i3 Webinars

Fight Spoofing and Restore Trust in International CLIs

Feb 25th, 2026

i3 Webinars

Agenda

- CLI principles and consistency checks
- Mobile roamer identification verification
- CLI checks to protect Italian subscribers
- Wrap up
- Q&A

i3 Webinars

CLI Principles and Consistency Checks

Enhancing Calling's Identity Reliability

Filippo Cauci

CLI principles

- Calling Line Identification (CLI) facilities provide information about the party making a telephone call

- CLI Data consists of:
  1. **Network information** referring to the caller's asserted identity that is included in either:
     - P-Asserted Identity (PAID) header for IP trunks
     - Calling Party Number parameter For TDM trunks
  2. **Presentation information** referring to the callers CLI to be presented to the called party in either:
     - FROM header for IP trunks
     - Generic Number parameter for TDM trunks

     The Presentation Information is accompanied with:
     - Privacy marking
     - Indication about the trustability of the presented CLI Data

- CLI Data needs to be provided/verified by originating operator

- Transit and terminating operators performing CLI consistency checks based on **format** and **content**

Known issues

- CLI data generated by the originating device/platform and validated by the originating operator collecting the call and confirming the “Right to Use” (RTU) of the CLI
- 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
- Legitimate scenarios where the CLI in the FROM field (Note) is altered (Uber driver, call center, work from home). Handled at the originating point
- 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

Use cases with domestic CLIs generated abroad

- Use cases where the domestic CLI 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 DIDs 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)

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

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:

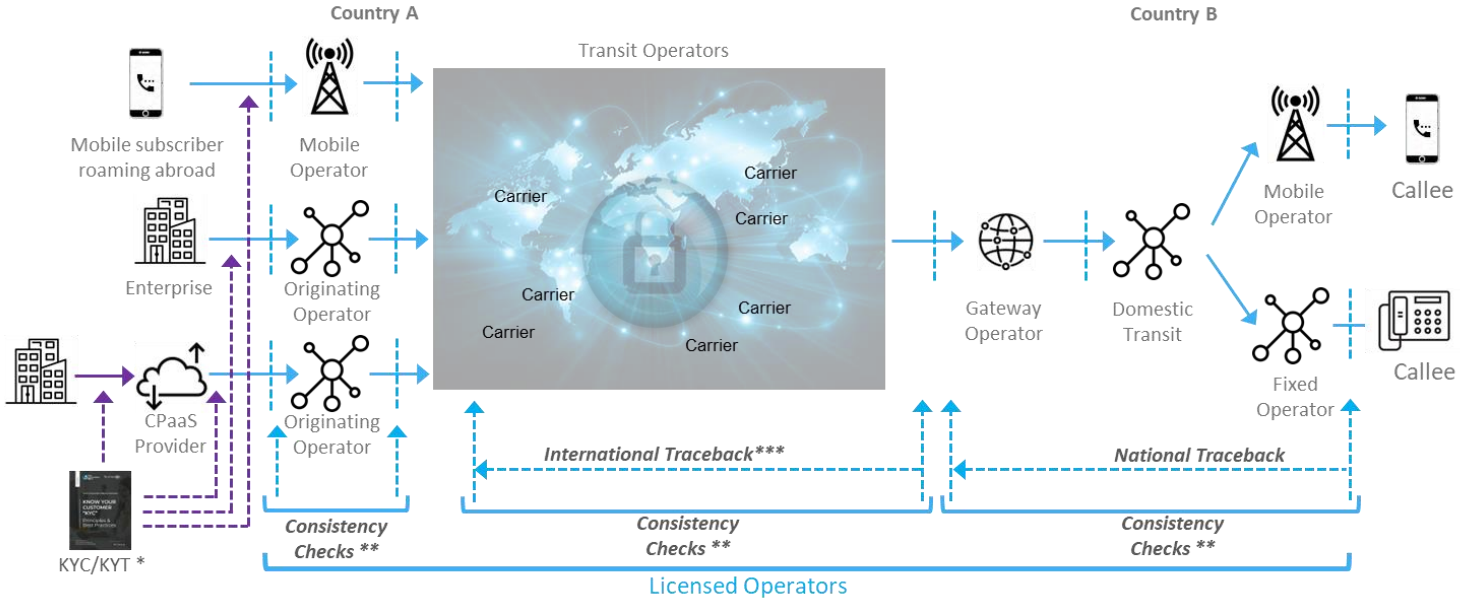
    - No calls allowed with a duration shorter than 3 minutes
    - No unsolicited marketing calls
    - No high volume of repeated calls from the same origination (From) Number within a rolling hour
    - No calls allowed from invalid, modified, spoofed or restricted origination (From) Numbers
    - Calls 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*

** *Consistency Checks executed per call/message*

*** *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 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
    Source: Licensed operator the number is assigned to
  - A **number uniquely identifies the caller** where it is one which the user has authority to use
    Source: Licensed operator or the third party the number is given rights to make calls to

