Analysis and Insights into the Technical Solutions for Restoring Trust with Mobile Roamer Identification Verification

Source: i3Forum Technology WG

Over the last few years, consumer trust in calling numbers (CLIs) displayed on their devices has significantly diminished. This is mainly due to the misuse and spoofing of CLIs by call originators from overseas, such as scammers and predatory sales callers, who exploit the ability to manipulate CLIs, compounded by a lack of global administrative control.

In response to the rapid increase in unwanted and fraudulent communications , the i3Forum launched the Restore Trust Initiative, bringing together the telecom industry (in One Consortium) and the regulators (in GIRAF) to fight global scams together. The i3Forum Technology Working Group compliments this work by creating recommendations, common understandings, uniform approaches, and technological frameworks. The set of WG deliverables can be found at https://i3forum.org/workgroups/technology/

The WG presentation "CLI consistency checks" provides an introduction to the various aspects why consumer trust in calling numbers (CLIs) displayed on their devices has significantly diminished over the last few years. This is followed by a comprehensive overview of CLI consistency checks and the countermeasures to guarantee CLI data reliability again.

This is accompanied by explanations in two abstract notations:

1. *The WG abstract "Solutions for Restoring Trust in CLI for International Calls" gives an overview of the Know Your Customer / Know Your Traffic (KYC / KYT) principes and best practices, numbering plan resources, call treatment actions, and the use of trusted trunks between operators.*
2. *The WG abstract "Solutions for Restoring Trust with Mobile Roamer Identification Verification" introduces the specific abuse of domestic mobile numbers from abroad, where attackers pose as roamers. This persistent problem forces operators to implement an iS Roaming Check solution, in addition to gradually mitigation the problem through IMS Home Routing with VoLTE and 5G SA and CAMEL Home Routing with 2G/3G networks.*

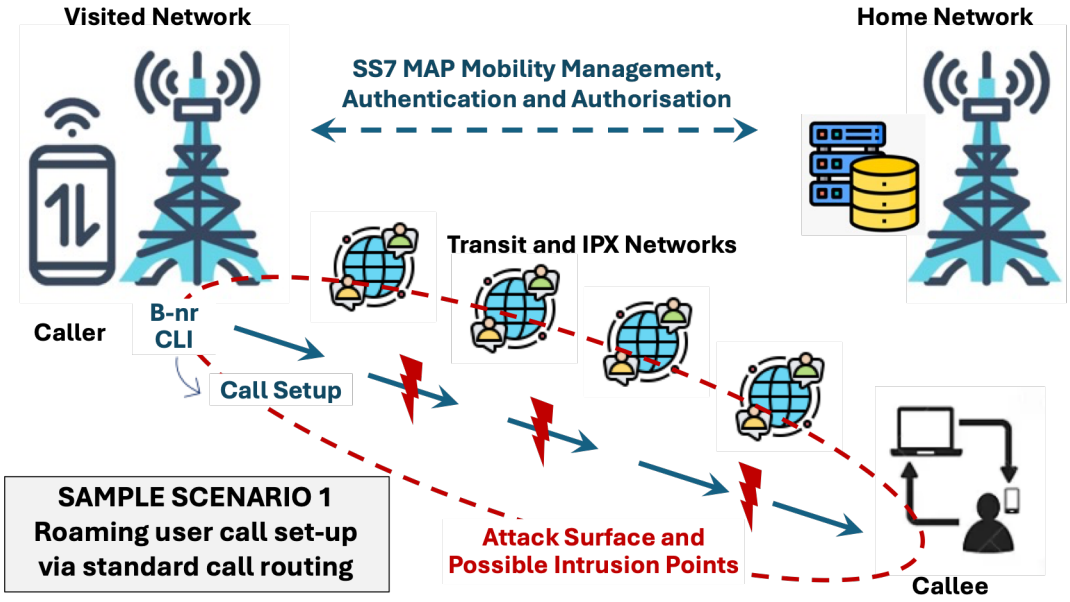
This position paper addresses the various aspects of item 2 in more detail. First, the technical working of outgoing calls made by roaming users in the various 2G-5G mobile systems is explained. Then, due to the coexistence of these roaming solutions, the needs are given for iS Roaming and for the support in international gateways. The paper concludes with a set of recommendations for IPX carriers.

