whereby a mobile Caller ID is included in outbound calls without direct control by the mobile operator
  - Screening for manipulated Mobile Caller IDs by the fixed network is not guaranteed