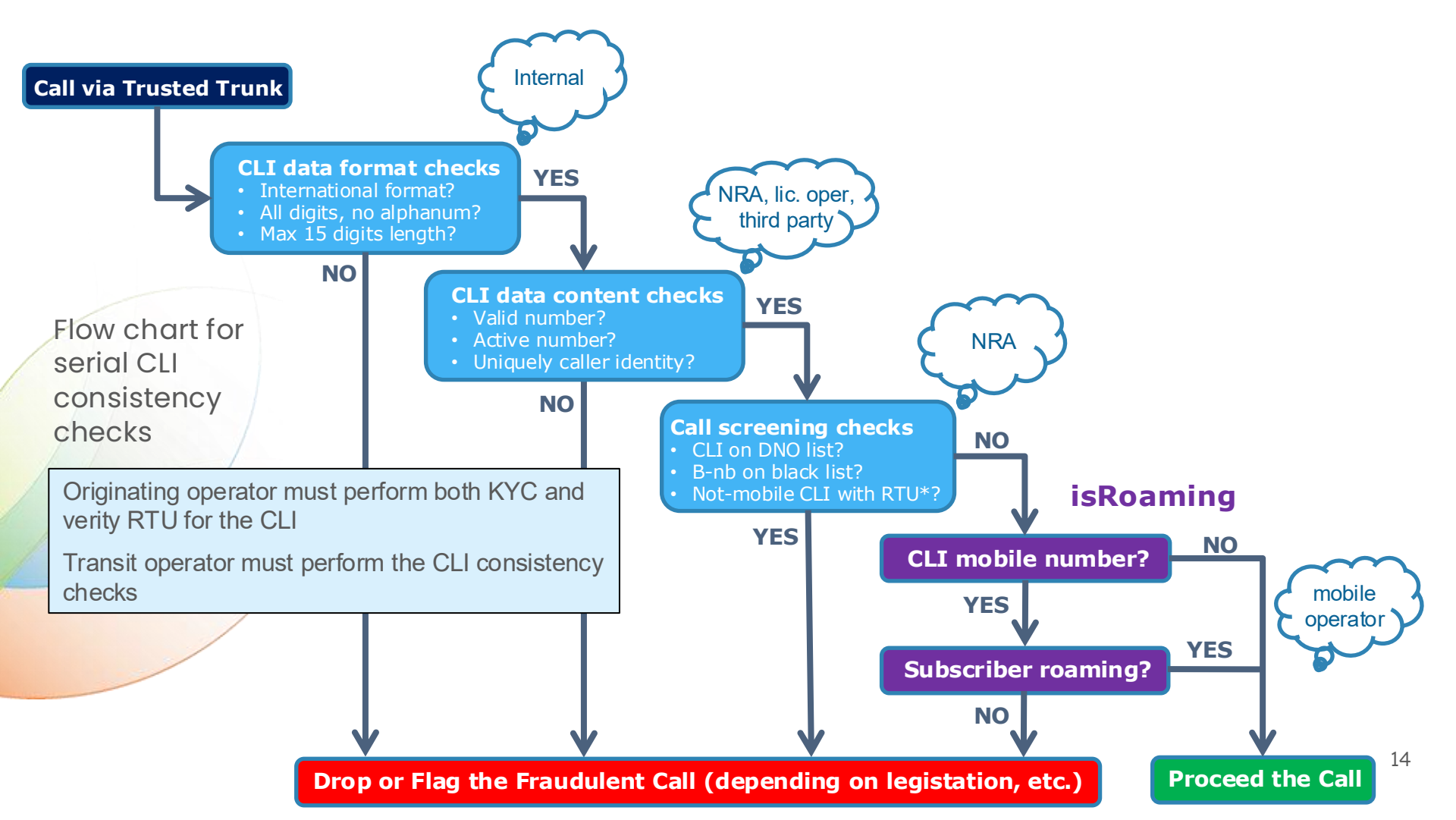
Authority matters & follow-up actions of CLI consistency checks

- Accurate, updated data is needed for the CLI consistency checks
  - For the CLI of a **landline** number 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
  - For the CLI of a **mobile** number 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
- The following guidelines apply:
  - CLI is **trusted;** then the CLI may be presented to the callee
  - CLI is **not trusted;** the call may be blocked or proceed. If the call proceeds:
    - 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 – additional 'isRoaming' technical check(s)
  - Telephone numbers assigned to users/organizations to generate calls from outside the country they belong to – explicit assignment for this use case could be requested by NRA
  - KYC/KYT polices can be set between:
    - Enterprises and CPaaS providers
    - CPaaS providers and licensed originating operators
    - Enterprises and originating operators
  - KYC/KYT polices about the use of numbers like:
    - Asymmetric numbers
    - Support of a Private Number service

- Trusted Trunks are secure logically separated trunks between carriers for transiting legitimate international traffic containing domestic CLI.
- Initial principles:
  - 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 polices above and it is therefore trusted


Call via Trusted Trunk
Internal
CLI data format checks
• International format?
• All digits, no alphanum?
• Max 15 digits length?
YES
NO
NRA, lic. oper, third party
CLI data content checks
• Valid number?
• Active number?
• Uniquely caller identity?
YES
NO
NRA
Call screening checks
• CLI on DNO list?
• B-nb on black list?
• Not-mobile CLI with RTU*?
NO
YES
isRoaming
CLI mobile number?
NO
YES
mobile operator
Subscriber roaming?
YES
NO
Drop or Flag the Fraudulent Call (depending on legistation, etc.)
Proceed the Call
Flow chart for serial CLI consistency checks
Originating operator must perform both KYC and verity RTU for the CLI
Transit operator must perform the CLI consistency checks

i3 Webinars

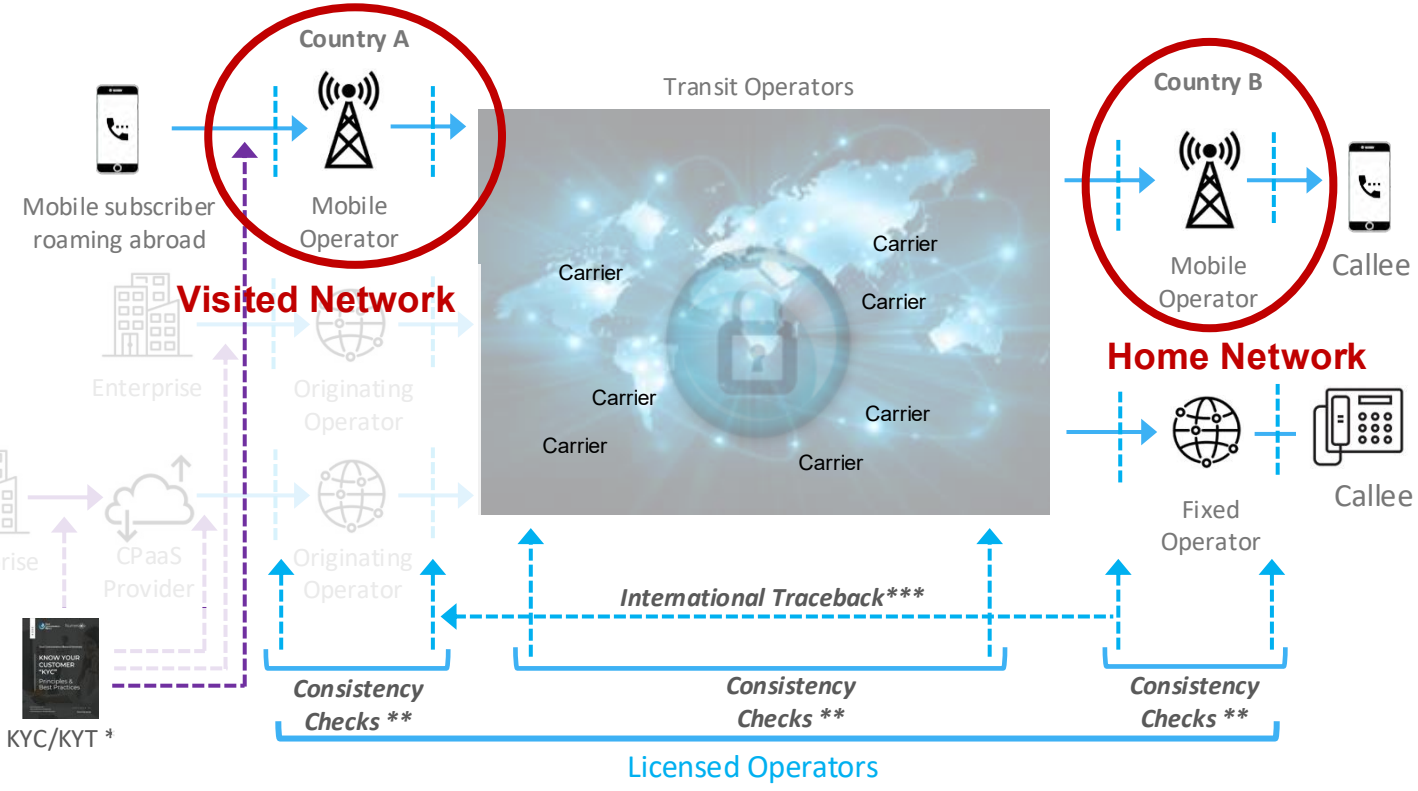
Mobile Roamer Identification Verification