1. Standard Call Handling in 2G/3G Systems [1]

Call handling in 2G/3G systems is handled by the circuit switching part. Initially calls initiated by roaming users where under control of the visited network only whereby the interactions between home network and visited network are limited to the authentication, authorisation and mobility management control commands via the MAP signalling in SS7. These calls are routed as standards calls with the CLI inserted by the visited network. The same working applies to call scenarios when 4G or 5G capable devices fall back to a 2G/3G network service due to limited radio coverage.

This comes with CLI validation challenges as the transit and IPX networks have limited knowledge about the validity of the CLI as the CLI is a number in the numbering plan of a foreign country. The figure gives this situation where the roaming user is the caller. The callee can be in any network and for the call there is no logical relation with the home network of the roaming user. The CLI is part of the Call Setup which makes the CLI vulnerable to manipulation on the path to the destination either during the routing actions by fraudulent Transit / IPX networks or by interception during its transfer.

[1] Detailed implementation guidelines are in GSMA IR.82 "SS7 Security Network Implementation Guidelines".

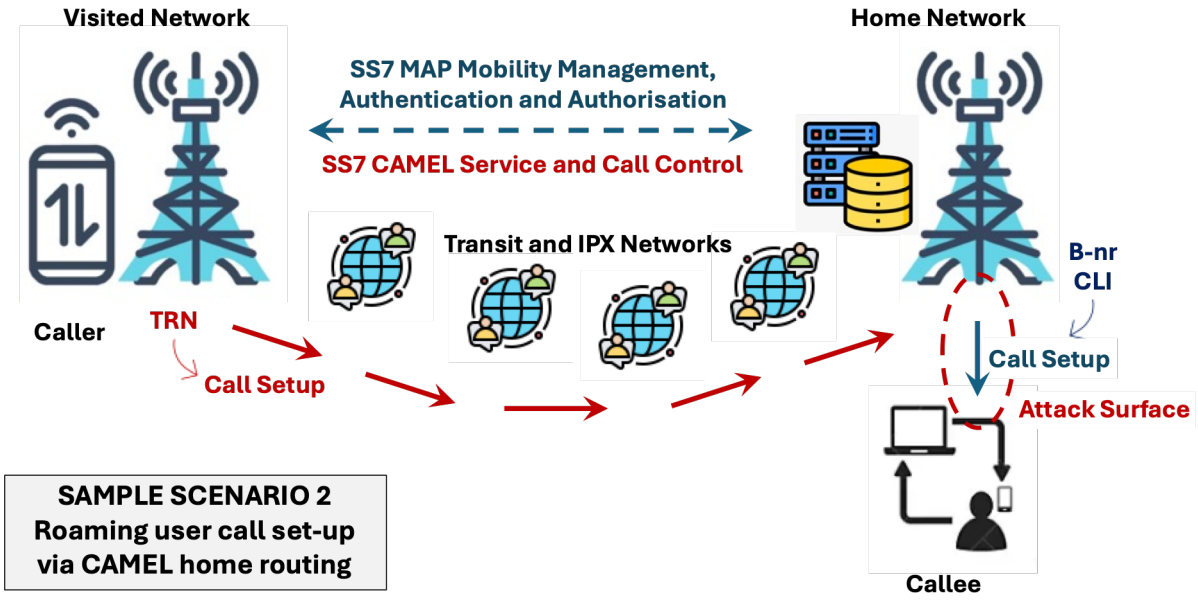


From the diagram it is clear that the transfer of the CLI is completely outside the control of the home network, making the attack surface widespread as it covers all network elements and connections between and including the Caller's visited network and the network serving the Callee.

2. Home Routing with CAMEL Support in 2G/3G Systems [2]

Initially CAMEL was introduced as an additional capability in SS7 for advanced service support to roaming users. The same CAMEL procedures can also be used for home routing as a means for the home network to protect its users against CLI manipulations practices as outlined above. When CAMEL is supported by the visited network and agreed in the roaming contract, then the home network is given control by CAMEL commands over the call handling actions in the visited network.

The following diagram illustrates how calls by roaming users are first routed to the home network via a Temporary Routing Number (TRN). Upon receipt, the home network replaces the TRN by the actual destination B-nr of the Callee and inserts the CLI of the Caller. Consequently, the CLI is not relevant on the CAMEL controlled call path to the home network and the CLI is fully trustable when the call leaves the home network to be routed to the network of the callee. The callee can be in any network and for the call there is no logical relation with the home network of the roaming user.



[2] Detailed implementation guidelines are in GSMA IR.82 "SS7 Security Network Implementation Guidelines".