Handling of Calls Originated by Mobile Subscribers Roaming Abroad

Pieter Veenstra

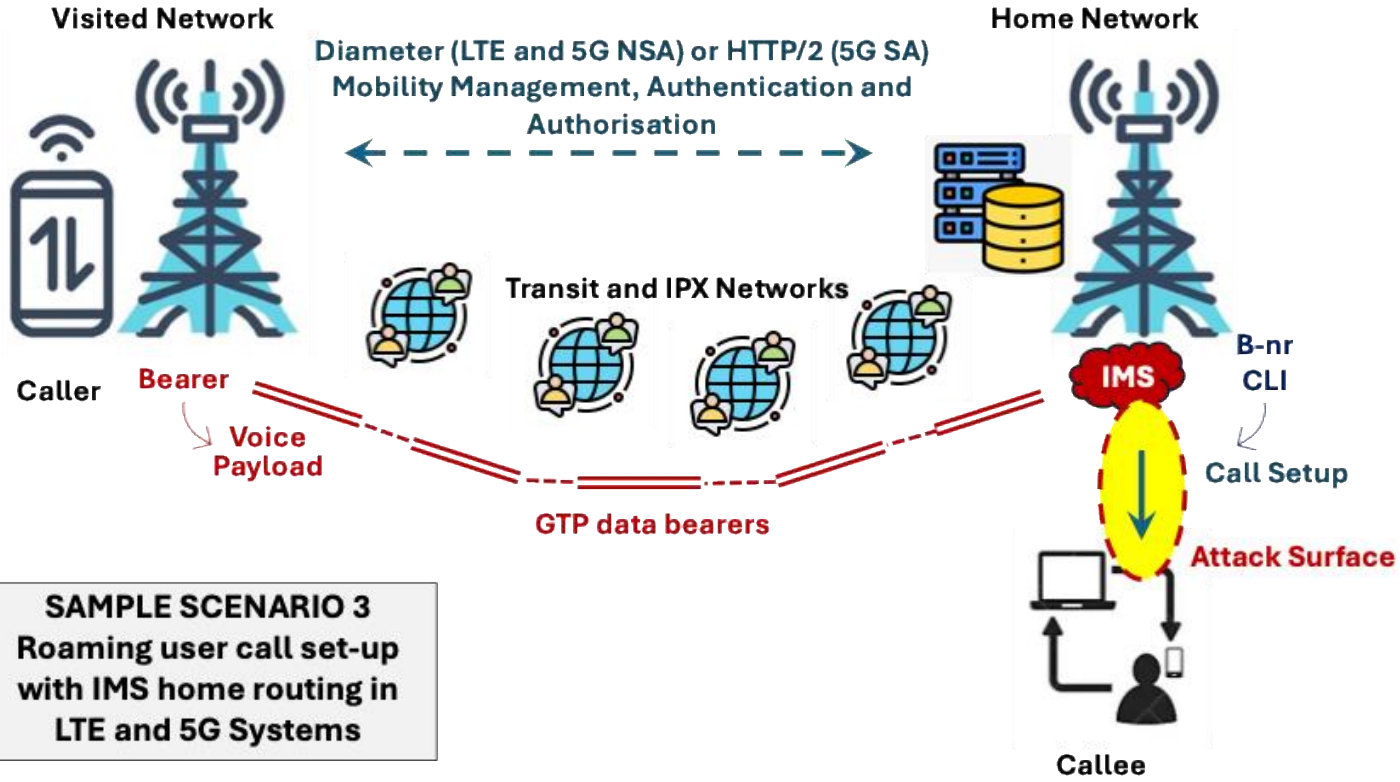
Use Case

- Refers to roamers in Visited Networks calling home (family/friends/business)
- Sensitive to vulnerabilities **if the Home Network is <u>not</u> in direct control**



Situation with VoLTE and 5G SA

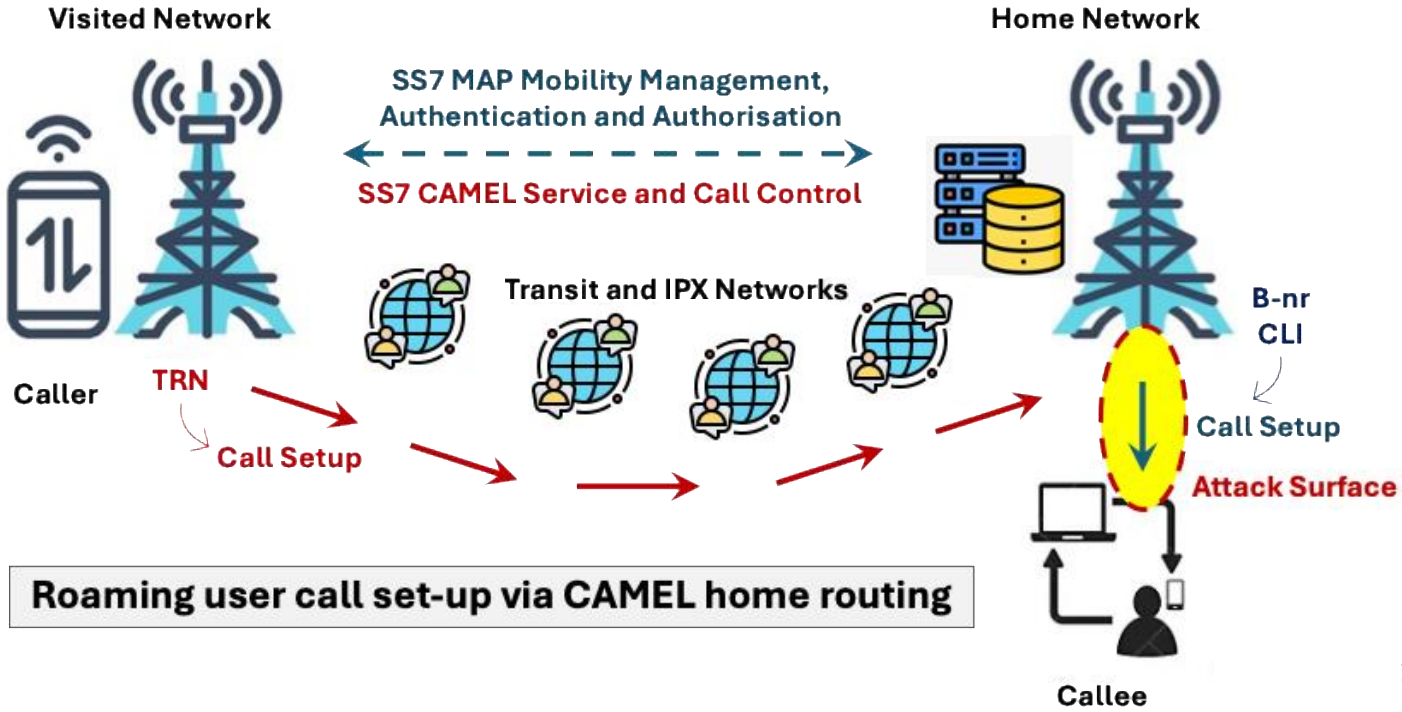
- Only the radio part of the Visited Network is involved by forwarding the voice packets from the device, all call control actions are within the Home Network
- **Home Network in full control**, reduction to **Minimum or Zero attack surface**



SAMPLE SCENARIO 3
Roaming user call set-up with IMS home routing in LTE and 5G Systems

- In this setting also the control part of the Visited Network is involved, with **all call control actions in the Visited Network controlled by the Home Network**
- Use of the Temporary Routing Number (TRN) makes a call **insensitive to manipulations** on the entire call path from Visited Network to Home Network
- **Home Network in full control**, reduction to **Minimum or Zero attack surface**

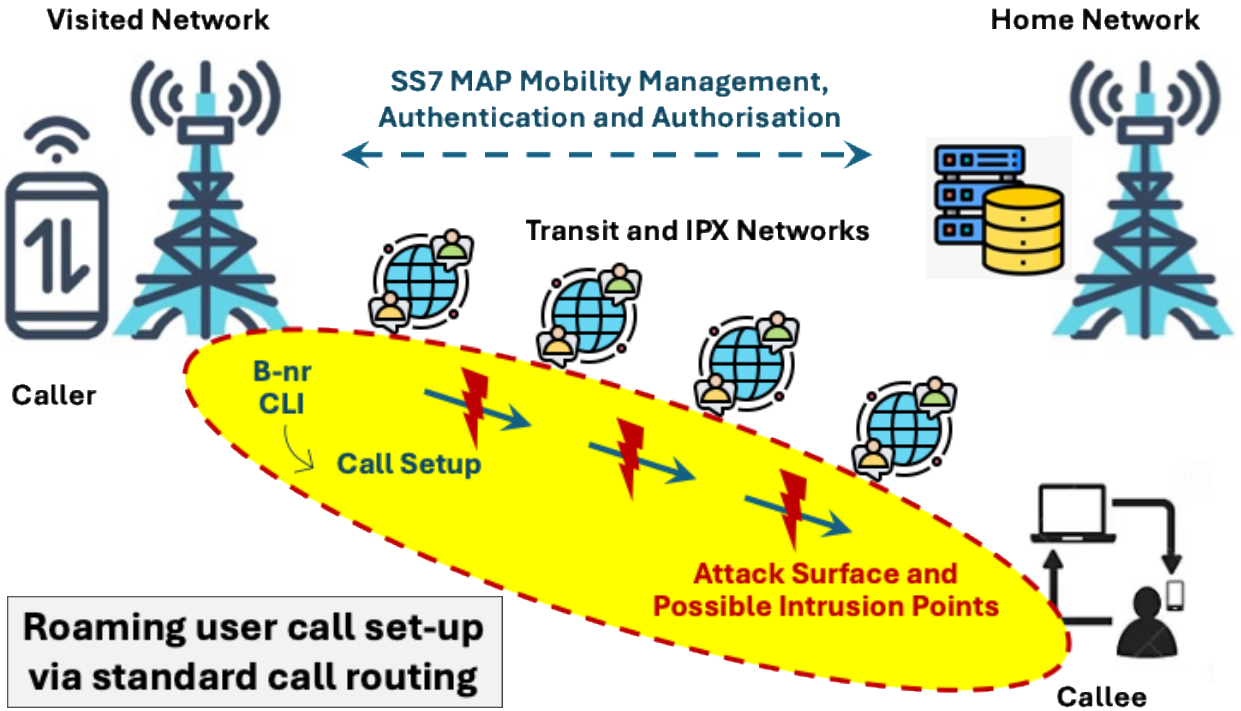
Situation 2G/3G with SS7 CAMEL*



* Needs implementation of TRN-based routing in CAMEL and voice trunks

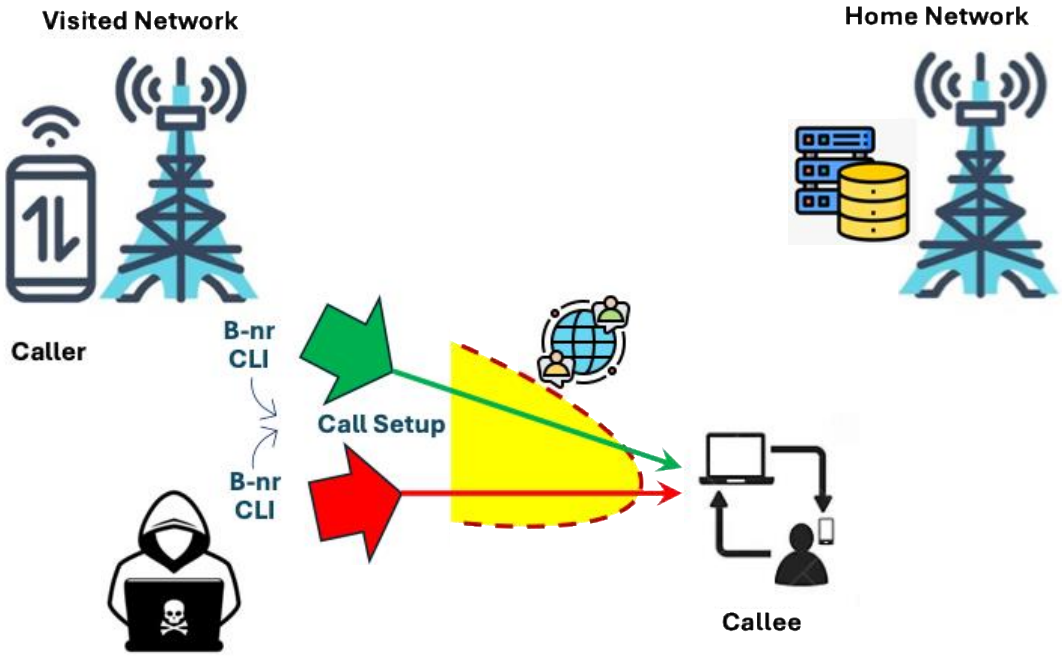
- Control part in Visited Network is involved **without control by Home Network**
- All call handling actions on transit (and possible manipulations) are **outside control and unverifiable by the Home Network**
- End-to-end call path vulnerable to intrusion, **no reduction of attack interface**