The diagram elucidates that the attack surface is significantly reduced with CAMEL home routing. As the home network has full control of the CLI, the attack surface is limited to the connections between and including the Caller's home network and the network serving the Callee.

3. Home Routing with IMS Voice Roaming in LTE Systems [3] and 5G Systems [4]

With LTE, a completely different approach was taken with S8 Home Routing (S8HR), which was initially intended as a short-term solution via Diameter roaming connections for pilot deployments only. However, operators worldwide quickly adopted the S8HR solution for the Voice-over-LTE (VoLTE) service as part of their LTE roaming agreements, making it the default standard.

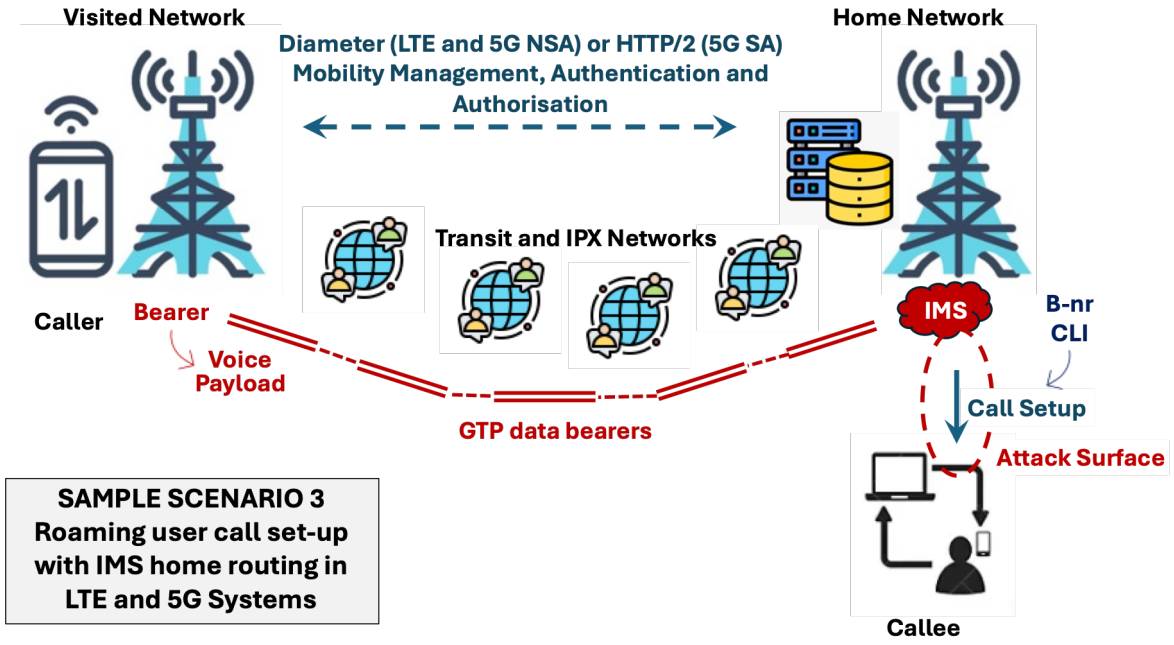
S8HR for VoLTE departs from the voice roaming services with SS7, as described in 1 and 2 above, because with S8HR there is no call logic involved anymore within the visited network. When a roaming user initiates a call, the voice payload from the device is directly exchanged via the radio network in the visited network to the IMS platform in the home network through GTP bearers via the S8 User Plane roaming interface.

The same S8HR solution is also used for roaming between 5G Non-Stand Alone (NSA) networks because in such scenarios the core networks are still using Diameter LTE-based service control.

As a result, the call setup begins in the home networks IMS. As the IMS platform provides the CLI for the caller, the CLI is effectively originated within the same region as the called number and the CLI is trustworthy.

In addition, the same IMS home routing approach was reapplied for the roaming solution between 5G Stand-Alone (5G SA) networks, implying that the core networks use the HTTP/2-based N32 control interface and the voice payload from the device is directly exchanged via the radio network in the visited network to the IMS platform in the home network through GTP bearers over the N8 User Plane roaming interface. In 5G this is referred to as the Voice-over-5G (Vo5G) service.

The following diagram illustrates this IMS home routing scenario with either Diameter for LTE and 5G NSA roaming control and HTTP/2 for 5G SA roaming control. In parallel, GTP data bearers are used to 'home route' the voice payload. As shown, only radio resources in the visited network are used, as the roaming user's device exchanges the voice payload directly with the IMS platform in the home network. The callee can be in any network and for the call there is no logical relation with the home network of the roaming user.