Situation 2G/3G with native SS7



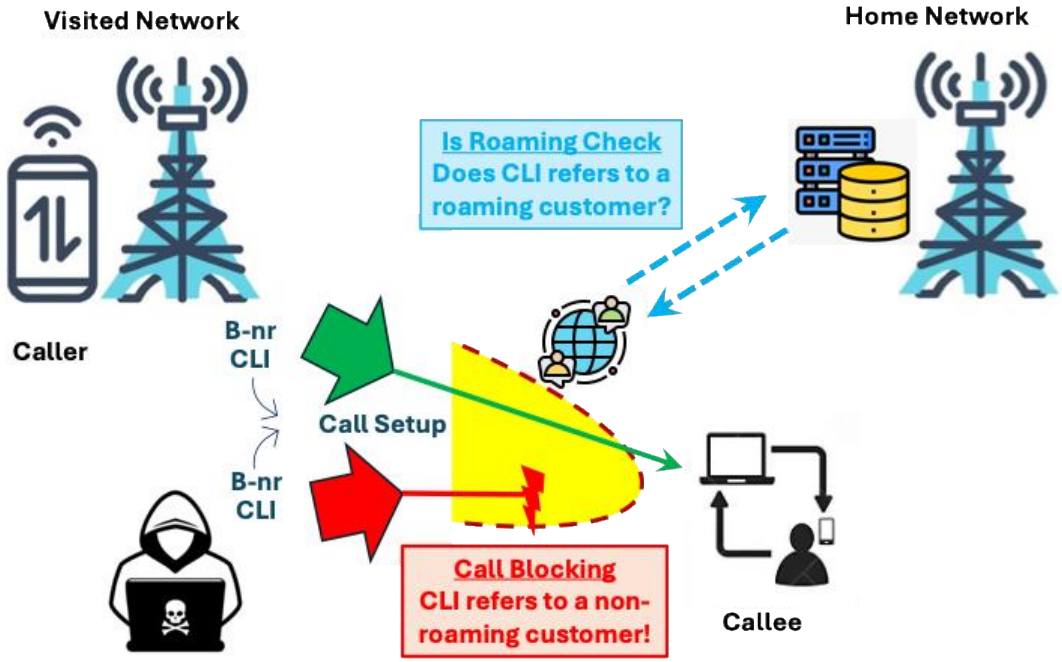
Problem

- At the outcoming International Switching Center (ISC), **true roaming calls** and **fake roaming calls** arrive with the same **B-nr and CLI, so not distinguishable**
- The KYC/KYT details of such CLIs (i.e., a national mobile number) are only known and verifiable **with the information known within the Home Network**
- **Fake roaming calls can pass unnoticed** to arrive at the Callee,
- These **attacks can be very harmful**



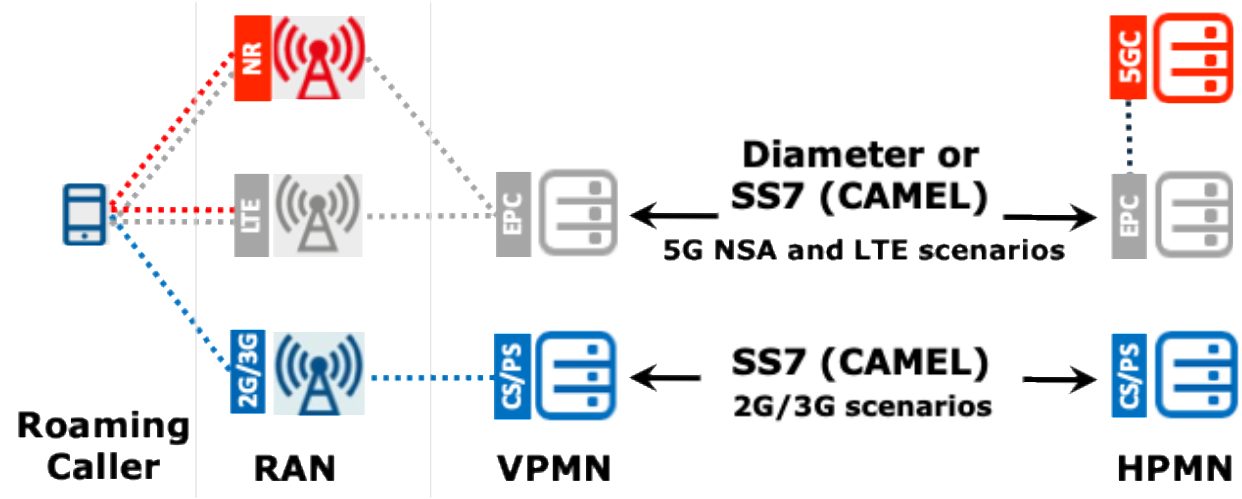
Solution =
Is Roaming Check

- **Current roaming status of an incoming roaming call** is checked by the ISC with the Home Network serving the CLI
- If the **Is Roaming Check is positive**, **the call proceeds to the Callee**
- If the **IS Roaming check is negative** , **the ISC blocks the call**
- Its implementation in operational networks (as of 2021) indicates a **very effective protection outcome**



Future need of Is Roaming Check

- **The risk continues** in the fragmented 2G-5G roaming global ecosystem with SS7 networks **and their signalling interworking scenarios** with Diameter
- Many operators with a CAMEL supporting SS7 signalling capability **are unwilling to deploy the TRN-based routing solution**
- **Additional entry points for the generation of fake roaming calls** are CPaaS cloud solutions and converged Fixed/Mobile enterprise solutions



Overview of the co-existence of the SS7, Diameter and interworking scenarios in the global 2G-5G roaming eco-system as per GSMA standard FS.40 – 5G Security Guide

i3 Webinars

CLI checks to protect italian subscribers

AGCom Regulation 106/25/CONS

Anna Lisa Scibetta

AGCOM 106/25/CONS Regulation - Key Players

General requirements

🌐 International Carriers

International carriers terminating traffic directed to Italian subscribers must register to AGCOM (public list).
They perform the blocking.