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

[3] Detailed implementation guidelines are in GSMA IR.88 "EPS Roaming Guidelines".

[4] Detailed implementation guidelines are in GSMA NG.113 "5GS Roaming Guidelines".

The diagram shows that, as in the CAMEL home routing scenario, the attack surface is limited to the connections between and including the Caller's home network and the network serving the Callee.

4. Coexistence Technical Roaming Solutions [5]

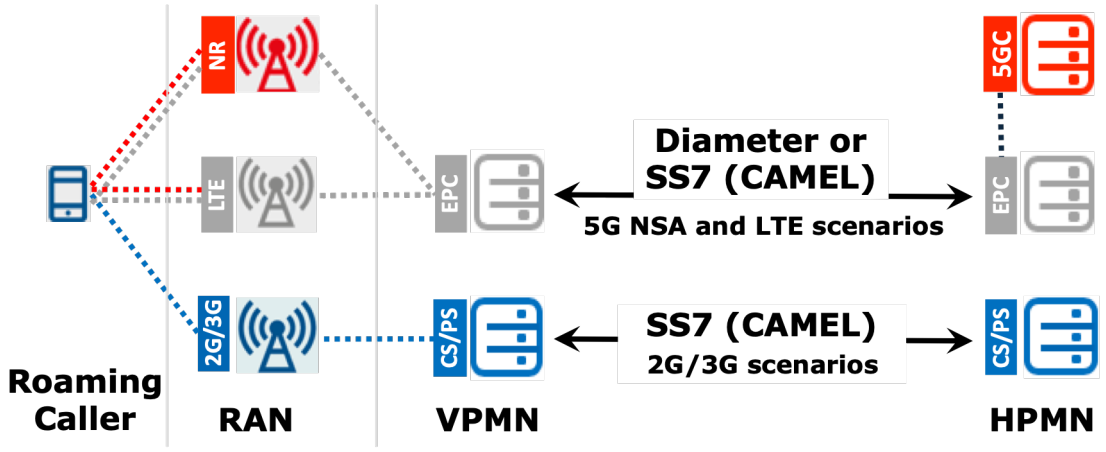
At present many international roaming contracts are still SS7 MAP based, and may include situations where operators already have their voice control migrated to SIP and decommissioned all SS7 ISUP signalling connections. This may refer to both bilateral roaming contracts, with direct SS7 signalling connections, or SS7 via intermediate roaming providers like IPX carriers and Roaming Hubs. In both direct and intermediate SS7 cases, home routing doesn't work unless both operator networks are able to support CAMEL and both operators have agreed to use the CAMEL home routing scenario.

Another reason that SS7 signalling connections are still popular is because of the roaming support needs for 2G and 3G devices. Though most handhelds are at least 4G enabled, limited 4G (5G) radio coverage will force handhelds to fallback to 2G/3G working. In addition, many M2M and IoT devices in automotive, metering, logistics, healthcare, etc. are still SS7 based given the lower costs of 2G/3G chipsets. This situation will not change very soon as M2M and IoT devices have long lifespans and involves huge cost and effort to replace.

So, a lot of ifs and buts that prevent operators to fully stop using SS7 for roaming support. And this will remain a risk for CLI integrity till the last SS7 signalling connection is phased out.

The following diagram sketches the situation that is typical for the years to come:

- The parallelism of technical mobile network generations showing that a 5G or LTE enabled device will automatically fall back to a 2G/3G working, with SS7 for the roaming connection, in case of limited LTE or NR radio coverage when paging in the visited network.
- Most network operators have implemented 5G New Radio (NR) but not yet a 5G Core (5GC), resulting in a 5G NSA working with an Evolved Packet Core (EPC), with Diameter (or SS7) for the roaming connection. The figure shows a missing 5GC in the visited network, but a 5GC may not yet be deployed in the home network either or may be missing in both.



5. Why is an 'is Roaming' check needed?

The above reasons and diagram show that even in the 5G NSA and LTE scenarios, not 100% of the calls by roaming users will be home routed because:

- The EPC standards support the interworking from Diameter to SS7. As a result, SS7 will be used between roaming partners for the 5G NSA and LTE roaming scenarios till their VoLTE roaming connections are upgraded to Diameter. Consequently, calls will not be home routed if CAMEL home routing is either not supported or not agreed as part of the roaming

[5] More details are provided in GSMA FS.40 "5G Security Guide".

agreement between a pair of roaming partners. This inability may be due various reasons such as:

- The implementation of CAMEL in older networks elements is not possible anymore.
- A functional limitation of the CAMEL implementation for support of home routing at either end because home routing requires a specific set of commands.
- A commercial reason (e.g., the HPMN would like to avoid the additional wholesale traffic costs of home routed calls by leaving the routing entirely to the VPMN).
- An operational reason (avoiding implementation effort) because the use of home routing needs more configuration work along the chain including active call filtering in the home country, see section 6.