📱 Italian Mobile Operators

Managing mobile number ranges. They verify customer status.
Reply: "Block" or "Not Block"

How It Works:

- Fraudulent calls **stopped at the border** before entering Italian network
- Mobile operators provide simple binary answer (ensures rapid processing)
- No changes on called party number and MNP (Mobile Number Portability) handling

Calls scenarios with Italian CLIs

AGCom regulation addresses the handling of calls generated abroad and directed to Italian subscribers (i.e. any Italian called party number):

- **Calls not requesting specific checks or queries among operators including:**
  - CLI belonging to other countries (international CLI)
  - Italian CLI belonging to numbering ranges (decades) not assigned to subscribers allowed to make calls
- **Calls with Italian fixed CLI**
- **Calls with Italian mobile CLI**

Handling of calls not requesting specific checks or queries among operators

Calls that must be blocked by any international carrier authorized to terminate traffic in Italy:

- CLI format not compliant to ITU-T Recc. E.164 and E.157
- Absent CLI
- CLI does not begin with “+”, i.e. it is not in international format
- CLI contains only “+39” with no other digits
- CLI begins with “+39X” with X different from “0” (reserved to fixed subscribers) and “3” (reserved to mobile subscribers)

Default rule:

Italian fixed CLI (+390xxx) from abroad → **BLOCKED**

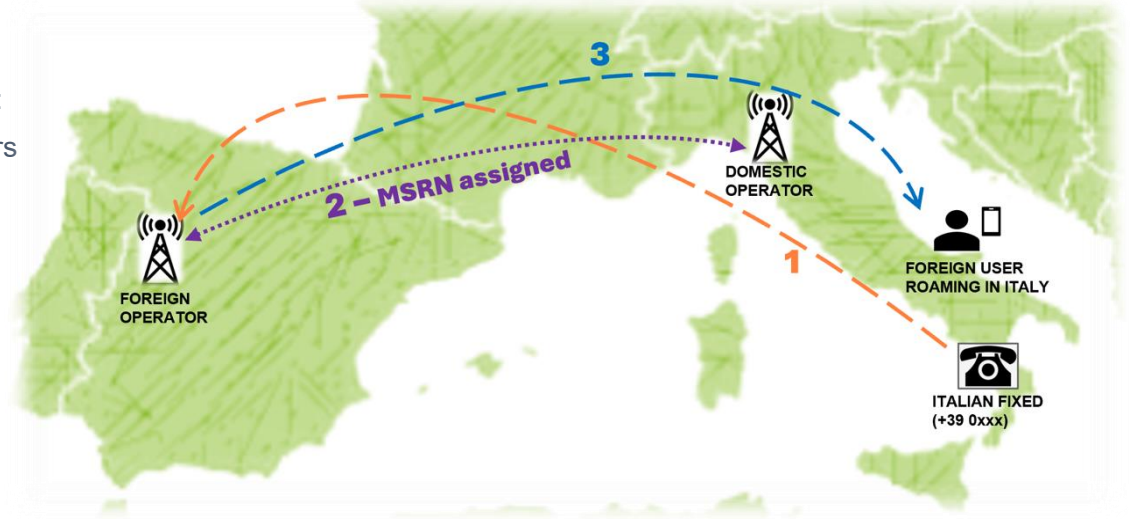
Exceptions (NOT BLOCKED):

Calls directed to "non-portable" number ranges:

✓ **MSRN** - temporary numbers for roaming users

✓ **Voicemail** - service numbers

Handling of calls with Italian fixed CLI

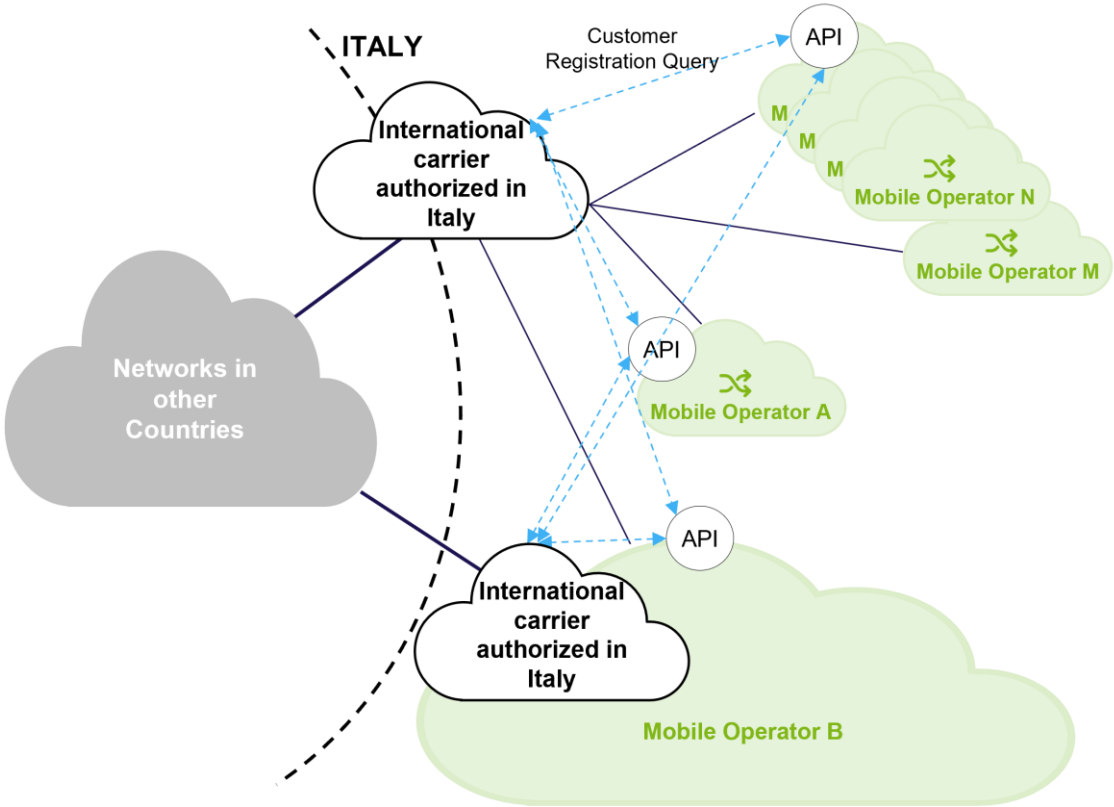


Legitimate Scenario:

1. Italian fixed calls foreign mobile subscriber roaming in Italy. Call routed to home network
2. Home network discovers that called subscribers is roaming in Italy. Italian MSRN assigned.
3. Call returns to Italy with MSRN as called party

Calls with Italian mobile CLI are allowed to be terminated only if the calling subscriber is actually roaming abroad

Handling of calls with Italian mobile CLI – Functional architecture



Handling of calls with Italian mobile CLI – first set of checks

1. Calls with Italian mobile CLI that does not belong to any range assigned to a licensed mobile operator must be blocked

2. Calls directed to “not portable” numbering ranges are allowed to be terminated without querying mobile operators. Legitimate call scenarios:

✓ An Italian mobile subscriber calling an **international mobile user** currently **roaming in Italy**

✓ An Italian mobile subscriber leaving a **message in the Voicemail** of another Italian mobile user roaming abroad and not reachable

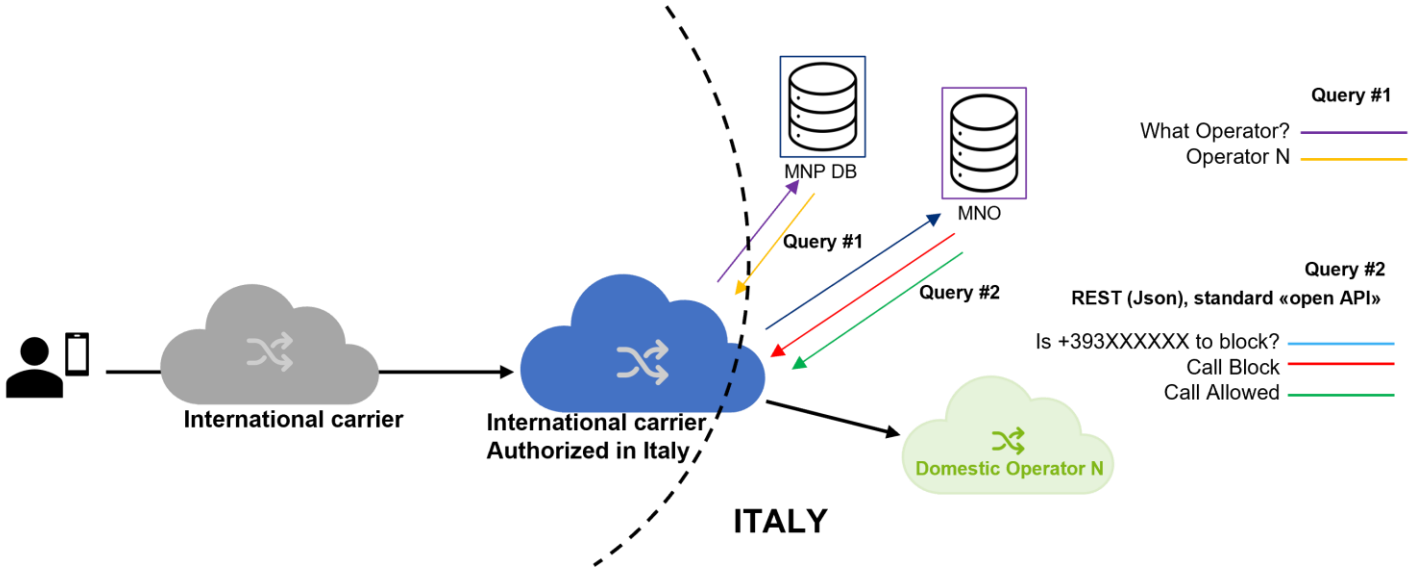
Handling of calls with Italian mobile CLI – query towards CLI recipient mobile operator

- International carriers authorized to terminate traffic in Italy are the only ones entitled to query mobile operators to retrieve information on calling subscriber
- international carrier authorized to terminate traffic in Italy must perform a **query via API** to the calling recipient mobile operator
- The operator performs internal checks to retrieve information on the calling subscriber and it replies with **“Block”** indication if:
  - 🚫 The CLI is not associated to any active subscriber
  - 🚫 The calling subscriber is attached to the home network
  - 🚫 The calling subscriber is not attached to any mobile network abroad
  - ✓ Otherwise the mobile operator provides back **“Not block”** indication
- The international carrier blocks or deliver the call depending on the response provided by the mobile operator

Handling of calls with Italian mobile CLI – query towards CLI recipient mobile operator

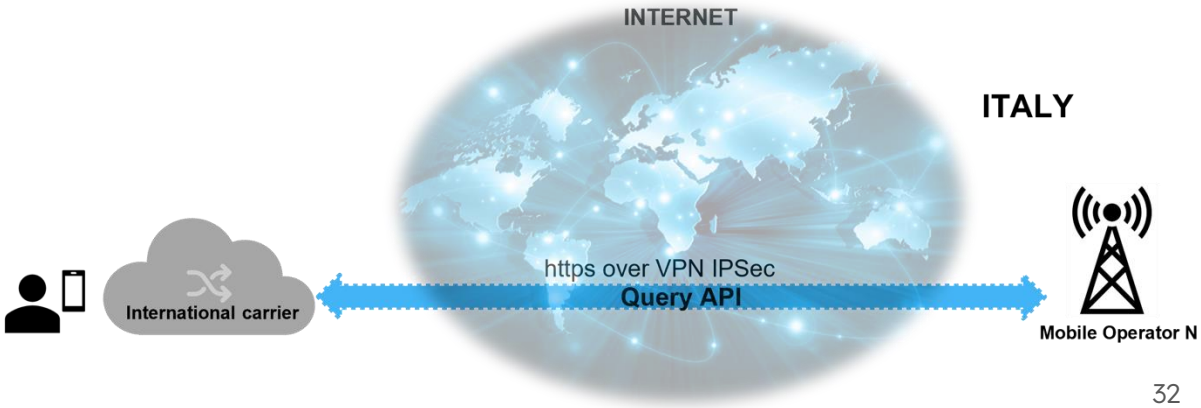
Call Allowed («Not Block») also in case of:

- query Timeout = max 2 sec
- Nr query/s > Max available query/s («Too many requests»)
- Nr query/s > Max sustenaible query/s («Bandwidth Limit Exceeded»)