- The SMS service is another roadblock for operators to completely disable SS7 as there is no support for the SMS service for all scenarios with Diameter and IP. This means that even if an operator has completely disabled its 2G/3G services, SS7 roaming connections still need to remain in service or via the interworking between SS7 to Diameter.

In conclusion, despite the risk of CLI abuse diminishes with home routing for actual calls, the risk of CLI spoofing does not disappear in due time given the massive SS7 roaming footprint and the many bypass actions via SS7. Mitigation this risk needs the implementation of 'is Roaming'.

Another need for 'is Roaming' is the inability to discriminate between calls from originating countries with CAMEL home routing implemented and countries that have not. This especially applies to incoming trunks that carry aggregated traffic from multiple originations. See for more details section 6.b.

6. What is needed in International Gateways (IGWs)?

Since IGWs are the first entry point into a country, actions against CLI spoofing should be implemented in these gateways due to their specific role and context.

a. Routing and per call filtering of MSRN and TRN number ranges

IGWs should forward calls to the mobile network to which the special MSRN and TRN number ranges are assigned.

No per call filtering action on these special number ranges apply for the international interfaces. Although these numbers are not allowed to be called by normal subscribers and originate calls, the IGWs do not know whether a MSRN or TRN is being called or originates a call abusively or not.

- Mobile Subscriber Routing Numbers (MSRN) are assigned to mobile networks by NRAs and used to route calls to users roaming on their network. MSRNs are temporary and are only 'live' for a few seconds.

- Only the visited network knows whether a MSRN is in use i.e. has been temporarily assigned to an inbound roamer and can therefore block incoming calls to MSRNs that have not been assigned.Temporary Routing Numbers (TRN) are assigned to mobile networks by NRAs and used by CAMEL enabled networks to route calls from any of it's users roaming abroad through it's network (CAMEL Home Routing). TRNs are temporary and are only 'live' for a few seconds.
  Only the home network knows whether a TRN is in use i.e. has been temporarily assigned to a call being made by its roaming user and can therefore block incoming calls to TRNs that have not assigned.

- Transit operators with IGWs, likely only in the terminating country, should filter MSRNs and TRNs as part of their Do Not Originate (DNO) lists to avoid that these CLIs are being abused.

b. Support of 'is Roaming' check and call treatment actions

Calls with a normal B-number and a CLI containing a domestic mobile number (i.e. calls made by roaming users abroad) are suspicious because they are not controlled via CAMEL home routing.

Either the call proceeds with the CLI deleted or anonymised, and so giving the callee an implicit indication that the CLI might be false, or and more accurately, an 'is Roaming' check is performed to block falsified calls referring to a CLI of a user that is not roaming.

Note - Anonymizing of the CLI (or replacing it with a specific string for no CLI) is the preferred option, allowing legitimate calls to pass with restricted CLIs while blocking calls may affect legitimate calls.

To perform the 'is Roaming' check, the IGW needs to query either the HPMN directly or send the query to a proxy solution. Further implementation details of the 'is Roaming' check are given hereafter in section c.

- If the query response indicates that the CLI refers to a non-roaming user, this is considered an exceptional situation. Then either the IGW should block the call or perform further checks to validate the trustworthy of the call and the CLI content. The last may refer to whitelists for exception cases or a making a call attempt to the CLI to cross-check the busy status of the user. The exact conditions may vary per national regulatory requirements and operator policies.
- If the query response indicates "not known", like in case of a network failure, errors, when the location is outdated (e.g., customer is on aboard of an airplane) or when the device is turned off, the call must proceed with the CLI deleted or anonymised.

c. CLI manipulation

With CAMEL home routing and/or 'is Roaming' solutions that is a need to manipulate CLI data like the home mobile network overwriting the received CLI data or when the CLI is to be anomysed due to an inclusive 'is Roaming' check.