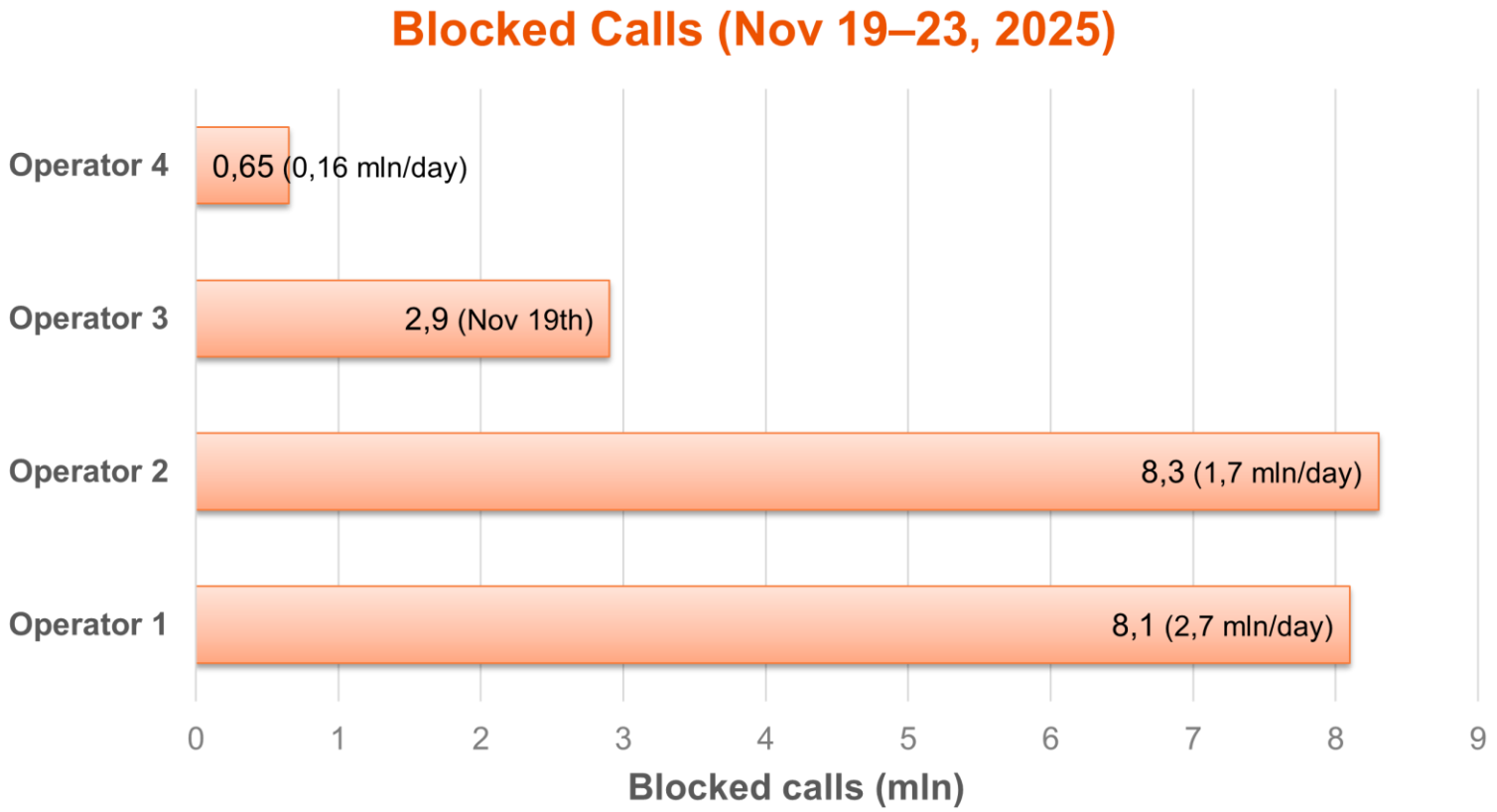


Handling of calls with Italian mobile CLI – API definition

- Standard API
- IP connectivity on IPSec VPN over Internet
- HTTPS with mutual authentication
- REST (JSON) standard OpenAPI
- The API includes periodic liveness query
- Standard reporting of queries and blocks



Handling of calls with Italian mobile CLI – CLI spoofing Block Result



In total, the four main Italian operators **blocked an average of approximately 7.46 million calls per day** between November 19 and 21, 2025.

Handling of calls with Italian mobile CLI – CLI spoofing Block Result

Impact of Measures

- Confirmation of widespread spoofing from abroad
- Effective blocking of illicit calls from Italian numbers
- Drastic reduction of phone scams via Italian CLI

Evolution of the Phenomenon

The phenomenon is shifting to new methods:

- Calls from abroad with international numbers (non-blockable)
- Possible increase in spam calls originated in Italy
- AGCOM intensifies surveillance and sanctions

Recommendations for Citizens

- Pay maximum attention to calls with international prefixes
- Be wary of contract/service offers over the phone
- Do not provide personal or banking data over the phone
- Report suspicious calls to authorities

AGCOM measures have proven effective in blocking millions of fraudulent calls.

i3 Webinars

Wrap up

Wrap up & conclusions

- CLI data generated by the originating platform/device and validated by the first licensed operator collecting the call, but it comes with issues

- There are legitimate use cases where the domestic CLI is used in international call paths without direct control from the network responsible for the numbering resource

- Countermeasures to guarantee CLI data reliability:

1. **Know Your Customer/Know Your Traffic** principles applied by the first licensed operator (originating operator)

2. **CLI consistency checks** (including isRoaming for mobile CLI) performed by originating, transit and terminating operators

3. **International Traceback** adopted by transit and terminating operators

4. **Trusted trunks** implemented among operators

5. **NRA requesting explicit assignment** of telephone numbers used to generate calls from outside the country they belong to

To learn more

i3forum Technology WG released the following documents (available at https://www.i3forum.org/workgroups/technology/):

- CLI consistency checks – Rel. 1.0
- Solutions for Restoring Trust in CLI for International Calls – Rel 1.0
- Solutions for Restoring Trust with Mobile Roamer Identification Verification – Rel. 1.0
- Analysis and Insights into the Technical Solutions for Restoring Trust with Mobile Roamer Identification Verification – Rel 1.0

i3 Webinars

Q&A

i3 Webinars

THANK YOU

Filippo Cauci
filippo.cauci@tisparkle.com

Pieter Veenstra
pieter@pietertelecom.com

Anna Lisa Scibetta
annalisa.scibetta@tisparkle.com