7. Implementation variants of the 'is Roaming' check

Over time different technical solution directions were adopted by mobile operators to open their networks and transit operators with IGWs for the 'is Roaming' check to validate the CLI of incoming international voice calls:

- **SS7 MAP interfaces**
  The first operational implementations reused SS7 MAP messages. This refers to the ATI and SRI-SM messages for CLI Location Check. As these SS7 MAP messages have serious known security risks that require masked ATI or SRI-SM responses to protect the privacy of the user by withholding the subscriber location, subscriber states and subscriber identities. The implementation details and the comparison of both solutions are specified in GSMA[6].

  Given the severe security risks of these interconnections, these SS7 MAP interfaces need extended monitoring and adequate SS7 firewalling to protect the sensitive user profile data in the HLR and HSS databases[7].

- **National specified API interface**
  Later implementations are based on an API solution with an API definition agreed between the mobile operators and transit operators with IGWs in a country. This offers the advantage that each operator is free about the specifics of their implementation solution within their

[6] GSMA FS.21 - Interconnect Signalling Security Recommendations section 15.2 "CLI Spoofing Check"
[7] GSMA FS.11 - "SS7 Interconnect Security Monitoring and Firewall Guidelines" that defines an extensive set of methods for operators to monitor and to secure their SS7 roaming connections

domain. This may include CAMEL queries for roaming customers and internal query interfaces to the HLR and HSS. This variant avoids access to sensitive SS7 network interfaces, and the protection of the API interface can be tailored around the specific characteristics of the API commands.

- **GSMA Open Gateway with CAMARA Device Status primitive**
  More recently mobile operators are adopting the GSMA standardised Open Gateway framework for what CAMARA has standardised the Device Status primitive for querying the roaming status of a user. This offers the advantage that the mobile operators and transit operators with IGWs can refer to a standard API definition and common of the shelf products.

Most important is that mobile operators in a country decide on the same solution direction, so either to follow the SS7 MAP, the national specified API or the standardised CAMARA primitive approach, and on an agreed interface specification.

An additional implementation choice is like what operators decided in the past for the support of number portability, whether they agree on a shared proxy solution or not:

- **Shared Proxy/Hub Solution**
  Mobile operators and transit operators with IGWs in a country may mutually agree on a shared proxy solution with the advantage that queries can be made to a central instance. This simplifies the query process because operators do not need to know which number is served by which operator. The prerequisite is that all mobile operators and transit operators with IGWs trust the organisation running the shared proxy/hub platform and agree on a shared cost and funding model. An additional choice to be made is whether the proxy/hub is implemented as a reference database (light weight solution) or as well as an operational real-time query database.

- **Distributed Solution**
  To prevent subscriber information being shared, mobile operators and transit operators with IGWs may decide on a distributed solution. This implies that:

    - Number Portability (NP) queries for the CLI are to be sent to the mobile operator serving the CLI number based on number portability information.
    - The existence of an infrastructure of query interfaces among mobile operators and transit carriers for these NP queries.

      Note - Such an infrastructure may already exist and can be reused when the solution for Number Portability was implemented based on the distributed solution.

Which isroaming solution is favoured depends on many different factors. In this regard it may be questioned to what extent the advantages of a shared proxy/hub solution yield if all mobile operators and transit operators with IGWs in a country already have a local query solution for number portability in service.

8. Recommendations for IPX carriers

Based on the analysis in this position paper, IPX carriers should implement the following measures for Mobile Roamer Identification Verification in their egress IGWs:

1. Implement routing on TRN for CAMEL home routing calls, see section 6.a.

2. Other calls with a B-number and a CLI containing a domestic mobile number should:

    - Perform an ‘is Roaming’ check and block falsified calls referring to a CLI of a user that is not roaming, see section 6.b. The query method for ‘is Roaming’ depends per country what is agreed between the mobile operators and transit operators with IGWs, see section 6.c.

- If the user is roaming, perform further checks to validate the trustworthy of the call and the CLI content like whether the CLI is part of a Do Not Originate (DNO) list. If successful the call shall proceed with an anonymized CLI content to alarm subscribers and allow legitimate calls to pass, see section 6.c.
- The implementation of the ‘is Roaming’ is preferred to be based on the GSMA standardised Open Gateway framework for what CAMARA has standardised the Device Status primitive, but depends on the per country agreed implementation method between mobile operators and transit operators with IGWs , see section 6.c.
- Whether the implementation of the ‘is Roaming’ should be based on a proxy/hub solution or a distributed solution depends on the present implementation for number portability and what is the per country agreed solution between mobile operators and transit operators with IGWs , see section 6.c.